kaspersky

Kaspersky Security Center 15.1 Windows

© 2025 AO Kaspersky Lab

Contenu

Système d'aide de Kaspersky Security Center 15.1

Nouveautés

À propos de Kaspersky Security Center

- Architecture
- Configurations logicielle et matérielle
  - Configuration requise pour le Serveur d'administration
  - Configuration requise pour Web Console
  - Configuration requise pour les serveurs mobiles
  - Configuration requise pour la Console d'administration
  - Configuration requise pour l'Agent d'administration
- Compatible avec les applications et les solutions de Kaspersky
- Licence et fonctionnalités de Kaspersky Security Center 15.1
- À propos de la compatibilité des modules de Kaspersky Security Center
- Comparaison de Kaspersky Security Center : basé sur Windows et basé sur Linux
- À propos de Kaspersky Security Center Cloud Console

Kaspersky Security Center 15.1

- Notions principales
  - Serveur d'administration
  - Hiérarchie des Serveurs d'administration
  - Serveur d'administration virtuel
  - Serveur des appareils mobiles
  - Serveur Web
  - Agent d'administration
  - Groupes d'administration
  - Appareil administré
  - Appareil non défini
  - Poste de travail de l'administrateur
  - Plug-in d'administration
  - Plug-in Web d'administration
  - Stratégies
  - Profils de stratégie
  - Tâches
  - Zone d'action d'une tâche
  - Corrélation de la stratégie et des paramètres locaux de l'application
  - Point de distribution
  - Passerelle des connexions
- Principal scénario d'installation
- Ports utilisés par Kaspersky Security Center
- Certificats pour l'utilisation de Kaspersky Security Center
  - À propos des certificats de Kaspersky Security Center
  - À propos du certificat du Serveur d'administration
  - Conditions requises pour les certificats personnalisés utilisés dans Kaspersky Security Center
  - Scénario : Spécifier le certificat personnalisé du Serveur d'administration

- Remplacement du certificat du Serveur d'administration à l'aide de l'utilitaire klsetsrvcert
- Connexion des Agents réseau au Serveur d'administration à l'aide de l'utilitaire klmover
- Réémettre le certificat du Serveur Web

Schémas pour le trafic de données et l'utilisation du port

- Serveur d'administration et appareils administrés sur le LAN
- Serveur d'administration principal sur LAN et deux Serveurs d'administration secondaires
- Serveur d'administration sur réseau local, appareils administrés sur Internet, proxy inversé en cours d'utilisation
- Le Serveur d'administration sur LAN, les appareils administrés sur Internet, la passerelle de connexion en cours d'utilisation
- Serveur d'administration en DMZ, appareils administrés sur Internet
- Schémas d'interaction des modules de Kaspersky Security Center et des applications de sécurité : plus d'informations
  - Conventions utilisées dans les schémas d'interaction
  - Serveur d'administration et SGBD
  - Serveur d'administration et la Console d'administration
  - Serveur d'administration et appareil client : administration de l'application de sécurité
  - Mise à jour du logiciel sur l'appareil client par un point de distribution
  - Hiérarchie des Serveurs d'administration : Serveur d'administration principal et Serveur d'administration secondaire
  - Hiérarchie des Serveurs d'administration avec Serveur d'administration secondaire dans la zone démilitarisée
  - Serveur d'administration, passerelle de connexion dans un segment du réseau et appareil client
  - Serveur d'administration et deux appareils en DMZ : une passerelle de connexion et un appareil client
  - Serveur d'administration et Kaspersky Security Center Web Console
  - Activation et administration de l'application de sécurité sur un appareil mobile

Bonnes pratiques de déploiement

- Guide de renforcement
  - Déploiement du Serveur d'administration
  - Sécurité des connexions
  - Comptes et authentification
  - Gestion de la protection du Serveur d'administration
  - Gestion de la protection des appareils clients
  - Configuration de la protection des applications administrées
  - Maintenance du Serveur d'administration
  - Transfert d'événements vers des systèmes tiers
  - Recommandations de sécurité pour les systèmes d'information des tiers
  - Recommandations relatives à l'utilisation des applications de sécurité de Kaspersky
- Préparatifs du déploiement
  - Planification du déploiement de Kaspersky Security Center
    - Schémas typiques de déploiement du système de protection
    - À propos de la planification du déploiement de Kaspersky Security Center dans le réseau de l'entreprise
    - Sélection de la structure de protection de la société
    - Configurations typiques de Kaspersky Security Center
      - Configuration typique : un bureau
      - Configuration typique : quelques bureaux importants répartis géographiquement avec leurs propres administrateurs
      - Configuration typique : plusieurs petits bureaux isolés
    - Sélection d'un SGBD pour le Serveur d'administration
    - Configuration du serveur MariaDB x64 pour fonctionner avec Kaspersky Security Center 15.1
    - Configuration du serveur MySQL x64 pour fonctionner avec Kaspersky Security Center 15.1
    - Configuration du serveur PostgreSQL ou Postgres Pro pour fonctionner avec Kaspersky Security Center 15.1

Administration des appareils mobiles dotés de Kaspersky Endpoint Security for Android
Octroi de l'accès au Serveur d'administration via Internet
Accès depuis Internet : Serveur d'administration dans le réseau local
Accès depuis Internet : Serveur d'administration dans la zone démilitarisée
Accès depuis Internet : Agent d'administration en tant que passerelle de connexion dans la zone démilitarisée
À propos des points de distribution
Augmentation du nombre de descripteurs de fichiers pour le service klnagent
Calcul de la quantité et de la configuration des points de distribution
Hiérarchie des Serveurs d'administration
Serveurs d'administration virtuels
Informations sur les restrictions de Kaspersky Security Center
Charge sur le réseau
Déploiement initial de la protection antivirus
Mise à jour initiale des bases antivirus
Synchronisation du client avec le Serveur d'administration
Mise à jour complémentaire des bases antivirus
Traitement des événements des clients par le Serveur d'administration
Débit du trafic pendant 24 heures
Préparation de l'administration des appareils mobiles
Serveur MDM iOS
Configuration typique : Kaspersky Device Management for iOS en zone démilitarisée
Configuration typique : serveur MDM iOS sur le réseau local de l'entreprise
Administration des appareils mobiles dotés de Kaspersky Endpoint Security for Android
Informations sur la productivité du Serveur d'administration
Restrictions de connexion au Serveur d'administration
Résultats des essais de performances du Serveur d'administration
Résultats des tests de performance du Serveur proxy KSN
Paramètres réseau pour l'interaction avec des services externes
Déploiement de l'Agent d'administration et de l'application de sécurité
Déploiement initial
Configuration des paramètres des programmes d'installation
Paquets d'installation
Propriétés MSI et fichiers de transformation
Déploiement à l'aide d'outils tiers d'installation à distance d'applications
À propos des tâches d'installation à distance des applications de Kaspersky Security Center
Déploiement par prise d'image et copie d'image d'un appareil
Erreur d'exécution de la copie de l'image du disque dur
Déploiement à l'aide du mécanisme des stratégies de groupe Microsoft Windows
Déploiement forcé à l'aide d'une tâche d'installation à distance des applications de Kaspersky Security Center
Lancement de paquets autonomes créés par Kaspersky Security Center
Possibilités d'installation manuelle des applications
Création d'un fichier MST
Installation à distance des applications sur les appareils dotés de l'Agent d'administration
Administration du redémarrage des appareils dans la tâche d'installation à distance
Utilité de la mise à jour des bases de données dans le paquet d'installation de l'application de sécurité
Utilisation des outils d'installation à distance des applications de Kaspersky Security Center pour lancer des fichiers exécutables arbitraires sur les appareils administrés

Surveillance du déploiement
Configuration des paramètres des programmes d'installation
Informations générales
Installation en mode silencieux (avec fichier des réponses)
Installation de l'Agent d'administration en mode silencieux (sans fichier des réponses)
Configuration partielle des paramètres d'installation via setup.exe
Paramètres d'installation du Serveur d'administration
Paramètres d'installation de l'Agent d'administration
Infrastructure virtuelle
Recommandations sur la réduction de la charge sur les machines virtuelles
Prise en charge des machines virtuelles dynamiques
Prise en charge de la copie des machines virtuelles
Prise en charge de la restauration du système de fichiers pour les appareils dotés de l'Agent d'administration
Installation locale des applications
Installation locale de l'Agent d'administration
Installation de l'Agent d'administration en mode silencieux
Installation de l'Agent d'administration pour Linux en mode silencieux (avec un fichier de réponse)
Préparation d'un appareil exécutant Astra Linux dans l'environnement logiciel fermé mode pour l'installation de l'Agent d'administration
Installation de l'Agent d'administration pour Linux en mode interactif
Installation locale du plug-in d'administration des applications
Installation des applications en mode silencieux
Installation de l'application à l'aide des paquets autonomes
Paramètres du paquet d'installation de l'Agent d'administration
Consultation de la politique de confidentialité
Déploiement des systèmes d'administration des appareils mobiles
Déploiement du système d'administration selon le protocole MDM iOS
Installer le Serveur MDM iOS
Installation du Serveur MDM iOS en mode silencieux
Schémas du déploiement du Serveur MDM iOS
Schéma de déploiement simplifié
Schéma de déploiement avec utilisation de la délégation forcée Kerberos (KCD)
Réception du certificat APNs
Mise à jour du certificat APNs
Configurer un certificat de Serveur MDM iOS de réserve
Installation du certificat APNs sur le Serveur MDM iOS
Configuration de l'accès au service Apple Push Notification
Émission et installation d'un certificat général sur l'appareil mobile
Ajout d'un appareil KES à la liste des appareils administrés
Connexion des appareils KES au Serveur d'administration
Connexion directe des appareils au Serveur d'administration
Schéma de la connexion des appareils KES au serveur avec utilisation de la délégation forcée Kerberos (KCD)
Utilisation de Firebase Cloud Messaging
Intégration avec l'infrastructure à clé publique
Serveur Web de Kaspersky Security Center
Installation de Kaspersky Security Center
Préparation de l'installation

Comptes utilisateur pour l'utilisation d'un SGBD
Configuration des comptes pour l'utilisation avec SQL Server (authentification Windows)
Configuration des comptes pour l'utilisation avec SQL Server (authentification SQL Server)
Configuration des comptes pour l'utilisation avec MySQL et MariaDB
Déplacement de données d'un tablespace partagé vers un tablespace fichier par table dans les SGBD MySQL ou MariaDB
Configuration des comptes pour l'utilisation avec PostgreSQL et Postgres Pro
Scénario : authentification de Microsoft SQL Server
Scénario : Authentification du serveur MySQL
Scénario : Authentification du serveur PostgreSQL
Recommandations d'installation du Serveur d'administration
Création des comptes utilisateurs pour les services du Serveur d'administration sur un cluster haute disponibilité
Désignation du dossier partagé
Installation à distance à l'aide des outils du Serveur d'administration à l'aide de stratégies de groupe Active Directory
Installation à distance via la diffusion du chemin UNC vers le paquet autonome
Mise à jour depuis le dossier partagé du Serveur d'administration
Installation d'images des systèmes d'exploitation
Indication de l'adresse du Serveur d'administration
Installation standard
Étape 1. Lecture du Contrat de licence utilisateur final et de la Politique de confidentialité
Étape 2. Sélection du type d'installation
Étape 3. Installation de Kaspersky Security Center Web Console
Étape 4. Sélection de la taille du réseau
Étape 5. Sélection d'une base de données
Étape 6. Configuration des paramètres du serveur SQL
Étape 7. Sélection de la méthode d'authentification
Étape 8. Décompression et installation des fichiers sur le disque dur
Installation personnalisée
Étape 1. Lecture du Contrat de licence utilisateur final et de la Politique de confidentialité
Étape 2. Sélection du type d'installation
Étape 3. Sélection des modules pour l'installation
Étape 4. Installation de Kaspersky Security Center Web Console
Étape 5. Sélection de la taille du réseau
Étape 6. Sélection d'une base de données
Étape 7. Configuration des paramètres du serveur SQL
Étape 8. Sélection de la méthode d'authentification
Étape 9. Sélection du compte utilisateur pour lancer le Serveur d'administration
Étape 10. Sélection du compte utilisateur pour lancer les services de Kaspersky Security Center
Étape 11. Définition du dossier partagé
Étape 12. Configuration des paramètres de connexion au Serveur d'administration
Étape 13. Définition de l'adresse du Serveur d'administration
Étape 14. Adresse du Serveur d'administration pour la connexion des appareils mobiles
Étape 15. Sélection des plug-ins d'administration des applications
Étape 16. Décompression et installation des fichiers sur le disque dur
Déploiement du cluster de basculement Kaspersky Security Center
Scénario : Déploiement du cluster de basculement Kaspersky Security Center
À propos du cluster de basculement Kaspersky Security Center

Préparation d'un serveur de fichiers pour un cluster de basculement Kaspersky Security Center
Préparation des nœuds pour un cluster de basculement Kaspersky Security Center
Installation de Kaspersky Security Center sur les nœuds du cluster de basculement Kaspersky Security Center
Démarrage et arrêt manuels des nœuds de cluster
Installation du Serveur d'administration sur un cluster de basculement Windows Server
Étape 1. Lecture du Contrat de licence utilisateur final et de la Politique de confidentialité
Étape 2. Sélection du type d'installation sur le cluster
Étape 3. Spécification du nom du Serveur d'administration virtuel
Étape 4. Spécification des détails du réseau du Serveur d'administration virtuel
Étape 5. Spécification d'un groupe de clusters
Étape 6. Sélection d'un stockage de données de cluster
Étape 7. Spécification d'un compte pour l'installation à distance
Étape 8. Sélection des modules pour l'installation
Étape 9. Sélection de la taille du réseau
Étape 10. Sélection d'une base de données
Étape 11. Configuration des paramètres du serveur SQL
Étape 12. Sélection de la méthode d'authentification
Étape 13. Sélection du compte utilisateur pour lancer le Serveur d'administration
Étape 14. Sélection du compte utilisateur pour lancer les services de Kaspersky Security Center
Étape 15. Définition du dossier partagé
Étape 16. Configuration des paramètres de connexion au Serveur d'administration
Étape 17. Définition de l'adresse du Serveur d'administration
Étape 18. Adresse du Serveur d'administration pour la connexion des appareils mobiles
Étape 19. Décompression et installation des fichiers sur le disque dur
Installation du Serveur d'administration en mode silencieux
Installation de la Console d'administration sur le poste de travail de l'administrateur
Modifications du système après l'installation de Kaspersky Security Center
Suppression de l'application
À propos de la mise à jour de Kaspersky Security Center
Mise à jour de Kaspersky Security Center depuis une version antérieure
Mise à jour de Kaspersky Security Center sur les nœuds du cluster de basculement Kaspersky Security Center
Mise à jour de Kaspersky Security Center sur les nœuds du cluster de basculement Microsoft
Configuration initiale de Kaspersky Security Center
Guide de renforcement
Assistant de configuration initiale du Serveur d'administration
À propos de l'assistant de démarrage rapide de l'application
Démarrage de l'Assistant de configuration initiale du Serveur d'administration
Étape 1. Configuration des paramètres du serveur proxy
Étape 2. Sélection de la méthode d'activation de l'application
Étape 3. Sélection des zones de protection et des systèmes d'exploitation
Étape 4. Installation des plug-ins pour les applications administrées
Étape 5. Téléchargement des paquets de distribution et création des paquets d'installation
Étape 6. Configuration de Kaspersky Security Network
Étape 7. Configuration des notifications par email
Étape 8. Configuration de la gestion des mises à jour
Étape 9. Création de la configuration initiale de la protection
Étape 10. Connexion pour les appareils mobiles

Étape 11. Téléchargement des mises à jour
Étape 12. Recherche d'appareils
Étape 13. Fin de l'Assistant de configuration initiale de l'application
Configuration de la connexion de la Console d'administration au Serveur d'administration
Configuration des paramètres d'accès Internet du Serveur d'administration.
Connexion d'appareils itinérants
Scénario : connexion d'appareils itinérants via une passerelle de connexion
Scénario : Connexion d'appareils itinérants via un Serveur d'administration secondaire dans la DMZ
À propos de la connexion d'appareils itinérants
Connexion d'appareils de bureau externes au Serveur d'administration
À propos des profils de connexion pour les utilisateurs itinérants
Création d'un profil de connexion pour les utilisateurs itinérants
À propos du transfert de l'Agent d'administration à d'autres Serveurs d'administration
Création d'une règle de permutation de l'Agent d'administration selon l'emplacement réseau
Notifications sur les événements
Configuration des paramètres de notification sur les événements
Vérification de déploiement des notifications
Notification relative aux événements via un fichier exécutable
Chiffrer la communication selon TLS
Configuration de l'interface
Recherche d'appareils en réseau
Scénario de recherche d'appareils en réseau
Appareils non définis
Recherche d'appareils
Sondage du réseau Windows
Sondage Active Directory
Sondage des plages IP
Sondage Zeroconf
Travail avec les domaines Windows. Affichage et modification des paramètres du domaine
Configuration des règles de rétention pour les appareils non définis
Travail avec les plages IP
Création de la plage IP
Affichage et modification des paramètres de plage IP
Travail avec les groupes Active Directory. Affichage et modification des paramètres du groupe
Création des règles de déplacement automatique des appareils dans un groupe d'administration
Utilisation du mode dynamique VDI sur les appareils clients
Activation du mode dynamique VDI dans les propriétés du paquet d'installation de l'Agent d'administration
Recherche d'appareils qui font partie de VDI
Déplacement dans le groupe d'administration des appareils qui font partie de VDI
Inventaire du matériel
Ajout d'informations sur les nouveaux appareils
Configuration des critères de définition des appareils d'entreprise
Configuration des champs personnalisés
Licences
Événements de dépassement de la restriction de licence
À propos des licences
À propos de la licence

À propos du contrat de licence utilisateur final
À propos du certificat de licence
À propos de la clé de licence
À propos du fichier clé
À propos de l'abonnement
À propos du code d'activation
Révocation d'un Contrat de licence utilisateur final
À propos de la collecte des données
Options de licence de Kaspersky Security Center
Particularités de l'octroi de la licence Kaspersky Security Center et des applications administrées
Applications Kaspersky. Déploiement centralisé
Remplacement d'application de sécurité d'éditeurs tiers
Installation des applications à l'aide de la tâche d'installation à distance
Installation de l'application sur les appareils sélectionnés
Installation de l'application sur les appareils clients d'un groupe d'administration
Installation de l'application à l'aide des stratégies de groupe Active Directory
Installation à distance des applications sur les appareils macOS
Installation des applications sur les Serveurs d'administration secondaires
Installation des applications à l'aide de l'Assistant de l'installation à distance
Utilisation des plug-ins d'administration
Consultation du rapport sur le déploiement de la protection
Désinstallation à distance des applications
Désinstallation à distance d'une application sur les appareils clients du groupe d'administration
Désinstallation à distance de l'application des appareils sélectionnés
Fonctionnement avec les paquets d'installation
Génération du paquet d'installation
Création de paquets d'installation autonomes
Génération des paquets d'installation personnalisés
Consultation et modification des propriétés des paquets d'installation personnalisés
Obtention du paquet d'installation de l'Agent d'administration à partir du kit de distribution de Kaspersky Security Center
Propagation des paquets d'installation sur les Serveurs d'administration secondaires
Propagation des paquets d'installation à l'aide des points de distribution
Transfert dans Kaspersky Security Center des informations sur les résultats d'installation de l'application
Définition de l'adresse du Serveur proxy KSN pour les paquets d'installation
Récupération des version actuelles des applications
Préparation de l'appareil Windows pour l'installation à distance
Préparation d'un appareil Linux et installation de l'Agent d'administration sur un appareil Linux à distance
Préparation d'un appareil exécutant SUSE Linux Enterprise Server 15 pour l'installation de l'Agent d'administration
Préparation de l'appareil fonctionnant sous le système d'exploitation macOS à l'installation à distance de l'Agent d'administration
Applications Kaspersky : licence et activation
Licence des applications administrées
Consultation des informations sur les clés de licence utilisées
Ajout de la clé de licence dans le stockage du Serveur d'administration
Suppression de la clé de licence du Serveur d'administration
Déploiement d'une clé de licence sur les appareils clients

Diffusion automatique de la clé de licence
Création et consultation du rapport sur les clés de licence utilisées
Affichage des informations sur les clés de licence d'application
Exportation d'un fichier de clé de licence
Configuration de la protection réseau
Scénario : Configuration de la protection réseau
Configuration et diffusion des stratégies : approche centrée sur l'appareil
À propos des méthodes d'administration de la sécurité centrées sur l'appareil et l'utilisateur
Configuration manuelle d'une stratégie de Kaspersky Endpoint Security
Configuration de la stratégie dans la section Protection avancée
Configuration de la stratégie dans la section Protection principale
Configuration de la stratégie dans la section Paramètres généraux
Configuration de la stratégie dans la section Configuration d'événement
Configuration manuelle d'une tâche de groupe de mise à jour de Kaspersky Endpoint Security
Configuration manuelle d'une tâche de groupe d'analyse de l'appareil de Kaspersky Endpoint Security
Planification de la tâche Recherche de vulnérabilités et des mises à jour requises
Configuration manuelle d'une tâche de groupe d'installation des mises à jour et de correction des vulnérabilités
Définition du nombre d'événements maximal dans le stockage d'événements
Définition de la durée maximale de stockage des informations sur les vulnérabilités corrigées
Gérer les tâches
Création d'une tâche
Création d'une tâche du Serveur d'administration
Création d'une tâche pour un ensemble d'appareils
Création d'une tâche locale
Affichage d'une tâche de groupe héritée dans l'espace de travail du groupe imbriqué
Activation automatique des appareils avec le lancement de la tâche
Arrêt automatique de l'appareil après l'exécution de la tâche
Limitation de la durée d'exécution de la tâche
Exportation d'une tâche
Importation d'une tâche
Conversion des tâches
Démarrage et arrêt manuels des tâches
Suspension et reprise manuelles d'une tâche
Suivi et affichage des comptes rendus d'activité des tâches
Affichage de l'historique des tâches entreposé sur le Serveur d'administration
Configuration du filtre d'informations sur les résultats de l'exécution de la tâche
Modification d'une tâche. Restauration des modifications
Comparaison des tâches
Comptes utilisateur pour le lancement des tâches
Exporter l'historique d'exécution des tâches
Assistant de modification du mot de passe des tâches
Étape 1. Spécification des informations d'identification
Étape 2. Sélection d'une action à entreprendre
Étape 3. Affichage des résultats
Création d'une hiérarchie des groupes d'administration soumis au Serveur d'administration virtuel
Stratégies et profils de stratégie
Hiérarchie des stratégies, utilisation des profils de stratégie

Hiérarchie des stratégies
Profils de stratégie
Héritage des paramètres d'une stratégie
Administration des stratégies
Création d'une stratégie
Affichage des stratégies héritées dans le groupe imbriqué
Activation d'une stratégie
Activation automatique d'une stratégie lors d'un événement " Propagation de virus "
Application des stratégies pour les utilisateurs autonomes
Modification d'une stratégie. Restauration des modifications
Comparaison des stratégies
Affichage du graphique de l'état de la distribution des stratégies
Suppression d'une stratégie
Copie d'une stratégie
Exportation d'une stratégie
Importation d'une stratégie
Conversion des stratégies
Administration des profils de stratégies
Création d'un profil de stratégie
Modification du profil de stratégie
Suppression d'un profil de stratégie
Création d'une règle d'activation du profil de stratégie
Règles de déplacement des appareils
Clonage Règles de déplacement des appareils
Catégorisation du logiciel
Conditions indispensables pour l'installation des applications sur les appareils de l'entreprise cliente
Consultation et modification des paramètres locaux de l'application
Mise à jour de Kaspersky Security Center et des applications administrées
Scénario : Mise à jour régulière des bases de données et des applications Kaspersky
À propos de la mise à jour des bases de données, des modules logiciels et des applications de Kaspersky
À propos de l'utilisation de fichiers diff pour la mise à jour des bases de données et des modules logiciels Kaspersky
Activation de la fonction de téléchargement des fichiers diff
Création de la tâche de téléchargement des mises à jour dans le stockage du Serveur d'administration
Création de la tâche de téléchargement des mises à jour sur les stockages des points de distribution
Configuration de la tâche Télécharger les mises à jour dans le stockage du Serveur d'administration
Analyse des mises à jour récupérées
Configuration des stratégies de vérification et des tâches auxiliaires
Affichage des mises à jour récupérées
Installation automatique des mises à jour pour Kaspersky Endpoint Security sur les appareils
Modèle hors ligne de téléchargement des mises à jour
Activation et désactivation d'un modèle hors ligne de téléchargement des mises à jour
Installation automatique des mises à jour et des correctifs pour les modules de Kaspersky Security Center
Activation et désactivation de l'installation automatique des mises à jour et des correctifs pour les modules de Kaspersky Security Center
Déploiement de mises à jour automatique
Déploiement automatique des mises à jour sur les appareils clients
Redistribution automatique des mises à jour sur les Serveurs d'administration secondaires

Assignation automatique des points de distribution
Assignation manuelle d'un point de distribution à un appareil
Suppression d'un appareil de la liste des points de distribution
Téléchargement des mises à jour par les points de distribution
Suppression des mises à jour logicielles dans le stockage
Installation du correctif pour l'application Kaspersky dans le modèle de cluster
Gestion des applications tierces sur les appareils client
À propos des applications tierces
Installation des mises à jour du logiciel tiers
Scénario : mise à jour des logiciels tiers
Affichage des informations sur les mises à jour disponibles pour les applications tierces
Approbation et refus des mises à jour du logiciel
Synchronisation des mises à jour Windows Update avec le Serveur d'administration
Étape 1. Définir s'il faut réduire le trafic
Étape 2. Applications
Étape 3. Mise à jours des catégories
Étape 4. Mises à jour des langues
Étape 5. Sélection du compte utilisateur pour télécharger une tâche
Étape 6. Paramètres de la programmation d'une tâche
Étape 7. Définition du nom de la tâche
Étape 8. Fin de la création d'une tâche
Installation manuelle des mises à jour sur les appareils
Configuration des mises à jour Windows dans la stratégie de l'Agent d'administration
Correction des vulnérabilités dans les applications tierces
Scénario : Recherche et correction des vulnérabilités dans les logiciels tiers
À propos de la recherche et de la correction des vulnérabilités dans les applications
Consultation des informations relatives aux vulnérabilités dans les applications
Consultation des statistiques relatives aux vulnérabilités sur les appareils administrés
Recherche de vulnérabilités dans les applications
Correction des vulnérabilités dans les applications
Correction des vulnérabilités dans un réseau isolé
Scénario : Correction des vulnérabilités des logiciels tiers dans un réseau isolé
À propos de la correction des vulnérabilités des logiciels tiers dans un réseau isolé
Configuration du Serveur d'administration avec accès à Internet pour corriger les vulnérabilités dans un réseau isolé
Configuration des Serveurs d'administration isolés pour corriger les vulnérabilités d'un réseau isolé
Transmission des correctifs et installation des mises à jour dans un réseau isolé
Désactivation de la possibilité de transmettre les correctifs et d'installer les mises à jour dans un réseau isolé
Ignorer les vulnérabilités dans les applications
Sélection des correctifs utilisateur pour les vulnérabilités dans le logiciel tiers
Règles pour l'installation de la mise à jour
Groupes des applications
Utilisation du Contrôle des applications pour gérer les fichiers exécutables
Obtention et consultation d'une liste des fichiers exécutables stockés sur les appareils client
Création de catégories d'applications pour les stratégies de Kaspersky Endpoint Security for Windows
Création d'une catégorie d'applications enrichie manuellement
Création d'une catégorie d'applications incluant des fichiers exécutables provenant des appareils sélectionnés
Création d'une catégorie d'applications incluant des fichiers exécutables provenant du dossier spécifié

Ajout de fichiers exécutables liés par un événement à la catégorie d'applications
Configuration d'administration du lancement des applications sur les appareils clients
Consultation des résultats de l'analyse statique des règles de lancement des fichiers exécutables
Affichage du registre des applications
Modification de l'heure de début de l'inventaire logiciel
À propos de la gestion des clés de licence d'applications tierces
Création des groupes des applications sous licence
Gestion des clés de licence pour les groupes des applications sous licence
Inventaire des fichiers exécutables
Consultation des informations sur les fichiers exécutables
Surveillance et rapports
Scénario : Surveillance et rapports
Surveillance des indicateurs de couleur et des événements consignés dans la Console d'administration
Utilisation des rapports, des statistiques et des notifications
Utilisation des rapports
Créer le nouveau rapport
Consultation et modification des propriétés du modèle de rapport
Format de filtre étendu dans les modèles de rapport
Conversion du filtre au format étendu
Configuration du filtre étendu
Génération et affichage des rapports
Enregistrement du rapport
Création d'une tâche d'envoi du rapport
Étape 1. Sélectionner le type de tâche
Étape 2. Sélection du type de rapport
Étape 3. Actions sur un rapport
Étape 4. Sélection du compte utilisateur pour télécharger une tâche
Étape 5. Planification d'une tâche
Étape 6. Définition du nom de la tâche
Étape 7. Fin de la création d'une tâche
Utilisation des données statistiques
Configuration des paramètres de notification sur les événements
Création d'un certificat pour le serveur SMTP
Sélections d'événements
Consultation d'une sélection d'événements
Configuration d'une sélection d'événements
Création d'une sélection d'événements
Exportation d'une sélection d'événements dans le fichier texte
Suppression des événements depuis la sélection
Ajout d'applications aux exclusions sur requêtes des utilisateurs
Sélections d'appareils
Affichage d'une sélection d'appareils
Configuration d'une sélection d'appareils
Exportation des paramètres de la sélection d'appareils dans un fichier
Création d'une sélection d'appareils
Création d'une sélection d'appareils selon les paramètres importés
Suppression des appareils depuis les groupes d'administration dans la sélection

Surveillance de l'installation et de la désinstallation des applications
Événements des modules de Kaspersky Security Center
Structure des données de la description du type d'événement
Événements du Serveur d'administration
Événements critiques du Serveur d'administration
Événements liés à des erreurs de fonctionnement du Serveur d'administration
Événements d'avertissement du Serveur d'administration
Événements informatifs du Serveur d'administration
Événements de l'Agent d'administration
Événements liés aux erreurs de fonctionnement de l'Agent d'administration
Événements d'avertissement de l'Agent d'administration
Événements informatifs de l'Agent d'administration
Événements du Serveur MDM iOS
Événements liés aux erreurs de fonctionnement du Serveur MDM iOS
Événements d'avertissement du Serveur MDM iOS
Événements d'information du Serveur MDM iOS
Blocage des événements fréquents
À propos du blocage des événements fréquents
Gestion du blocage des événements fréquents
Suppression du blocage des événements fréquents
Exportation d'une liste d'événements fréquents vers un fichier
Contrôle de modification de l'état des machines virtuelles
Suivi de l'état de la protection antivirus à l'aide d'informations du registre système
Consultation et configuration des actions quand les appareils sont inactifs
Désactivation des annonces de Kaspersky
Réglage des points de distribution et des passerelles de connexion
Configuration typique des points de distribution : un bureau simple
Configuration typique des points de distribution : plusieurs petits bureaux isolés
Désignation d'un appareil administré pour servir de point de distribution
Connexion d'un appareil Linux en tant que passerelle dans la zone démilitarisée
Connexion d'un appareil sous Linux au Serveur d'administration via une passerelle de connexion
Ajout d'une passerelle de connexion dans la DMZ en tant que point de distribution
Assignation automatique des points de distribution
À propos de l'installation locale de l'Agent d'administration sur l'appareil choisi comme point de distribution
À propos de l'utilisation d'un point de distribution comme passerelle de connexion
Ajout de plages IP à la liste des plages sondées par un point de distribution
Utilisation d'un point de distribution en tant que serveur push
Autres travaux de routine
Administration des Serveurs d'administration
Création d'une hiérarchie des Serveurs d'administration : ajout d'un Serveur d'administration secondaire
Connexion au Serveur d'administration et permutation entre les Serveurs d'administration
Privilèges d'accès au Serveur d'administration et à ses objets
Conditions de connexion au Serveur d'administration via Internet
Connexion sécurisée au Serveur d'administration
Authentification du Serveur d'administration lors de la connexion de l'appareil
Authentification du Serveur d'administration lors de la connexion de la Console d'administration
Configuration de la liste d'autorisation d'adresses IP pour se connecter au Serveur d'administration

Utilisation de l'utilitaire klsclag pour fermer le port 13291
Se déconnecter du Serveur d'administration
Ajout d'un Serveur d'administration à l'arborescence de la console
Suppression d'un Serveur d'administration de l'arborescence de console
Ajout d'un Serveur d'administration virtuel à l'arborescence de la console
Changement du compte utilisateur du service du Serveur d'administration. Utilitaire klsrvswch
Modification des informations d'identification du SGBD
Modification du dossier partagé du Serveur d'administration
Résolution des problèmes avec les entrées du Serveur d'administration
Affichage et modification des paramètres du Serveur d'administration
Configuration des paramètres généraux du Serveur d'administration
Paramètres d'interface de la Console d'administration
Traitement et stockage des événements sur le Serveur d'administration
Consultation du journal des connexions au Serveur d'administration
Contrôle de l'émergence d'épidémies de virus
Restriction du trafic
Configuration des paramètres du Serveur Web
Travail avec les utilisateurs internes
Copie de sauvegarde et restauration des paramètres du Serveur d'administration
Utilisation de la capture du système de fichiers pour réduire la durée de la copie de sauvegarde
Panne de l'appareil doté du Serveur d'administration
Endommagement des paramètres du Serveur d'administration ou de la base de données
Copie de sauvegarde et restauration des données du Serveur d'administration
Tâche de sauvegarde des données du Serveur d'administration
Utilitaire de copie de sauvegarde et de restauration des données (klbackup)
Sauvegarde et restauration des données en mode interactif
Sauvegarde et restauration des données en mode silencieux
Utilisation de l'utilitaire klbackup pour basculer des appareils gérés sous l'administration d'un autre Serveur d'administration
Sauvegarde et restauration des données du Serveur d'administration avec MySQL ou MariaDB
Optimiation de la sauvegarde et de la restauration des données du Serveur d'administration
Déplacement du Serveur d'administration sur un autre appareil
Évitement des conflits entre plusieurs Serveurs d'administration
Administration des groupes d'administration
Création des groupes d'administration
Déplacement des groupes d'administration
Suppression des groupes d'administration
Création automatique de structure des groupes d'administration
Installation automatique des applications sur les appareils du groupe d'administration
Administration des appareils clients
Connexion des appareils clients au Serveur d'administration
Connexion manuelle de l'appareil client au Serveur d'administration. Utilitaire klmover
Connexion en tunnel de l'appareil client avec le Serveur d'administration
Connexion à distance au bureau de l'appareil client
Connexion aux appareils clients Windows
Connexion aux appareils clients macOS
Connexion aux appareils à l'aide du Partage du bureau Windows

Paramètres du redémarrage de l'appareil client
Audit des actions sur un appareil client distant
Vérification de la connexion de l'appareil client avec le Serveur d'administration
Vérification automatique de la connexion de l'appareil client avec le Serveur d'administration
Vérification manuelle de la connexion de l'appareil client avec le Serveur d'administration. Utilitaire klnagchk
À propos de la vérification de la durée de connexion de l'appareil avec le Serveur d'administration
Identification des appareils clients sur le Serveur d'administration
Déplacement des appareils à un groupe d'administration
Modification du Serveur d'administration pour les appareils clients
Déplacement des appareils connectés au Serveur d'administration via les passerelles de connexion vers un autre Serveur d'administration
Clusters et matrices des serveurs
Démarrage, arrêt et redémarrage à distance des appareils clients
À propos de l'utilisation de la connexion continue entre un appareil administré et le Serveur d'administration
À propos de la synchronisation forcée
À propos du gestionnaire des connexions
Envoi d'un message aux utilisateurs des appareils
Utilisation de l'application Kaspersky Security for Virtualization
Configuration de la permutation des états des appareils
Attribution des tags aux appareils et consultation des tags attribués
Attribution automatique de tags aux appareils
Consultation et configuration des tags attribués à l'appareil
Diagnostic à distance des appareils clients. Utilitaire de diagnostic à distance Kaspersky Security Center
Connexion de l'utilitaire de diagnostic à distance à l'appareil client
Génération d'un fichier dump pour une application
Activation et désactivation du traçage, téléchargement du fichier de traçage
Télécharger les paramètres de l'application
Téléchargement des journaux des événements
Téléchargement de plusieurs éléments d'information de diagnostic
Lancement du diagnostic et téléchargement des résultats
Lancement, arrêt ou relancement des applications
Appareils protégés au niveau UEFI
Paramètres de l'appareil administré
Paramètres généraux de la stratégie
Paramètres de la stratégie de l'Agent d'administration
Administration des comptes utilisateurs
Utilisation des comptes utilisateurs
Ajout d'un compte d'un utilisateur interne
Modification d'un compte d'un utilisateur interne
Modification du nombre de tentatives de saisie du mot de passe autorisées
Configuration du contrôle de l'originalité du nom de l'utilisateur interne
Ajout d'un groupe de sécurité
Ajout d'un utilisateur dans le groupe
Configuration des droits d'accès aux fonctionnalités de l'application. Restriction d'accès selon un rôle
Droits d'accès aux fonctionnalités de l'application
À propos des rôles d'utilisateurs prédéfinis
Ajout d'un rôle d'utilisateur

Attribution d'un rôle à un utilisateur ou à un groupe de sécurité
Attribution des permissions aux utilisateurs et aux groupes
Propagation des rôles d'utilisateurs sur les Serveurs d'administration secondaires
Désignation d'un utilisateur comme propriétaire de l'appareil
Diffusion des messages aux utilisateurs
Consultation de la liste des appareils mobiles de l'utilisateur
Installation du certificat pour l'utilisateur
Consultation de la liste des certificats octroyés à l'utilisateur
À propos de l'administrateur du Serveur d'administration virtuel
Installation à distance des systèmes d'exploitation et des applications
Création des images des systèmes d'exploitation
Installation d'images des systèmes d'exploitation
Configuration de l'adresse du serveur proxy KSN
Ajout des pilotes pour l'environnement de préinstallation Windows (WinPE)
Ajout des pilotes dans le paquet d'installation avec l'image du système d'exploitation
Configuration des paramètres de l'utilitaire sysprep.exe
Déploiement des systèmes d'exploitation sur les nouveaux appareils dans le réseau
Déploiement des systèmes d'exploitation sur les appareils clients
Création des paquets d'installation des applications
Établissement d'un certificat pour les paquets d'installation des applications
Installation des applications sur les appareils clients
Utilisation des révisions des objets
À propos des révisions des objets
Consultation de la Section Historique des révisions
Comparaison des révisions des objets
Définition de la durée de stockage pour les révisions de l'objet et pour les informations sur l'objet supprimé
Description de la révision de l'objet
Enregistrement de la révision de l'objet dans un fichier
Restauration des modifications
Ajout d'une description de la révision
Suppression d'objets
Suppression d'un objet
Consultation des informations relatives aux objets supprimés
Suppression permanente des objets dans la liste des objets supprimés
Administration des appareils mobiles
Scénario : déploiement de l'administration des appareils mobiles
À propos de la stratégie de groupe pour la gestion des appareils MDM iOS
Activation de l'Administration des appareils mobiles
Modification des paramètres de l'Administration des appareils mobiles
Désactivation de l'Administration des appareils mobiles
Utilisation des commandes pour les appareils mobiles
Commandes d'administration des appareils mobiles
Utilisation de Firebase Cloud Messaging
Envoi d'une commande
Consultation de l'état des commandes dans le journal des commandes
Utilisation des certificats d'appareils mobiles
Lancement de l'Assistant d'installation des certificats

Étape 1. Sélection du type de certificat
Étape 2. Séléction du type d'appareil
Étape 3. Sélection d'un utilisateur
Étape 4. Sélection de la source du certificat
Étape 5. Attribution d'un tag au certificat
Étape 6. Définition des paramètres d'édition du certificat
Étape 7. Sélection du mode de notification des utilisateurs
Étape 8. Génération du certificat
Configurer les règles d'émission des certificats
Intégration avec l'infrastructure à clé publique
Activation de la prise en charge de Kerberos Constrained Delegation
Ajout des appareils mobiles iOS à la liste des appareils administrés
Ajout des appareils mobiles Android à la liste des appareils administrés
Administration des appareils MDM iOS
Signature d'un profil MDM iOS par un certificat
Ajout du profil de configuration
Définition du profil de configuration sur l'appareil
Suppression du profil de configuration de l'appareil
Ajout d'un nouvel appareil à l'aide de la publication d'un lien vers le profil
Ajout d'un nouvel appareil via l'installation d'un profil par l'administrateur
Ajout d'un profil provisioning
Définition du profil provisioning sur l'appareil
Suppression du profil provisioning de l'appareil
Ajout d'une app administrée
Installation de l'app sur l'appareil mobile
Suppression de l'app de l'appareil
Configuration des paramètres d'itinérance sur un appareil mobile MDM iOS
Affichage des informations sur l'appareil MDM iOS
Désactivation de l'administration de l'appareil MDM iOS
Envoi de commandes sur un appareil
Contrôle de l'état d'exécution des commandes envoyées
Administration des appareils KES
Création du paquet des applications mobiles pour les appareils KES
Activation de l'authentification basée sur certificat des appareils KES
Affichage des informations sur l'appareil KES
Désactivation d'un appareil KES de l'administration
Chiffrement et protection des données
Consultation de la liste des appareils chiffrés
Consultation de la liste des événements du chiffrement
Exportation de la liste des événements du chiffrement dans le fichier texte
Formation et consultation des rapports sur le chiffrement
Transmission des clés de chiffrement entre les Serveurs d'administration
Stockages des données
Exportation de la liste des objets dans le stockage dans le fichier texte
Paquets d'installation
Principaux états des fichiers dans le stockage
Déclenchement des règles en mode Apprentissage intelligent

Consultation de la liste des détections réalisées à l'aide des règles du contrôle évolutif des anomalies
Ajout d'exclusions au départ des règles du contrôle évolutif des anomalies
Étape 1. Sélection d'une application
Étape 2. Sélection de la ou des stratégies
Étape 3. Traitement de la ou des stratégies
Quarantaine et sauvegarde
Activation de l'administration à distance des fichiers dans les stockages
Consultation des propriétés du fichier placé dans le stockage
Suppression des fichiers depuis les stockages
Restauration des fichiers depuis les stockages
Enregistrement du fichier depuis les stockages sur le disque
Analyse des fichiers en quarantaine
Menaces actives
Désinfection d'un fichier non traité
Enregistrement d'un fichier non traité sur le disque
Suppression des fichiers du dossier " Menaces actives "
Kaspersky Security Network (KSN)
À propos de KSN
Configuration de l'accès à Kaspersky Security Network
Activation et désactivation de KSN
Affichage de la Déclaration KSN acceptée
Consulter les statistiques du serveur proxy KSN
Accepter une Déclaration KSN mise à jour
Protection complémentaire avec l'utilisation de Kaspersky Security Network
Vérifier si le point de distribution fonctionne en tant que serveur proxy KSN
Basculer entre l'aide en ligne et l'aide hors ligne
Exportation des événements dans les systèmes SIEM
Configuration de l'export d'événements vers des systèmes SIEM
Conditions préalables
À propos des événements de Kaspersky Security Center
À propos de l'exportation des événements
À propos de la configuration de l'exportation d'événements dans le système SIEM
Marquage des événements pour l'export vers les systèmes SIEM au format Syslog
Marquage des événements d'une application Kaspersky pour l'exportation au format Syslog
Marquage d'événements généraux pour l'exportation au format Syslog
À propos de l'exportation des événements via le format Syslog
À propos de l'exportation des événements via les formats CEF et LEEF
Configuration de Kaspersky Security Center pour l'exportation des événements vers le système SIEM
Exportation des événements directement depuis la base de données
Exécution d'une requête SQL à l'aide de l'utilitaire klsql2
Exemple de requête SQL créée à l'aide de l'utilitaire klsql2
Consultation du nom de la base de données de Kaspersky Security Center
Consultation des résultats de l'exportation
Utilisation du service SNMP pour envoyer des statistiques à des applications tierces
Configuration du service SNMP à utiliser avec Kaspersky Security Center
Agent SNMP et identificateurs d'objets
Obtention d'un nom de compteur de chaîne à partir d'un identificateur d'objet

Valeurs des identificateurs d'objet pour SNMP
Elimination des défaillances
Fonctionnement dans le Cloud
À propos de l'utilisation dans le Cloud
Scénario : déploiement pour une utilisation dans le Cloud
Conditions indispensables pour le déploiement de Kaspersky Security Center our une utilisation dans le Cloud
Configuration matérielle requise pour le Serveur d'administration dans le Cloud
Options de licence pour l'environnement cloud
Options pour les bases de données pour travailler dans le Cloud
Utilisation de l'environnement cloud Amazon Web Services
À propos de l'utilisation de l'environnement cloud d'Amazon Web Services
Création de rôles IAM et de comptes utilisateurs IAM pour les instances Amazon EC2
Garantie des privilèges pour le fonctionnement du Serveur d'administration de Kaspersky Security Center avec AWS
Création d'un rôle IAM pour le Serveur d'administration
Création d'un compte utilisateur IAM pour utiliser Kaspersky Security Center
Création du rôle IAM pour l'installation des applications sur l'instance Amazon EC2
Utilisation avec Amazon RDS
Création d'une instance Amazon RDS
Création d'un groupe d'options pour une instance Amazon RDS
Modification du groupe d'options
Modifications des permissions pour un rôle IAM pour une instance de base de données Amazon RDS
Préparation d'un compartiment Amazon S3 pour la base de données
Migration de la base de données vers Amazon RDS
Manipulation dans l'environnement cloud Microsoft Azure
À propos de l'utilisation de Microsoft Azure
Création d'un abonnement, d'un identifiant de l'application et d'un mot de passe
Attribution d'un rôle à un identifiant de l'application Azure
Déploiement du Serveur d'administration dans Microsoft Azure et sélection d'une base de données
Utilisation d'Azure SQL
Création d'un compte du stockage Azure
Création de la base de données Azure SQL et du serveur SQL
Migration de la base de données vers Azure SQL
Travailler dans Google Cloud
Création d'un email client, d'un identifiant de projet et d'une clé privée
Utilisation de l'instance Google Cloud SQL for MySQL
Conditions indispensables pour des appareils clients dans l'environnement Cloud en vue de l'utilisation avec Kaspersky Security Center
Création des paquets d'installation requis pour configurer l'environnement cloud
Configuration de l'environnement cloud
À propos de l'Assistant de configuration pour une utilisation dans le Cloud
Étape 1. Sélection de la méthode d'activation de l'application
Étape 2. Sélection de l'environnement du Cloud
Étape 3. Autorisation dans le cloud
Étape 4. Configuration de la synchronisation avec Cloud et détermination des étapes à suivre
Étape 5. Configuration de Kaspersky Security Network dans l'environnement Cloud
Étape 6. Configuration des notifications par Email dans l'environnement Cloud
Étape 7. Création d'une configuration initiale pour la protection de l'environnement Cloud

Étape 8. Sélection de l'action si le système d'exploitation doit être redémarré pendant l'installation (pour l'environnement Cloud)
Étape 9. Réception des mises à jour par le Serveur d'administration
Contrôle de réussite de la configuration
Groupe d'appareils Cloud
Sondage du segment dans le cloud
Ajout de connexions pour le sondage des segments dans le Cloud
Suppression de connexions pour le sondage des segments dans le Cloud
Configuration de la programmation du sondage
Installation des applications sur les appareils dans le Cloud
Affichage des propriétés des appareils du Cloud
Synchronisation avec le cloud
Déploiement de Kaspersky Security Center dans Yandex.Cloud
Appendice
Possibilités complémentaires
Automatisation du fonctionnement de Kaspersky Security Center. Utilitaire klakaut
Fonctionnement avec les outils externes
Mode de clonage du disque de l'Agent d'administration
Préparation d'un appareil étalon sur lequel l'Agent d'administration est installé pour créer une image du système d'exploitation
Configuration des paramètres de réception des messages du Contrôle de l'intégrité des fichiers
Maintenance du Serveur d'administration
Accès aux serveurs DNS publics
Fenêtre Moyen de notification des utilisateurs
Fenêtre Sélection d'appareils
Fenêtre Définition du nom de l'objet créé
Section Catégories d'applications
Particularités d'utilisation de l'interface d'administration
Arborescence de la console
Comment mettre à jour les données dans l'espace de travail
Comment se déplacer dans l'arborescence de la console
Comment ouvrir la fenêtre des propriétés de l'objet dans l'espace de travail
Comment sélectionner le groupe des objets dans l'espace de travail
Comment modifier l'ensemble des colonnes dans l'espace de travail
Aide
Commandes du menu contextuel
Liste des appareils administrés. Valeur des colonnes
États des appareils, des tâches et des stratégies
Icônes des états des fichiers dans la Console d'administration
Recherche et exportation de données
Recherche d'appareils
Paramètres de recherche des appareils
Utilisation des masques dans les variables chaînes
Utilisation des expressions régulières dans la ligne de recherche
Exportation des listes depuis les fenêtres de dialogue
Paramètres des tâches
Paramètre de la tâche générale

Télécharger les mises à jour dans les paramètres de la tâche du stockage du Serveur d'administration
Paramètres de la tâche de Téléchargement des mises à jour sur les stockages des points de distribution
La tâche Recherche de vulnérabilités et de mises à jour requises est créée
Paramètres de la tâche Installation des mises à jour requises et correction des vulnérabilités
Liste globale des sous-réseaux
Ajout de sous-réseaux à la liste globale des sous-réseaux
Consultation et modification des propriétés d'un sous-réseau dans la liste globale des sous-réseaux
Utilisation de l'Agent d'administration pour Windows, Linux et macOS : comparaison
Kaspersky Security Center Web Console
Diagramme de déploiement du Serveur d'administration de Kaspersky Security Center et de Kaspersky Security Center Web Console
Ports utilisés par Kaspersky Security Center Web Console
Interface de Kaspersky Security Center Web Console
Épinglage et désépinglage de sections du menu principal
Scénario d'installation et de configuration initiale de Kaspersky Security Center Web Console
Installation
Installation de Kaspersky Security Center (installation standard)
Installation de Kaspersky Security Center Web Console
Installation de Kaspersky Security Center Web Console connecté au Serveur d'administration installé sur les nœuds du cluster de basculement
Mise à niveau de Kaspersky Security Center Web Console
Certificats pour travailler avec Kaspersky Security Center Web Console
Réémission du certificat pour Kaspersky Security Center Web Console
Remplacement de certificat pour Kaspersky Security Center Web Console
Définition des certificats pour les Serveurs d'administration de confiance dans Kaspersky Security Center Web Console
Conversion d'un certificat PFX au format PEM
Migration depuis Kaspersky Security Center Windows
Migration vers Kaspersky Security Center Cloud Console
Migration vers Kaspersky Next XDR Expert
Migration vers Kaspersky Security Center Linux
Migration vers Kaspersky Security Center Linux à l'aide de la sauvegarde des données du Serveur d'administration
Migration vers Kaspersky Security Center Linux à l'aide de l'Assistant de migration
Exportation des objets du groupe depuis Kaspersky Security Center Windows
Importation du fichier d'exportation Kaspersky Security Center Cloud Linux
Basculer les appareils administrés vers l'administration de Kaspersky Security Center Linux
Connexion et déconnexion de Kaspersky Security Center Web Console
Gestionnaire des identités et des accès dans Kaspersky Security Center Web Console
À propos du Gestionnaire des identités et des accès
Activation du Gestionnaire des identités et des accès : scénario
Configuration du Gestionnaire des identités et des accès dans Kaspersky Security Center Web Console
Enregistrement de l'application Kaspersky Industrial CyberSecurity for Networks dans Kaspersky Security Center Web Console
Durée de vie des jetons et délai d'expiration de l'autorisation pour le Gestionnaire des identités et des accès
Téléchargement et distribution des certificats IAM
Désactivation du Gestionnaire des identités et des accès
Configuration de l'authentification de domaine à l'aide des protocoles NTLM et Kerberos
Configuration du Serveur d'administration

Configuration de la connexion de Kaspersky Security Center Web Console au serveur d'administration
Configuration du journal des événements de connexion au Serveur d'administration
Configuration des paramètres d'accès Internet du Serveur d'administration
Définition du nombre d'événements maximal dans le stockage d'événements
Paramètres de connexion des appareils protégés au niveau UEFI
Création d'une hiérarchie des Serveurs d'administration : ajout d'un Serveur d'administration secondaire
Affichage de la liste des Serveurs d'administration secondaires
Suppression d'une hiérarchie des Serveurs d'administration
Maintenance du Serveur d'administration
Configuration de l'interface
Administration des Serveurs d'administration virtuels
Création d'un Serveur d'administration virtuel
Activation et désactivation d'un Serveur d'administration virtuel
Désignation d'un administrateur pour un Serveur d'administration virtuel
Modification du Serveur d'administration pour les appareils clients
Suppression d'un Serveur d'administration virtuel
Activation de la protection du compte contre les modifications non autorisées
Copie de sauvegarde et restauration des données du Serveur d'administration
Création d'une tâche de copie de sauvegarde des données
Déplacement du Serveur d'administration sur un autre appareil
Vérification de l'intégrité des modules à l'aide des utilitaires klscmodchk et integrity_checker
Configuration initiale de Kaspersky Security Center Web Console
Assistant de configuration initiale de l'application (Kaspersky Security Center Web Console)
Étape 1. Spécification des paramètres de connexion Internet
Étape 2. Téléchargement des mises à jour requises
Étape 3. Sélection des actifs à sécuriser
Étape 4. Sélection du chiffrement dans les solutions
Étape 5. Configuration de l'installation de plug-ins pour les applications administrées
Étape 6. Installation des plug-ins sélectionnés
Étape 7. Téléchargement des paquets de distribution et création des paquets d'installation
Étape 8. Configuration de Kaspersky Security Network
Étape 9. Sélection de la méthode d'activation de l'application
Étape 10. Spécification des paramètres de gestion des mises à jour tierces
Étape 11. Création de la configuration de base de la protection d'un réseau
Étape 12. Configuration des notifications par email
Étape 13. Réalisation d'un sondage réseau
Étape 14. Fin de l'assistant de démarrage rapide de l'application
Connexion d'appareils itinérants
Scénario : connexion d'appareils itinérants via une passerelle de connexion
Scénario : Connexion d'appareils itinérants via un Serveur d'administration secondaire dans la DMZ
À propos de la connexion d'appareils itinérants
Connexion d'appareils de bureau externes au Serveur d'administration
À propos des profils de connexion pour les utilisateurs itinérants
Création d'un profil de connexion pour les utilisateurs itinérants
À propos du transfert de l'Agent d'administration à d'autres Serveurs d'administration
Création d'une règle de permutation de l'Agent d'administration selon l'emplacement réseau
Assistant de déploiement de la protection

Étape 1. Démarrage de l'assistant de déploiement de la protection
Étape 2. Sélection du paquet d'installation
Étape 3. Sélection d'une méthode pour la distribution du fichier clé ou du code d'activation
Étape 4. Sélection de la version de l'Agent d'administration
Étape 5. Sélection des appareils
Étape 6. Indiquez les paramètres de la tâche d'installation à distance
Étape 7. Administration du redémarrage
Étape 8. Suppression des applications incompatibles avant l'installation
Étape 9. Déplacement des appareils vers Appareils administrés
Étape 10. Sélection des comptes pour accéder aux appareils
Étape 11. Démarrage de l'installation
Déploiement d'applications Kaspersky dans Kaspersky Security Center Web Console
Scénario : déploiement d'applications Kaspersky dans Kaspersky Security Center Web Console
Obtention des plug-ins pour les applications de Kaspersky
Téléchargement et création des paquets d'installation pour les applications de Kaspersky
Modification de la limite de la taille des données du paquet d'installation personnalisé
Téléchargement d'un paquet de distribution pour les applications Kaspersky
Vérification du bon déploiement de Kaspersky Endpoint Security
Création de paquets d'installation autonomes
Affichage de la liste des paquets d'installation autonomes
Génération des paquets d'installation personnalisés
Propagation des paquets d'installation sur les Serveurs d'administration secondaires
Installation des applications à l'aide de la tâche d'installation à distance
Installation d'une application à distance
Installation de l'application à l'aide des stratégies de groupe Active Directory
Installation des applications sur les Serveurs d'administration secondaires
Spécification des paramètres pour l'installation à distance sur les appareils Unix
Lancement et arrêt des applications Kaspersky.
Administration des appareils mobiles
Remplacement d'application de sécurité d'éditeurs tiers
Recherche d'appareils en réseau
Scénario de recherche d'appareils en réseau
Recherche d'appareils
Sondage du réseau Windows
Sondage des plages IP
Ajout et modification d'une plage IP
Sondage Zeroconf
Sondage du contrôleur de domaine
Authentification et connexion au contrôleur de domaine
Configuration d'un contrôleur de domaine Samba
Configuration des règles de rétention pour les appareils non définis
Inventaire du matériel
Ajout d'informations sur les nouveaux appareils
Configuration des critères de définition des appareils d'entreprise
Applications Kaspersky : licence et activation
Licence des applications administrées
Ajout de la clé de licence dans le stockage du Serveur d'administration

- Ajout de la clé de licence du Serveur d'administration
- Déploiement d'une clé de licence sur les appareils clients
- Diffusion automatique de la clé de licence
- Consultation des informations sur les clés de licence utilisées
- Suppression d'une clé de licence du stockage
- Révocation d'un Contrat de licence utilisateur final
- Renouvellement des licences des applications Kaspersky
- Utilisation de la place de marché de Kaspersky pour choisir les solutions d'entreprise de Kaspersky

Configuration de la protection réseau

- Scénario : Configuration de la protection réseau
- À propos des méthodes d'administration de la sécurité centrées sur l'appareil et l'utilisateur
- Configuration et diffusion des stratégies : approche centrée sur l'appareil
- Configuration et diffusion des stratégies : approche centrée sur l'utilisateur
- Paramètres de la stratégie de l'Agent d'administration
  - Comparaison des paramètres de stratégie de l'Agent d'administration par système d'exploitation
- Activation et désactivation du mode de faible consommation de ressources pour l'Agent d'administration
- Configuration manuelle d'une stratégie de Kaspersky Endpoint Security
  - Configuration de Kaspersky Security Network
  - Consultation de la liste des réseaux protégés par le Pare-feu
  - Désactivation de l'analyse des disques réseau
  - Exclusion des détails du logiciel de la mémoire du Serveur d'administration
  - Configuration de l'accès à l'interface de Kaspersky Endpoint Security for Windows sur les postes de travail
  - Enregistrement des événements de stratégie importants dans la base de données du Serveur d'administration
- Configuration manuelle d'une tâche de groupe de mise à jour de Kaspersky Endpoint Security
- Autorisation de l'accès hors ligne à l'appareil externe bloqué par le Contrôle des appareils
- Suppression d'applications ou de mises à jour logicielles à distance
- Tâches
  - À propos des tâches
  - À propos de la zone d'action des tâches
  - Création d'une tâche
  - Lancer une tâche manuellement
  - Affichage de la liste des tâches
  - Paramètre de la tâche générale
  - Exportation d'une tâche
  - Importation d'une tâche
  - Démarrage de l'Assistant de modification du mot de passe des tâches
    - Étape 1. Spécification des informations d'identification
    - Étape 2. Sélection d'une action à entreprendre
    - Étape 3. Affichage des résultats
  - Création de la tâche Exécuter des scripts à distance
    - Installation à distance d'applications sur les appareils à l'aide de la tâche Exécuter des scripts à distance
    - Configuration des notifications et de la surveillance de la tâche Exécuter des scripts à distance
    - Préparation d'une archive pour la tâche Exécuter des scripts à distance
    - Création d'un paquet d'installation sur la base d'un fichier manifeste
- Administration des appareils clients
  - Paramètres de l'appareil administré
  - Création des groupes d'administration

Ajout manuel d'appareils à un groupe d'administration
Déplacement manuel des appareils ou des clusters à un groupe d'administration
Création des règles de déplacement des appareils
Copie des règles de déplacement des appareils
Conditions d'une règle de déplacement de l'appareil
À propos des clusters et des groupes des serveurs
Propriétés d'un cluster ou d'un groupe de serveurs
Consultation et configuration des actions quand les appareils sont inactifs
À propos des états des appareils
Configuration de la permutation des états des appareils
Connexion à distance au bureau de l'appareil client
Connexion aux appareils à l'aide du Partage du bureau Windows
Sélections d'appareils
Consultation de la liste des appareils à partir d'une sélection d'appareils
Création d'une sélection d'appareils
Configuration d'une sélection d'appareils
Exportation de la liste des appareils à partir d'une sélection d'appareils
Suppression des appareils depuis les groupes d'administration dans la sélection
Tags de l'appareil
Création d'un tag de l'appareil
Renommage d'un tag de l'appareil
Suppression d'un tag de l'appareil
Affichage des appareils ayant reçu un tag
Consultation des tags attribués à un appareil
Attribution manuelle d'un tag à un appareil
Suppression d'un tag attribué à un appareil
Consultation des règles pour l'attribution automatique de tags aux appareils
Modification d'une règle d'attribution automatique de tags aux appareils
Création d'une règle d'attribution automatique de tags aux appareils
Règles d'exécution pour l'attribution automatique de tags aux appareils
Suppression d'une règle d'attribution automatique de tags aux appareils
Gestion des tags d'appareil à l'aide de l'utilitaire klscflag
Stratégies et profils de stratégie
Stratégies et profils de stratégies
À propos du cadenas et des paramètres verrouillés
Héritage des stratégies, utilisation des profils des stratégies
Hiérarchie des stratégies
Profils de stratégie dans une hiérarchie de stratégies
Comment les paramètres sont mis en œuvre sur un appareil administré
Administration des stratégies
Affichage de la liste des stratégies
Création d'une stratégie
Modification d'une stratégie
Paramètres généraux de la stratégie
Activation et désactivation d'une option d'héritage de stratégie
Copie d'une stratégie
Déplacement d'une stratégie

Exportation d'une stratégie
Importation d'une stratégie
Affichage du graphique de l'état de la distribution des stratégies
Suppression d'une stratégie
Administration des profils de stratégies
Consultation des profils d'une stratégie
Modification de la priorité d'un profil de stratégie
Création d'un profil de stratégie
Modification du profil de stratégie
Copie d'un profil de stratégie
Création d'une règle d'activation du profil de stratégie
Suppression d'un profil de stratégie
Chiffrement et protection des données
Consultation de la liste des disques chiffrés
Consultation de la liste des événements du chiffrement
Formation et consultation des rapports sur le chiffrement
Accorder l'accès à un disque chiffré en mode déconnecté
Utilisateurs et rôles d'utilisateurs
À propos des rôles d'utilisateurs
Consultation des comptes utilisateurs et des sessions
Configuration des droits d'accès aux fonctionnalités de l'application. Restriction d'accès selon un rôle
Droits d'accès aux fonctionnalités de l'application
À propos des rôles d'utilisateurs prédéfinis
Attribution de droits d'accès à des objets spécifiques
Attribution de droits d'accès aux utilisateurs et aux groupes de sécurité
Ajout d'un compte d'un utilisateur interne
Création d'un groupe de sécurité
Modification d'un compte d'un utilisateur interne
Modification d'un groupe de sécurité
Attribution d'un rôle à un utilisateur ou à un groupe de sécurité
Ajout de comptes utilisateurs à un groupe de sécurité interne
Désignation d'un utilisateur en tant que propriétaire de l'appareil
Configuration de la vérification en deux étapes pour tous les utilisateurs
À propos de la vérification en deux étapes
Activation de la vérification en deux étapes pour votre compte (Web Console)
Activation de la vérification en deux étapes pour votre compte (basée sur MMC)
Activation de la vérification en deux étapes obligatoire pour tous les utilisateurs (Web Console)
Activation de la vérification en deux étapes pour tous les utilisateurs (basée sur MMC)
Désactivation de la vérification en deux étapes d'un compte utilisateur (Web Console)
Désactivation de la vérification en deux étapes d'un compte utilisateur (basée sur MMC)
Désactivation de la vérification en deux étapes obligatoire pour tous les utilisateurs (Web Console)
Désactivation de la vérification en deux étapes obligatoire pour tous les utilisateurs (basée sur MMC)
Exclusion de comptes de la vérification en deux étapes (Web Console)
Exclusion de comptes de la vérification en deux étapes (basée sur MMC)
Modification du nom d'un émetteur de code de sécurité (Web Console)
Modification du nom d'un émetteur de code de sécurité (basé sur MMC)
Configuration de la vérification en deux étapes pour votre compte (Web Console)

Configuration de la vérification en deux étapes pour votre compte (basée sur MMC)
Création d'une nouvelle clé secrète
Interdire aux nouveaux utilisateurs de configurer eux-mêmes la vérification en deux étapes
Désignation d'un utilisateur en tant que propriétaire de l'appareil Linux après l'installation de l'Agent d'administration
Suppression d'un utilisateur ou d'un groupe de sécurité
Modification du mot de passe d'un compte utilisateur
Création d'un rôle d'utilisateur
Modification d'un rôle d'utilisateur
Modification de la zone d'action d'un rôle d'utilisateur
Suppression d'un rôle d'utilisateur
Association des profils des stratégies aux rôles
Propagation des rôles d'utilisateurs sur les Serveurs d'administration secondaires
Modification du mot de passe d'un compte
Révocation des droits d'administrateur local
Utilisation des révisions des objets
Restauration d'un objet à une révision précédente
Ajout d'une description de la révision
Affichage et enregistrement d'une révision de la stratégie
Suppression d'objets
Kaspersky Security Network (KSN)
À propos de KSN
Configuration de l'accès à KSN
Activation et désactivation de l'utilisation de KSN
Affichage de la Déclaration KSN acceptée
Accepter une Déclaration KSN mise à jour
Vérifier si le point de distribution fonctionne en tant que serveur proxy KSN
Scénario de mise à niveau de Kaspersky Security Center et des applications de sécurité administrées
Mise à jour des bases de données et des applications Kaspersky
Scénario : Mise à jour régulière des bases de données et des applications Kaspersky
À propos de la mise à jour des bases de données, des modules logiciels et des applications de Kaspersky
Créez la tâche Téléchargement des mises à jour sur le stockage du Serveur d'administration
Analyse des mises à jour récupérées
Création de la tâche de téléchargement des mises à jour sur les stockages des points de distribution
Activation et désactivation de l'installation automatique des mises à jour et des correctifs pour les modules de Kaspersky Security Center
Installation automatique des mises à jour pour Kaspersky Endpoint Security for Windows
Approbation et refus des mises à jour du logiciel
Mise à jour du Serveur d'administration
Activation et désactivation d'un modèle hors ligne de téléchargement des mises à jour
Mise à jour des bases de données et des modules logiciels de Kaspersky sur des appareils déconnectés
Sauvegarde et restauration des plug-ins Web
Réglage des points de distribution et des passerelles de connexion
Configuration typique des points de distribution : un bureau simple
Configuration typique des points de distribution : plusieurs petits bureaux isolés
À propos des points de distribution
Assignation automatique des points de distribution
Assignation manuelle des points de distribution

Modifier la liste des points de distribution pour un groupe d'administration
Synchronisation forcée
Activation d'un serveur push
Gestion des applications tierces sur les appareils client
Installation des mises à jour du logiciel tiers
Scénario : mise à jour des logiciels tiers
Installation des mises à jour du logiciel tiers
Création de la tâche Recherche de vulnérabilités et des mises à jour requises
La tâche Recherche de vulnérabilités et de mises à jour requises est créée
Création de la tâche Installer les mises à jour requises et corriger les vulnérabilités
Ajout de règles pour l'installation de la mise à jour
Création de la tâche Installation des mises à jour Windows Update
Consultation des informations sur les mises à jour du logiciel tiers disponibles
Exportation de la liste des mises à jour du logiciel disponibles vers un fichier
Approuver et refuser les mises à jour du logiciel tiers
Création de la tâche Synchronisation des mises à jour Windows Update
Mise à jour automatique des applications tierces
Correction des vulnérabilités dans les applications tierces
Scénario : Recherche et correction des vulnérabilités dans les logiciels tiers
À propos de la recherche et de la correction des vulnérabilités dans les applications
Correction des vulnérabilités dans les applications tierces
Création de la tâche Correction des vulnérabilités
Création de la tâche Installer les mises à jour requises et corriger les vulnérabilités
Ajout de règles pour l'installation de la mise à jour
Sélection des correctifs utilisateur pour les vulnérabilités dans le logiciel tiers
Consultation des informations relatives aux vulnérabilités dans les applications sur tous les appareils administrés
Consultation des informations relatives aux vulnérabilités dans les applications sur l'appareil administré sélectionné
Consultation des statistiques relatives aux vulnérabilités sur les appareils administrés
Exportation de la liste des vulnérabilités dans les applications vers un fichier
Ignorer les vulnérabilités dans les applications
Gestion des applications exécutées sur les appareils client
Utilisation du Contrôle des applications pour gérer les fichiers exécutables
Modes et catégories du Contrôle des applications
Obtention et consultation d'une liste des fichiers exécutables stockés sur les appareils client
Création d'une catégorie d'applications enrichie manuellement
Création d'une catégorie d'applications incluant des fichiers exécutables provenant des appareils sélectionnés
Création d'une catégorie d'applications incluant des fichiers exécutables provenant du dossier sélectionné
Affichage de la liste des catégories d'applications
Ajout de fichiers exécutables liés par un événement à la catégorie d'applications
Configuration du Contrôle des applications dans la stratégie Kaspersky Endpoint Security for Windows
Obtention et consultation d'une liste des applications installées sur les appareils client
Création d'un paquet d'installation d'une application tierce à partir de la base de données Kaspersky
Affichage et modification des paramètres d'un paquet d'installation d'une application tierce à partir de la base de données de Kaspersky
Paramètres d'un paquet d'installation d'une application tierce à partir de la base de données de Kaspersky
Tags de l'application
Création d'un tag de l'application

Renommage d'un tag de l'application
Attribution de tags à une application
Suppression de tags attribués à un appareil
Suppression d'un tag de l'application
Surveillance et rapports
Scénario : Surveillance et rapports
À propos des types de surveillance et de rapport
Tableau de bord et widgets
À propos du tableau de bord
Ajout de widgets au tableau de bord
Dissimulation d'un widget dans le tableau de bord
Déplacement d'un widget sur le tableau de bord
Modification de la taille et de l'apparence du widget
Modification des réglages d'un widget
À propos le mode Tableau de bord uniquement
Configuration du mode Tableau de bord uniquement
Rapports
Utilisation des rapports
Créer le nouveau rapport
Consultation et modification des propriétés du modèle de rapport
Exportation d'un rapport dans un fichier
Génération et affichage d'un rapport
Création d'une tâche d'envoi du rapport
Suppression des modèles de rapport
Événements et sélections d'événements
À propos des événements de Kaspersky Security Center
Utilisation des sélections d'événements
Création d'une sélection d'événements
Édition d'une sélection d'événements
Affichage d'une liste d'une sélection d'événements
Exportation d'une sélection d'événements
Importation d'une sélection d'événements
Affichage des détails d'un événement
Exportation des événements dans un fichier
Voir un historique d'objet à partir d'un événement
Supprimer des événements
Suppression de sélections d'événements
Définition de la condition de stockage pour un événement
Événements des modules de Kaspersky Security Center
Structure des données de la description du type d'événement
Événements du Serveur d'administration
Événements critiques du Serveur d'administration
Événements liés à des erreurs de fonctionnement du Serveur d'administration
Événements d'avertissement du Serveur d'administration
Événements informatifs du Serveur d'administration
Événements de l'Agent d'administration
Événements liés aux erreurs de fonctionnement de l'Agent d'administration

Événements d'avertissement de l'Agent d'administration
Événements informatifs de l'Agent d'administration
Événements du Serveur MDM iOS
Événements liés aux erreurs de fonctionnement du Serveur MDM iOS
Événements d'avertissement du Serveur MDM iOS
Événements d'information du Serveur MDM iOS
Blocage des événements fréquents
À propos du blocage des événements fréquents
Gestion du blocage des événements fréquents
Suppression du blocage des événements fréquents
Réception des événements de Kaspersky Security for Microsoft Exchange Servers
Notifications et états de l'appareil
Utilisation des notifications
Affichage des notifications à l'écran
À propos des états des appareils
Configuration de la permutation des états des appareils
Configuration des paramètres d'envoi des notifications
Notification relative aux événements via un fichier exécutable
Annonces de Kaspersky
À propos des annonces de Kaspersky
Spécification des paramètres d'annonces de Kaspersky
Désactivation des annonces de Kaspersky
Affichage d'informations sur les détections de menaces
Cloud Discovery
Activation de Cloud Discovery à l'aide du widget
Ajout du widget Cloud Discovery au tableau de bord
Affichage des informations sur l'utilisation des services cloud
Niveau de risque d'un service cloud
Bloquer l'accès aux services cloud indésirables
Journal d'activité de Kaspersky Security Center Web Console
Intégration entre Kaspersky Security Center et d'autres solutions
Établissement d'une connexion en arrière-plan
Exportation des événements dans les systèmes SIEM
Configuration de l'export d'événements vers des systèmes SIEM
Conditions préalables
À propos des événements de Kaspersky Security Center
À propos de l'exportation des événements
À propos de la configuration de l'exportation d'événements dans le système SIEM
Marquage des événements pour l'export vers les systèmes SIEM au format Syslog
À propos du marquage des événements pour l'exportation vers les systèmes SIEM au format Syslog
Marquage des événements d'une application Kaspersky pour l'exportation au format Syslog
Marquage d'événements généraux pour l'exportation au format Syslog
À propos de l'exportation des événements via les formats CEF et LEEF
Conversion d'événements au format CEF ou LEEF
À propos de l'exportation des événements via le format Syslog
Configuration de Kaspersky Security Center pour l'exportation des événements vers le système SIEM
Exportation des événements directement depuis la base de données

Exécution d'une requête SQL à l'aide de l'utilitaire klsql2
Exemple de requête SQL créée à l'aide de l'utilitaire klsql2
Consultation du nom de la base de données de Kaspersky Security Center
Consultation des résultats de l'exportation
Utilisation de Kaspersky Security Center Web Console dans le Cloud
Configuration pour une utilisation dans le Cloud dans Kaspersky Security Center Web Console
Étape 1. Vérification des plug-ins et des paquets d'installation requis
Étape 2. Licence de l'application
Étape 3. Sélection de l'environnement cloud et de l'autorisation
Étape 4. Sondage des segments, configuration de la synchronisation avec le Cloud et sélection des actions ultérieures
Étape 5. Sélection de l'application pour laquelle créer une stratégie et des tâches
Étape 6. Configuration de Kaspersky Security Network pour Kaspersky Security Center
Étape 7. Création d'une configuration initiale de protection
Sondage de segments du réseau via Kaspersky Security Center Web Console
Ajout de connexions pour le sondage des segments dans le Cloud
Suppression d'une connexion pour le sondage des segments dans le Cloud
Configuration de la programmation du sondage via Kaspersky Security Center Web Console
Affichage des résultats du sondage des segments dans le Cloud via Kaspersky Security Center Web Console
Affichage des propriétés des appareils du Cloud via Kaspersky Security Center Web Console
Synchronisation avec le Cloud : Configuration de la règle de déplacement
Installation à distance d'applications sur les machines virtuelles Azure
Création d'une tâche de sauvegarde des données du Serveur d'administration à l'aide d'un SGBD dans le Cloud
Diagnostic à distance des appareils clients
Ouverture de la fenêtre de diagnostic à distance
Activation et désactivation du traçage pour les applications
Téléchargement des fichiers de traçage d'une application
Suppression de fichiers de traçage
Télécharger les paramètres de l'application
Téléchargement des journaux des événements
Lancement, arrêt, relancement de l'application
Exécuter le diagnostic à distance de l'Agent d'administration de Kaspersky Security Center et télécharger les résultats
Exécution d'une application sur un appareil client
Génération d'un fichier dump pour une application
Exécution de diagnostics à distance sur un appareil client basé sur Linux
Téléchargement et suppression de fichiers de la Quarantaine et de la Sauvegarde
Téléchargement de fichiers à partir de la Quarantaine et de la Sauvegarde
Modification de la langue de l'interface de Kaspersky Security Center Web Console
Guide de référence de l'API
Meilleures pratiques pour les prestataires de services
Planification du déploiement de Kaspersky Security Center
Octroi de l'accès au Serveur d'administration via Internet
Configuration typique de Kaspersky Security Center
À propos des points de distribution
Hiérarchie des Serveurs d'administration
Serveurs d'administration virtuels
Administration des appareils mobiles dotés de Kaspersky Endpoint Security for Android
Déploiement et configuration initiale

Recommandations d'installation du Serveur d'administration
Création des comptes utilisateurs pour les services du Serveur d'administration sur un cluster haute disponibilité
Choix d'un SGBD
Indication de l'adresse du Serveur d'administration
Configuration de la protection sur le réseau d'une entreprise cliente
Configuration manuelle d'une stratégie de Kaspersky Endpoint Security
Configuration de la stratégie dans la section Protection avancée
Configuration de la stratégie dans la section Protection principale
Configuration de la stratégie dans la section Paramètres généraux
Configuration de la stratégie dans la section Configuration d'événement
Configuration manuelle d'une tâche de groupe de mise à jour de Kaspersky Endpoint Security
Configuration manuelle d'une tâche de groupe d'analyse de l'appareil de Kaspersky Endpoint Security
Planification de la tâche Recherche de vulnérabilités et des mises à jour requises
Configuration manuelle d'une tâche de groupe d'installation des mises à jour et de correction des vulnérabilités
Élaboration de la structure de groupes d'administration et désignation des points de distribution
Configuration standard d'un client MSP : un bureau
Configuration standard d'un client MSP : plusieurs petits bureaux isolés
Hiérarchie des stratégies, utilisation des profils de stratégie
Hiérarchie des stratégies
Profils de stratégie
Tâches
Règles de déplacement des appareils
Catégorisation du logiciel
À propos des applications multilocataires
Copie de sauvegarde et restauration des paramètres du Serveur d'administration
Panne de l'appareil doté du Serveur d'administration
Endommagement des paramètres du Serveur d'administration ou de la base de données
Déploiement de l'Agent d'administration et de l'application de sécurité
Déploiement initial
Configuration des paramètres des programmes d'installation
Paquets d'installation
Propriétés MSI et fichiers de transformation
Déploiement à l'aide d'outils tiers d'installation à distance d'applications
Informations générales sur les tâches d'installation à distance des applications de Kaspersky Security Center
Déploiement à l'aide du mécanisme des stratégies de groupe Microsoft Windows
Déploiement forcé à l'aide d'une tâche d'installation à distance des applications de Kaspersky Security Center
Lancement de paquets autonomes créés par Kaspersky Security Center
Possibilités d'installation manuelle des applications
Installation à distance des applications sur les appareils dotés de l'Agent d'administration
Administration du redémarrage des appareils dans la tâche d'installation à distance
Utilité de la mise à jour des bases de données dans le paquet d'installation de l'application antivirus
Remplacement de programmes de protection incompatibles d'éditeurs tiers
Suppression de l'Agent d'administration protégé par mot de passe à l'aide de l'invite de commande
Utilisation des outils d'installation à distance des applications de Kaspersky Security Center pour lancer des fichiers exécutables arbitraires sur les appareils administrés
Surveillance du déploiement
Configuration des paramètres des programmes d'installation

Informations générales
Installation en mode silencieux (avec fichier des réponses)
Installation de l'Agent d'administration en mode silencieux (sans fichier des réponses)
Configuration partielle des paramètres d'installation via setup.exe
Paramètres d'installation du Serveur d'administration
Paramètres d'installation de l'Agent d'administration
Infrastructure virtuelle
Recommandations sur la réduction de la charge sur les machines virtuelles
Prise en charge des machines virtuelles dynamiques
Prise en charge de la copie des machines virtuelles
Prise en charge de la restauration du système de fichiers pour les appareils dotés de l'Agent d'administration
À propos des profils de connexion pour les utilisateurs itinérants
Déploiement de la fonction Administration des appareils mobiles
Connexion des appareils KES au Serveur d'administration
Connexion directe des appareils au Serveur d'administration
Schéma de la connexion des appareils KES au serveur avec utilisation de la délégation forcée Kerberos (KCD)
Utilisation de Firebase Cloud Messaging
Intégration avec l'infrastructure à clé publique
Serveur Web de Kaspersky Security Center
Autres travaux de routine
Surveillance des indicateurs de couleur et des événements consignés dans la Console d'administration
Accès à distance aux appareils administrés
Utilisation de l'option " Maintenir la connexion au Serveur d'administration " pour fournir une connexion permanente entre un appareil administré et le Serveur d'administration
À propos de la vérification de la durée de connexion de l'appareil avec le Serveur d'administration
À propos de la synchronisation forcée
À propos du tunneling
Guide de dimensionnement
Présentation du manuel
Informations sur les restrictions de Kaspersky Security Center
Calculs pour les Serveurs d'administration
Calcul des ressources matérielles pour le Serveur d'administration
Configuration matérielle pour le SGBD et le Serveur d'administration
Calcul de l'espace dans la base de données
Calcul de l'espace sur le disque (avec et sans utilisation de la Gestion des vulnérabilités et des correctifs)
Calcul du nombre et de la configuration des Serveurs d'administration
Recommandations pour la connexion des machines virtuelles dynamiques à Kaspersky Security Center
Calculs pour les points de distribution et les passerelles de connexion
Exigences d'un point de distribution
Calcul de la quantité et de la configuration des points de distribution
Calcul du nombre de passerelles de connexion
Conservation des événements pour les tâches et les stratégies
Particularités et paramètres optimums de certaines tâches
Fréquence de la recherche d'appareils
Tâches de sauvegarde des données du Serveur d'administration et de maintenance du Serveur d'administration
Tâches de groupe de mise à jour de Kaspersky Endpoint Security
Tâche d'inventaire

Informations sur la charge sur le réseau entre le Serveur d'administration et les appareils protégés
Débit du trafic lors de l'exécution de divers scénarios
Débit moyen du trafic par 24 heures
Contacter le Support Technique
Façons de profiter du support technique
Support technique via le Kaspersky CompanyAccount
Obtention des fichiers de vidage du Serveur d'administration
Sources d'informations sur l'application
Glossaire
Administrateur de Kaspersky Security Center
Administrateur du client
Administrateur du prestataire de services
Administration centralisée des applications
Agent d'administration
Agent d'authentification
Appareil KES
Appareil MDM iOS
Appareil protégé au niveau UEFI
Appareils administrés
Application incompatible
Attaque MITM
AWS Application Program Interface (AWS API)
Base antivirus
Boutique des apps
Certificat du Serveur d'administration
Certificat général
Clé active
Clé d'accès AWS IAM
Clé de licence complémentaire (ou de réserve)
Client du Serveur d'administration (Appareil client)
Cloud
Cloud Discovery
Console d'administration
Console de gestion AWS
Domaine multicast
Dossier de sauvegarde
Durée de validité de la licence
État de la protection
État de la protection du réseau
Fichier clé
Gestion des identités et des accès (IAM)
Gestion directe des applications
Groupe d'administration
Groupe des applications sous licence
Guide de renforcement
HTTPS
Image machine Amazon (AMI)

Importance de l'événement
Installation à distance
Installation forcée
Installation locale
Installation manuelle
Instance Amazon EC2
JavaScript
Kaspersky Private Security Network (KPSN)
Kaspersky Security Center System Health Validator (SHV)
Kaspersky Security Network (KSN)
Mise à jour
Mise à jour disponible
Mise à niveau de Kaspersky Security Center
Nagent léger (LWNGT)
Niveau d'importance du correctif
Paquet d'installation
Paramètres de l'application
Paramètres de la tâche
Passerelle des connexions
Plug-in d'administration
Point de distribution
Poste de travail de l'administrateur
Prestataire de services de protection antivirus
Privilèges d'administrateur
Profil de configuration
Profil MDM iOS
Profil provisioning
Propagation de virus
Propriétaire de l'appareil
Protection antivirus du réseau
Reconnaissance de l'emplacement réseau (NLA)
Restauration
Restauration des données du Serveur d'administration
Rôle IAM
Sauvegarde des données du Serveur d'administration
Serveur d'administration
Serveur d'administration domestique
Serveur d'administration virtuel
Serveur des appareils mobiles
Serveur MDM iOS
Serveur Web de Kaspersky Security Center
Serveurs de mise à jour de Kaspersky
Services de mise à jour du serveur Windows (WSUS)
Seuil d'activité de virus
SSL
Stockage d'événements
Stratégie

Tâche
Tâche de groupe
Tâche locale
Tâches pour l'ensemble d'appareils
Utilisateur de Kaspersky Security Center
Utilisateur IAM
Utilisateurs internes
Vulnérabilité
Zone démilitarisée (DMZ)
Informations sur le code tiers
Avis de marques déposées
Problèmes connus

Système d'aide de Kaspersky Security Center 15.1

Nouveautés Découvrez les nouveautés de la version la plus récente d'application.	**Configuration de la protection réseau** Gérer la sécurité de l'organisation.
Configurations logicielle et matérielle Découvrez quels sont les systèmes d'exploitation et les versions de l'application prises en charge.	**Applications Kaspersky. Mise à jour des bases de données et des modules d'application** Maintenir la fiabilité du système de protection.
Déploiement et configuration initiale Planifiez l'utilisation des ressources, installez le Serveur d'administration, Installer l'Agent d'administration et les applications de sécurité sur les appareils clients et organisez les appareils en groupes d'administration.	**Surveillance et rapports** Consultez votre infrastructure, les états de la protection et les statistiques. Gérez l'accès aux services cloud à l'aide de Cloud Discovery.
Recherche d'appareils en réseau Découvrez les appareils nouveaux et existants sur le réseau de votre organisation.	**Remplacement d'application de sécurité d'éditeurs tiers** Découvrez comment supprimer les applications incompatibles.
Applications Kaspersky. Déploiement centralisé Déploiement d'applications Kaspersky.	**Réglage des points de distribution et des passerelles de connexion** Configurer les points de distribution.
Mise à jour de Kaspersky Security Center depuis une version antérieure Mise à niveau de Kaspersky Security Center 15.1 depuis une version antérieure.	**Meilleures pratiques pour les prestataires de services (Aide en ligne uniquement)** Découvrez les recommandations sur le déploiement, la configuration et l'utilisation de l'application, ainsi que les solutions pour résoudre les problèmes les plus fréquents qui surviennent pendant le fonctionnement de l'application.
Applications Kaspersky. Licence et activation Activez les applications Kaspersky en quelques étapes simples.	**Guide de dimensionnement (Aide en ligne uniquement)** Pour obtenir les performances optimales dans les conditions d'utilisation les plus diverses, tenez compte du nombre d'appareils dans le réseau, de la topologie du réseau et des fonctions de Kaspersky Security Center dont vous avez besoin.
Exportation des événements dans les systèmes SIEM Configurez l'exportation d'événements vers des systèmes SIEM pour analyse.	**Gestion des vulnérabilités et des correctifs** Recherchez et corrigez les vulnérabilités dans les logiciels tiers.
Fonctionnement dans le Cloud Déployez Kaspersky Security Center dans le Cloud : Amazon Web Services™, Microsoft Azure™, Google™ Cloud Platform.	**Foire aux questions (en anglais uniquement)** Trouvez des instructions sur la façon de résoudre les problèmes courants.
Guide de démarrage rapide de Kaspersky Endpoint Security for Business Premiers pas avec Kaspersky Endpoint Security for Business : installez et configurez cette solution. Vous pouvez également consulter la comparaison des fonctionnalités de Kaspersky Security Center pour choisir la manière la plus appropriée d'administrer la sécurité du réseau.	

Nouveautés

Kaspersky Security Center 15.1 Mise à jour 2

Kaspersky Security Center 15.1 Mise à jour 2 est axé sur la correction des problèmes signalés par les utilisateurs et l'équipe de test :

- Les tâches sont désormais exécutées correctement pour la portée des appareils administrés basés sur Linux définie par l'importation d'un fichier TXT.
- Désormais, lorsqu'une application Kaspersky est installée à l'aide d'une tâche d'installation à distance créée sur un Serveur d'administration virtuel, les paquets d'installation sont transmis aux appareils administrés à l'aide des outils du système d'exploitation uniquement via le point de distribution géré par ce Serveur d'administration virtuel.
- Résolution d'un problème où un Serveur d'administration secondaire ne parvenait pas à se reconnecter au Serveur d'administration principal après la rotation du certificat du Serveur secondaire.
- Résolution de problèmes affectant les connexions TLS.
- Résolution d'un problème qui provoquait plusieurs erreurs « typecast incorrect » lors de la connexion de l'utilisateur.
- Kaspersky Security Center envoie désormais correctement les notifications d'événements par email.
- Correction d'un problème empêchant l'ajout du dossier *Mises à jour* à la copie de sauvegarde lors de la mise à niveau de Kaspersky Security Center de la version 14.2 vers la version 15.1.
- La date d'expiration de la licence de l'application Kaspersky s'affiche désormais correctement dans Kaspersky Security Center Web Console.
- Les commandes **Géolocaliser l'appareil mobile** et **Obtenir l'historique des données de localisation de l'appareil** fonctionnent désormais correctement.
- Correction d'un problème qui empêchait la suppression automatique des paquets d'installation contenant des certificats mobiles 1 heure après leur téléchargement ou 24 heures après leur dernière utilisation.
- Le profil de stratégie activé par un tag particulier est désormais correctement appliqué aux appareils dont les descriptions contiennent ce tag.
- Correction d'un problème qui entraînait l'affichage de messages d'erreur de la base de données PostgreSQL dans le journal des événements.
- L'exclusion d'un compte de la vérification en deux étapes fonctionne désormais correctement.
- Correction d'un problème qui empêchait la déconnexion de Kaspersky Security Center Web Console lorsque l'authentification de domaine était activée avec Identity and Access Manager.
- Désormais, lors de la mise à jour d'un plug-in d'administration Internet, un clic sur le lien correspondant à la version requise du plug-in lance le téléchargement.

- Problèmes corrigés dans les rapports :
  - Lorsque vous créez une tâche de diffusion des rapports sur les menaces et sur les mises à jour, et que vous définissez la planification de la tâche sur **Chaque mois**, les rapports sont correctement complétés avec les données.
  - Dans le modèle *Rapport sur l'état des modules de l'application*, les filtres par nom de module sont correctement appliqués.
  - Il est désormais possible de filtrer le *Rapport sur le déploiement de la protection* pour afficher uniquement les appareils sur lesquels les applications Kaspersky ne sont pas installées. Cela permet de visualiser le nombre d'appareils sur lesquels les applications doivent être installées.
- Le widget **Cloud Discovery** s'affiche correctement, que vous disposiez ou non du droit **Exécuter** dans la zone **Fonctionnalités générales : fonctionnalités de base**.
- Amélioration des performances des procédures stockées et des opérations sur les bases de données.
- Correction d'un problème où les certificats expirés liés à des utilisateurs inexistants provoquaient l'arrêt du processus de renouvellement pour tous les utilisateurs.
- Résolution des problèmes liés au traitement des certificats.
- Après la mise à niveau de Kaspersky Security Center de la version 14.2 vers la version 15.1, le téléchargement d'un paquet d'installation autonome à partir d'un Serveur d'administration virtuel secondaire dans la Console d'administration fonctionne désormais correctement.
- Correction d'un problème dans Kaspersky Security Center Web Console où, lors de l'activation de l'utilisation de Kaspersky Security Network (KSN) dans la stratégie de l'application Kaspersky, l'acceptation de la Déclaration de KSN n'était pas disponible pour les applications suivantes : Kaspersky Endpoint Security for Linux version 12.2 ou version antérieure, Kaspersky Industrial CyberSecurity for Linux Nodes version 1.5 ou version antérieure, Kaspersky Security for Virtualization Light Agent versions 6.0 et 6.1, Kaspersky Embedded Systems Security for Linux version 3.3 et Kaspersky Security for Windows Server version 11.0.1.897.
- Correction d'un problème où un profil de stratégie n'était pas appliqué aux appareils Linux inclus dans un groupe de domaine Active Directory.
- Correction d'un problème qui se produisait lors des tentatives de connexion à partir de plusieurs Serveurs d'administration secondaires de deuxième niveau vers le Serveur d'administration principal.

Kaspersky Security Center 15.1

Kaspersky Security Center 15.1 comprend plusieurs nouvelles fonctionnalités et améliorations :

- Cloud Discovery. Cette nouvelle fonctionnalité vous permet de surveiller les tentatives d'utilisation des services cloud sur les appareils administrés fonctionnant sous Windows et de bloquer l'accès aux services cloud que vous considérez comme indésirable. Cette fonctionnalité est disponible uniquement dans Kaspersky Security Center Web Console.
- Le sondage du contrôleur de domaine vous permet désormais de sonder un contrôleur de domaine Samba via un point de distribution basé sur Linux. Des améliorations supplémentaires ont été apportées pour permettre le sondage de grands domaines.
- Diagnostics à distance améliorés des appareils administrés basés sur Linux.

- Inventaire matériel étendu des appareils macOS. L'Agent d'administration sur l'appareil macOS envoie l'adresse MAC et le numéro de série de l'appareil au Serveur d'administration.
- Vous pouvez maintenant vérifier la connexion à un système SIEM.
- La longueur maximale du mot de passe pour un utilisateur interne a été portée à 256 caractères.
- Lors de la migration de Kaspersky Security Center Windows vers Kaspersky Security Center Linux, vous pouvez désormais faire passer les appareils administrés sous la gestion de Kaspersky Security Center Linux en restaurant le certificat et la clé privée du Serveur d'administration à partir d'une copie de sauvegarde.
- Lorsque vous exécutez l'outil de nettoyage ou l'utilitaire klmover pour supprimer un Agent d'administration protégé par mot de passe, vous êtes invité à saisir le mot de passe de désinstallation.
- La mise à niveau de Kaspersky Security for Windows Server vers Kaspersky Endpoint Security for Windows ne requiert plus le redémarrage de l'appareil cible.
- Un utilisateur peut être désigné en tant que propriétaire de l'appareil pendant ou après l'installation de l'Agent d'administration sur un appareil client sous Linux.
- Vous pouvez désormais recevoir un rapport sur l'installation à distance lorsque vous installez un logiciel sur les appareils administrés via des scripts personnalisés.
- Lorsque vous exécutez plusieurs scripts personnalisés sur un appareil administré, vous pouvez attribuer une priorité à chaque script pour définir l'ordre d'exécution. Les scripts seront exécutés du plus prioritaire vers le moins prioritaire.
- Audit de stratégie étendu. Vous pouvez désormais consulter le contenu d'une révision de la stratégie et enregistrer la révision de la stratégie dans un fichier. Actuellement, ces fonctionnalités ne sont disponibles que pour la stratégie du Serveur d'administration et la stratégie de l'Agent d'administration.
- Améliorations de l'expérience utilisateur, y compris :
  - Personnalisation du menu principal en épinglant des sections de Kaspersky Security Center Web Console pour un accès rapide depuis la section **Épinglé**.
  - Utilisation des tableaux optimisée. La vue par défaut de chaque tableau contient désormais les colonnes les plus fréquemment utilisées. En outre, vous pouvez désormais sélectionner tous les éléments de la page en cours ou de l'ensemble du tableau, ainsi que trier les éléments de l'ensemble du tableau.
  - Amélioration de la configuration de la diffusion des rapports. Vous pouvez désormais définir jusqu'à 20 adresses email auxquelles envoyer le rapport, ainsi que la planification de la remise du rapport.
- Vous pouvez révoquer les droits d'administrateur local des comptes sur les appareils administrés basés sur Linux. Cela vous offre un niveau de contrôle supplémentaire sur les comptes utilisateurs. Par exemple, vous pouvez révoquer les droits d'administrateur local à l'issue d'une attribution à usage unique.
- Vous pouvez modifier le mot de passe du compte local sur les appareils administrés basés sur Linux, par exemple, si un utilisateur oublie le mot de passe du compte local ou pour effectuer une modification planifiée du mot de passe.
- La sous-section **Gestion des certificats utilisateurs** permet d'indiquer les certificats racines à installer. Ces certificats peuvent servir, par exemple, à vérifier l'authenticité de sites Internet ou de serveurs Internet.
- Le Rapport d'attaques réseau inclut désormais l'adresse MAC et le port de l'appareil attaquant.

- Nouvelle option permettant de forcer un utilisateur interne à modifier un mot de passe lors de la prochaine tentative de connexion à Kaspersky Security Center Web Console.
- La licence commerciale n'est plus vérifiée lorsque vous exportez des événements vers un système SIEM au format CEF ou LEEF.
- Lorsque vous passez d'une application Kaspersky à une autre et que votre application actuelle est protégée par mot de passe, vous pouvez maintenant indiquer le mot de passe de désinstallation dans la tâche d'installation à distance.
- Exchange ActiveSync n'est plus pris en charge.

Kaspersky Security Center 14.2

Kaspersky Security Center 14.2 comprend plusieurs nouvelles fonctionnalités et améliorations :

- Un nouveau guide de sécurisation renforcée a été publié. Nous vous recommandons vivement de lire attentivement le guide et de suivre les recommandations de sécurité pour configurer Kaspersky Security Center et votre infrastructure réseau.

  Veuillez également installer la dernière mise à jour de Kaspersky Security Center. Cette mise à jour inclut des fonctionnalités de protection de l'infrastructure telles que la vérification en deux étapes des comptes utilisateurs et d'autres améliorations.
- L'accès aux serveurs de Kaspersky est désormais vérifié automatiquement. Si l'accès aux serveurs via le système DNS n'est pas possible, l'application utilise le DNS public.
- Les privilèges des utilisateurs sur le Serveur d'administration virtuel peuvent être configurés à tout moment, indépendamment du Serveur d'administration principal. Vous pouvez également attribuer aux utilisateurs du Serveur primaire les droits d'administration d'un Serveur virtuel.
- Kaspersky Security Center prend désormais en charge les SGBD suivants :
  - PostgreSQL 13.x
  - PostgreSQL 14.x
  - Postgres Pro 13.x (toutes les éditions)
  - Postgres Pro 14.x (toutes les éditions)
  - MariaDB 10.1, 10.4, 10.5
- Vous pouvez utiliser Kaspersky Security Center Web Console pour exporter des stratégies et des tâches dans un fichier, puis importer les stratégies et les tâches dans Kaspersky Security Center Windows ou Kaspersky Security Center Linux.
- L'option **Ne pas utiliser de serveur proxy** a été supprimée des tâches suivantes :
  - *Téléchargement des mises à jour sur le stockage du Serveur d'administration*
  - *Téléchargement des mises à jour sur les stockages des points de distribution*

- Pour protéger les appareils clients dans l'environnement cloud, vous pouvez déployer Kaspersky Endpoint Security for Windows au lieu de Kaspersky Security for Windows Server. Cette fonctionnalité est désormais disponible après la sortie de Kaspersky Endpoint Security 12.0 for Windows.

- L'utilisation des clés de chiffrement est désormais limitée par les droits d'accès à la zone fonctionnelle **Fonctions générales** : **Gestion des clés de chiffrement**. Les utilisateurs de Kaspersky Security Center peuvent désormais exporter les clés de chiffrement s'ils disposent du droit **Lire**, et peuvent importer des clés de chiffrement s'ils disposent du droit **Écrire**.

Kaspersky Security Center 14

Kaspersky Security Center 14 comprend plusieurs nouvelles fonctionnalités et améliorations :

- Vous pouvez installer des mises à jour et corriger les vulnérabilités de logiciels tiers (à l'exception des logiciels Microsoft) dans un réseau isolé. Ces réseaux incluent les Serveurs d'administration et les appareils administrés qui n'ont pas accès à Internet. Pour corriger les vulnérabilités de ce type de réseau, vous devez télécharger les mises à jour requises à l'aide d'un Serveur d'administration avec accès à Internet, puis transmettre les correctifs aux Serveurs d'administration isolés.

- Des profils de connexion pour les utilisateurs absents du bureau ont été ajoutés pour les appareils macOS. En utilisant des profils de connexion, vous pouvez configurer les règles pour que les Agents d'administration sur les appareils macOS se connectent au même Serveur d'administration ou à des Serveurs d'administration différents, selon l'emplacement de l'appareil.

- L'Agent d'administration peut maintenant être installé sur les appareils exécutant Microsoft Windows 10 IoT Enterprise.

- Dans **Rapport sur les menaces**, vous pouvez maintenant filtrer la liste des menaces pour afficher uniquement les menaces qui ont été détectées par Cloud Sandbox.

- Kaspersky Security Center prend désormais en charge Kaspersky Industrial CyberSecurity for Linux Nodes 1.3 en tant qu'application administrée.

Kaspersky Security Center Web Console comprend plusieurs nouvelles fonctionnalités et améliorations :

- Vous pouvez configurer le mode Tableau de bord uniquement pour les employés qui ne gèrent pas le réseau mais qui souhaitent consulter les statistiques de protection du réseau dans Kaspersky Security Center (par exemple, un cadre supérieur). Lorsqu'un utilisateur a activé ce mode, l'utilisateur voit uniquement un tableau de bord avec un ensemble prédéfini de widgets. Ainsi, il peut suivre les statistiques indiquées dans les widgets, par exemple, l'état de protection de tous les appareils administrés, le nombre de menaces récemment détectées ou la liste des menaces les plus fréquentes sur le réseau.

- Kaspersky Security Center Web Console prend maintenant en charge Kaspersky Security for iOS en tant qu'application de sécurité.

- Dans les propriétés de la tâche, vous pouvez indiquer si vous souhaitez ou non appliquer la tâche aux sous-groupes et aux Serveurs d'administration secondaires (y compris virtuels).

- Kaspersky Security Center prend désormais en charge Kaspersky Industrial CyberSecurity for Linux Nodes 1.3 en tant qu'application administrée.

Kaspersky Security Center 13.2

Kaspersky Security Center 13.2 comprend plusieurs nouvelles fonctionnalités et améliorations :

- Il est possible d'installer le Serveur d'administration, la Console d'administration, Kaspersky Security Center 13.2 Web Console et l'Agent d'administration sur les nouveaux systèmes d'exploitation suivants (voir la configuration logicielle requise pour obtenir plus de détails) :
  - Microsoft Windows 11
  - Microsoft Windows 10 21H2 (mise à jour octobre 2021)
  - Windows Server 2022
- Vous pouvez utiliser MySQL 8.0 comme base de données.
- Vous pouvez déployer Kaspersky Security Center sur un cluster de basculement Kaspersky Security Center pour assurer la haute disponibilité de Kaspersky Security Center.
- Kaspersky Security Center gère désormais les adresses IPv6 ainsi que les adresses IPv4. Le Serveur d'administration peut interroger les réseaux qui ont des appareils avec des adresses IPv6.

Kaspersky Security Center 13.2 Web Console comprend plusieurs nouvelles fonctionnalités et améliorations :

- Vous pouvez maintenant gérer des appareils mobiles exécutant Android via Kaspersky Security Center 13.2 Web Console.
- La place de marché Kaspersky est disponible en tant que nouvelle section de menu : vous pouvez rechercher l'application Kaspersky via Kaspersky Security Center 13.2 Web Console.
- Kaspersky Security Center prend désormais en charge les applications Kaspersky suivantes :
  - Kaspersky Endpoint Detection and Response Optimum 2.0
  - Kaspersky Sandbox 2.0
  - Kaspersky Industrial CyberSecurity for Networks 3.1

Kaspersky Security Center 13.1

Kaspersky Security Center 13.1 comprend plusieurs nouvelles fonctionnalités et améliorations :

- L'intégration avec les systèmes SIEM a été améliorée. Vous pouvez désormais exporter des événements dans les systèmes SIEM via le canal chiffré (TLS). La fonctionnalité est disponible pour Kaspersky Security Center Web Console et la Console d'administration basée sur MMC.
- Vous pouvez désormais recevoir des correctifs pour le Serveur d'administration en tant que paquet de distribution, que vous pouvez utiliser pour les futures mises à jour vers les versions ultérieures.
- Une nouvelle section baptisée, **Alertes**, a été ajoutée pour Kaspersky Endpoint Detection and Response Optimum à Kaspersky Security Center 13.1 Web Console. Plusieurs nouveaux widgets sont également ajoutés pour travailler avec les menaces détectées par Kaspersky Endpoint Detection and Response Optimum.

- Dans Kaspersky Security Center 13.1 Web Console, vous pouvez désormais recevoir les notifications relatives aux licences sur le point d'expirer pour les applications de Kaspersky.

- Le temps de réponse de Kaspersky Security Center 13.1 Web Console a été réduit.

Kaspersky Security Center 13

Les fonctionnalités suivantes ont été ajoutées à Kaspersky Security Center 13 Web Console :

- Mise en œuvre de la vérification en deux étapes. Vous pouvez activer la vérification en deux étapes pour réduire le risque d'accès non autorisé à Kaspersky Security Center 13 Web Console.

- Mise en œuvre de l'authentification de domaine à l'aide des protocoles NTLM et Kerberos (authentification unique). La fonctionnalité d'authentification unique permet à un utilisateur Windows d'activer l'authentification sécurisée dans Kaspersky Security Center 13 Web Console sans avoir à saisir à nouveau le mot de passe sur le réseau de l'entreprise.

- Vous pouvez maintenant configurer un plug-in pour qu'il fonctionne avec Kaspersky Managed Detection and Response. Vous pouvez utiliser cette intégration pour visualiser les incidents et administrer les postes de travail.

- Vous pouvez désormais spécifier les paramètres de Kaspersky Security Center 13 Web Console dans l'assistant d'installation du Serveur d'administration.

- Des notifications sont affichées concernant les nouvelles versions de mises à jour et de correctifs. Vous pouvez installer une mise à jour immédiatement ou ultérieurement à tout moment. Vous pouvez maintenant installer des correctifs pour le Serveur d'administration via Kaspersky Security Center 13 Web Console.

- Lorsque vous travaillez avec des tableaux, vous pouvez désormais spécifier l'ordre et la largeur des colonnes, trier les données et spécifier la taille de la page.

- Vous pouvez maintenant ouvrir n'importe quel rapport en cliquant sur son nom.

- Kaspersky Security Center 13 Web Console est désormais disponible en coréen.

- Une nouvelle section, les annonces de Kaspersky, est disponible dans le menu **Surveillance et rapports**. Cette section vous tient informé en fournissant des informations relatives à votre version de Kaspersky Security Center et aux applications administrées installées sur les appareils administrés. Kaspersky Security Center met régulièrement à jour les informations de cette section en supprimant les annonces obsolètes et en ajoutant de nouvelles informations. Cependant, vous pouvez désactiver les annonces de Kaspersky si vous le souhaitez.

- Implémentation d'une authentification supplémentaire après la modification des paramètres d'un compte utilisateur. Vous pouvez activer la protection d'un compte utilisateur contre les modifications non autorisées. Si cette option est activée, la modification des paramètres du compte utilisateur nécessite l'autorisation d'un utilisateur disposant de droits de modification.

Les fonctionnalités suivantes ont été ajoutées à Kaspersky Security Center 13 :

- Mise en œuvre de la vérification en deux étapes. Vous pouvez activer la vérification en deux étapes pour réduire le risque d'accès non autorisé à la Console d'administration. Si cette option est activée, la modification des paramètres du compte utilisateur nécessite l'autorisation de l'utilisateur disposant des droits de modification. Vous pouvez désormais activer ou désactiver la vérification en deux étapes pour les appareils KES.

- Vous pouvez envoyer des messages au Serveur d'administration via le protocole HTTP. Un guide de référence et une bibliothèque Python pour travailler avec l'OpenAPI du Serveur d'administration sont désormais disponibles.

- Vous pouvez émettre un certificat de réserve destiné à être utilisé dans les profils MDM iOS, afin de garantir une commutation transparente des appareils iOS administrés après l'expiration du certificat du Serveur MDM iOS.

- Le dossier des applications mutualisées n'est plus affiché dans la Console d'administration.

À propos de Kaspersky Security Center

Cette section contient des informations sur l'objectif de Kaspersky Security Center, ses principales fonctionnalités et ses principaux modules, ainsi que sur les moyens d'acheter Kaspersky Security Center.

Les informations de Online Help peuvent différer de celles reprises dans les documents qui accompagnent l'application. Elles sont également à jour. Pour accéder à l'aide en ligne, cliquez sur les liens qui apparaissent dans l'interface de l'application ou dans la documentation. Le contenu de l'aide en ligne peut être mis à jour sans préavis. Vous pouvez basculer entre l'aide en ligne et l'aide hors ligne, si nécessaire.

L'application Kaspersky Security Center a été développée pour centraliser les principales tâches d'administration et assurer le système de protection du réseau d'une entreprise. L'application offre à l'administrateur l'accès aux informations détaillées sur le niveau de sécurité du réseau de l'entreprise et permet de configurer tous les modules de protection élaborée à partir des applications de Kaspersky.

L'application Kaspersky Security Center est un outil destiné aux administrateurs de réseaux d'entreprise et aux responsables de la sécurité.

A l'aide de Kaspersky Security Center, vous pouvez :

- Former une hiérarchie des Serveurs d'administration pour administrer le réseau de votre propre entreprise, ainsi que les réseaux des postes distants ou des entreprises clientes.

  Une *entreprise cliente* est une entreprise dont la protection antivirus est assurée par le fournisseur de service.

- Former une hiérarchie des groupes d'administration pour administrer les appareils (les appareils clients et les machines virtuelles) comme un ensemble.

- Administrer le système de protection antivirus formé à partir des applications de Kaspersky.

- Créer de manière centralisée les images des systèmes d'exploitation et les déployer sur les appareils clients par le réseau, ainsi qu'exécuter l'installation à distance des applications de Kaspersky et d'autres éditeurs de logiciels.

- Gérer à distance les applications de Kaspersky et d'autres éditeurs installées sur les appareils clients : Installer les mises à jour, rechercher et fermer les vulnérabilités.

- Déployer de manière centralisée les clés de licence des applications de Kaspersky sur les appareils clients, suivre l'utilisation des clés et prolonger la durée de validité des licences.

- Recevoir les statistiques et les rapports de fonctionnement des applications et des appareils.

- Recevoir les notifications pour les événements critiques survenus pendant le fonctionnement des applications de Kaspersky.

- Administrer les appareils mobiles.

- Administrer le chiffrement des informations enregistrées sur les disques durs et les disques amovibles, et administrer l'accès des utilisateurs aux données chiffrées.

- Faire l'inventaire du matériel connecté au réseau de l'entreprise.
- Travailler de façon centralisée avec les objets placés en quarantaine ou dans la Sauvegarde par les applications de sécurité, ainsi qu'avec les fichiers dont le traitement est différé par les applications de sécurité.

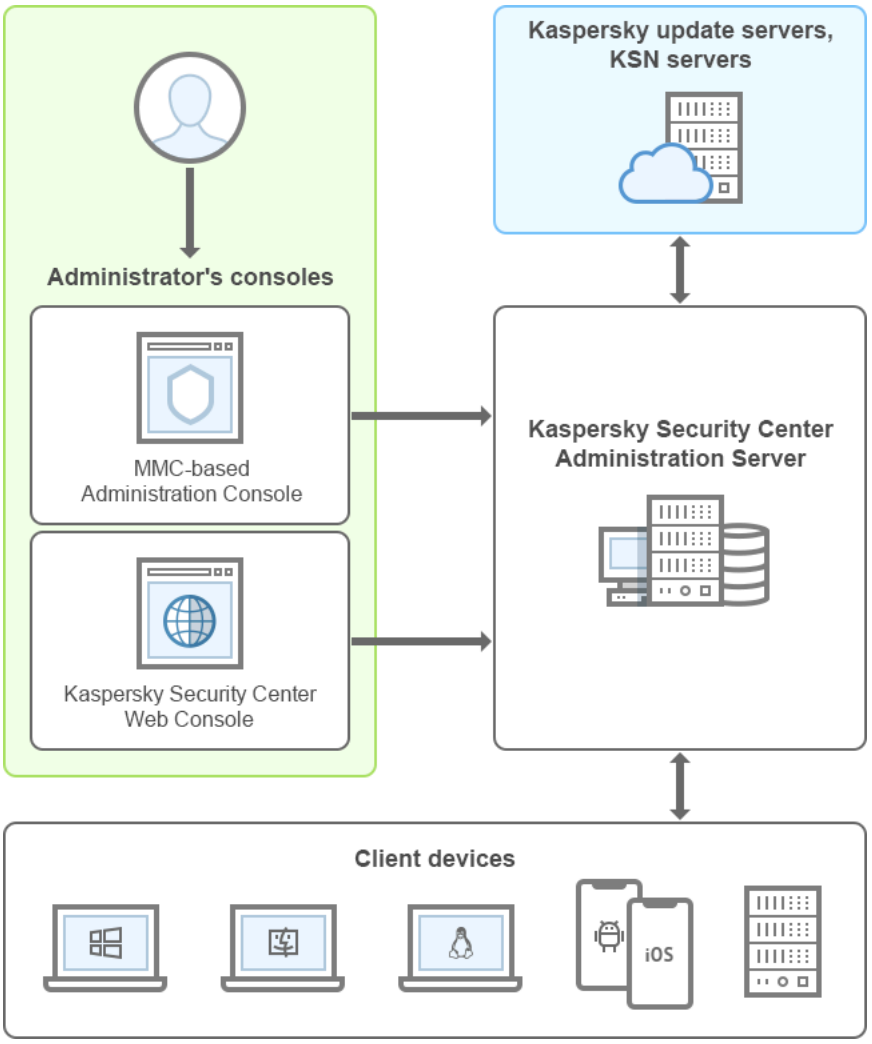
Vous pouvez acheter Kaspersky Security Center via Kaspersky (par exemple, à l'adresse https://www.kaspersky.fr) ou par l'intermédiaire d'entreprises partenaires.

Si vous achetez Kaspersky Security Center via Kaspersky, vous pouvez copier l'application depuis notre site Internet. Les informations indispensables à l'activation de l'application vous seront envoyées par email après le traitement de votre paiement.

La fonctionnalité de mises à jour (y compris la fourniture de mises à jour des signatures antivirus et des bases de code), ainsi que la fonctionnalité KSN peuvent ne pas être disponibles dans le logiciel aux États-Unis.

Architecture

Cette section décrit les modules de Kaspersky Security Center et leur interaction.



Architecture Kaspersky Security Center

L'application Kaspersky Security Center inclut les modules principaux suivants :

- *Console d'administration* (ci-après aussi *Console*). Fournit l'interface utilisateur nécessaire pour les services administratifs du Serveur d'administration et de l'Agent d'administration. La Console d'administration est conçue comme une extension de la console de gestion Microsoft (MMC). La Console d'administration permet de se connecter au Serveur d'administration distant par Internet.

- *Kaspersky Security Center Web Console*. Ceci offre une interface Web pour créer et maintenir le système de protection du réseau d'une entreprise cliente administrée par le Kaspersky Security Center.

- *Serveur d'administration de Kaspersky Security Center* (également désigné le *Serveur*). Est un entrepôt centralisé d'informations sur les applications installées sur le réseau local de la société et un outil efficace d'administration de ces applications.

- *Serveurs de mise à jour de Kaspersky*. Serveurs HTTP(S) Kaspersky sur lesquels les applications de Kaspersky récupèrent les mises à jour des bases de données et des modules de l'application.

- *Serveurs KSN*. Serveurs contenant la base de données de Kaspersky, qui reçoit des informations mises à niveau sur la réputation des fichiers, des ressources Internet et du logiciel. L'utilisation des données de Kaspersky Security Network assure une vitesse de réaction plus élevée des applications de Kaspersky sur les menaces, augmente l'efficacité de fonctionnement de certains modules de protection, ainsi que diminue la possibilité des faux positifs.

- *Appareils Client*. Appareils de l'entreprise cliente protégés à l'aide de Kaspersky Security Center. L'une des applications de sécurité Kaspersky doit être installée sur chacun des appareils à protéger.

Configurations logicielle et matérielle

- Configuration requise pour le Serveur d'administration
- Configuration requise pour Web Console
- Configuration requise pour les serveurs mobiles
- Configuration requise pour la Console d'administration
- Configuration requise pour l'Agent d'administration

Configuration requise pour le Serveur d'administration

Configuration matérielle minimale requise :

- Processeur cadencé à 1 GHz ou plus. La cadence minimale du processeur avec un système d'exploitation 64 bits est de 1,4 GHz.

- Mémoire vive : 4 Go.

- Espace disque disponible : 2 GO. Lors de l'utilisation de la fonctionnalité de Gestion des vulnérabilités et des correctifs, le volume d'espace libre sur le disque doit être au moins de 100 Go.

Pour le déploiement dans des environnements Cloud, les exigences du Serveur d'administration et du serveur de base de données sont les mêmes que celles du Serveur d'administration physique (en fonction du nombre d'appareils que vous souhaitez administrer).

Configuration logicielle :

- Microsoft® Data Access Components (MDAC) 2.8
- Microsoft Windows® DAC 6.0
- Microsoft Windows Installer 4.5

Les systèmes d'exploitation suivants sont pris en charge :

- Windows Server 2012 R2 Standard/Datacenter/Essentials/Foundation/Server Core 64 bits
- Windows Server 2016 Standard/Datacenter/Essentials/Server Core (option d'installation) (LTSB) 64 bits
- Windows Server 2019 Standard/Datacenter/Core 64 bits
- Windows Server 2022 Standard/Datacenter/Core 64 bits
- Windows Server 2025 Standard/Datacenter/Core 64 bits
- Windows Storage Server 2019 64 bits

Plateformes de virtualisation prises en charge :

- VMware vSphere 6.7
- VMware vSphere 7.0
- VMware vSphere 8.0
- Microsoft Hyper-V Server 2019 64 bits
- Microsoft Hyper-V Server 2022 64 bits
- Citrix XenServer 7.1 LTSR
- Citrix XenServer 8.x
- Parallels Desktop 18
- Oracle VM VirtualBox 7.x

Les serveurs de base de données suivants sont pris en charge (peuvent être installés sur un autre appareil) :

- Microsoft SQL Server 2016 (toutes les versions) 64 bits
- Microsoft SQL Server 2017 (toutes les versions) sur Windows/Linux 64 bits
- Microsoft SQL Server 2019 (toutes les versions) sur Windows/Linux 64 bits (nécessite des actions supplémentaires)

- Microsoft SQL Server 2022 (toutes les versions) sur Windows/Linux 64 bits
- MySQL 5.7 Community 32 bits / 64 bits
- MySQL Standard Edition 8.0 (version 8.0.20 et supérieure) 32 bits / 64 bits
- MySQL Enterprise Edition 8.0 (version 8.0.20 et supérieures) 32 bits / 64 bits
- MariaDB 10.5 (version 10.5.27 et versions ultérieures) 32 bits / 64 bits
- MariaDB Galera Cluster 10.3 32 bits / 64 bits avec moteur de stockage InnoDB
- PostgreSQL 13.x 64 bits
- PostgreSQL 14.x 64 bits
- PostgreSQL 15.x 64 bits
- Postgres Pro 13.x Windows/Linux 64 bits
- Postgres Pro 14.x Windows/Linux 64 bits

Pour en savoir plus et connaître les limitations, reportez-vous dans la section suivante : Sélection d'un SGBD.

SIEM et autres systèmes de gestion de l'information :

- HP (Micro Focus) ArcSight ESM 7.0
- IBM QRadar 7.3
- Splunk 7.1

Configuration requise pour Web Console

Serveur de Kaspersky Security Center Web Console

Configuration matérielle minimale requise :

- Processeur : quadricœur, cadencé à 2,5 GHz
- Mémoire vive : 8 Go
- Espace disque disponible : 40 Go

Conditions requises pour les certificats du Serveur d'administration :

- Algorithme de signature de certificat SHA-2
- Longueur de clé minimale : 2 048

Si vous devez réémettre le certificat, consultez la Base de connaissances de Kaspersky Security Center.

Systèmes d'exploitation pris en charge par le serveur de Kaspersky Security Center Web Console

Systèmes d'exploitation. Microsoft Windows (version 64 bits uniquement)	Windows Server 2012 R2 Standard/Datacenter/Foundation/Essentials/Server Core Windows Server 2016 Standard/Datacenter/Essentials/Server Core (option d'installation) (LTSB) Windows Server 2019 Standard/Datacenter/Core Windows Server 2022 Standard/Datacenter/Core Windows Server 2025 Standard/Datacenter/Core Windows Storage Server 2019
Plateformes de virtualisation	VMware vSphere 6.7 VMware vSphere 7.0 VMware vSphere 8.0 Citrix XenServer 7.1 LTSR Citrix XenServer 8.x Parallels Desktop 18 Oracle VM VirtualBox 7.x

Appareils Client

Pour un client, l'utilisation de Kaspersky Security Center Web Console requiert seulement un navigateur.

La résolution minimale de l'écran est de 1 366 x 768 pixels.

La configuration logicielle et matérielle requise de l'appareil correspond à celle du navigateur sur lequel vous utiliserez Kaspersky Security Center Web Console.

Navigateurs :

- Google Chrome 128.0.6613.120 ou version ultérieure
- Microsoft Edge 128.0.2739.67 ou version ultérieure
- Safari 17.6 sur macOS
- "Yandex" Browser 24.7.3.1081 ou version ultérieure
- Mozilla Firefox Extended Support Release 115.14.0 ou version ultérieure

Configuration requise pour les serveurs mobiles

Serveur iOS Mobile Device Management (MDM iOS)

Configuration matérielle :

- Processeur cadencé à 1 GHz ou plus. La cadence minimale du processeur avec un système d'exploitation 64 bits est de 1,4 GHz.
- Mémoire vive : 2 Go.
- Espace disque disponible : 2 Go.

Configuration logicielle : système d'exploitation Microsoft Windows (la version du système d'exploitation prise en charge est fixée par les exigences du Serveur d'administration).

Configuration requise pour la Console d'administration

Configuration matérielle :

- Processeur cadencé à 1 GHz ou plus. La cadence minimale du processeur avec un système d'exploitation 64 bits est de 1,4 GHz.
- Mémoire RAM : 512 Mo.
- Espace disque disponible : 1 Go.

Configuration logicielle :

- Système d'exploitation Microsoft Windows (la version du système d'exploitation prise en charge est déterminée par les exigences du Serveur d'administration) :
  - Windows Server 2012 R2 Standard/Datacenter/Foundation/Essentials 64 bits
  - Windows Server 2016 Standard/Datacenter/Essentials (LTSB) 64 bits
  - Windows Server 2019 Standard/Datacenter 64 bits
  - Windows Server 2022 Standard/Datacenter 64 bits
  - Windows Server 2025 Standard/Datacenter/Core 64 bits
  - Windows Storage Server 2019 64 bits
- Microsoft Management Console version 2.0
- Microsoft Windows Installer 4.5
- Microsoft Internet Explorer 11.0 exécuté sur :
  - Microsoft Windows Server 2012 R2
  - Microsoft Windows Server 2016
  - Microsoft Windows Server 2019
  - Microsoft Windows Storage Server 2019
- Microsoft Edge fonctionnant sous Microsoft Windows Server 2022 Standard

Configuration requise pour l'Agent d'administration

Configuration matérielle minimale requise :

- Processeur cadencé à 1 GHz ou plus. La cadence minimale du processeur avec un système d'exploitation 64 bits est de 1,4 GHz.
- Mémoire RAM : 512 Mo.
- Espace disque disponible : 1 Go.

Configuration logicielle requise pour les appareils Linux : l'interprète Perl version 5.10 ou supérieure doit être installé.

Systèmes d'exploitation. Microsoft Windows	Windows Embedded POSReady 2009 avec le dernier Service Pack 32 bits Windows Embedded 7 Standard avec Service Pack 1 32 bits / 64 bits Windows Embedded 8.1 Industry Pro 32 bits / 64 bits Windows 10 Entreprise 2015 LTSB 32 bits / 64 bits Windows 10 Entreprise 2016 LTSB 32 bits / 64 bits Windows 10 IoT Entreprise 2015 LTSB 32 bits / 64 bits Windows 10 IoT Entreprise 2016 LTSB 32 bits / 64 bits Windows 10 Entreprise 2019 LTSC 32 bits / 64 bits Windows 10 IoT Entreprise version 1703 32 bits / 64 bits Windows 10 IoT Entreprise version 1709 32 bits / 64 bits Windows 10 IoT Entreprise version 1803 32 bits / 64 bits Windows 10 IoT Entreprise version 1809 32 bits / 64 bits Windows 10 20H2 IoT Entreprise 32 bits / 64 bits Windows 10 21H2 IoT Entreprise 32 bits / 64 bits Windows 10 IoT Entreprise 32 bits / 64 bits Windows 10 IoT Entreprise version 1909 32 bits / 64 bits Windows 10 IoT Entreprise LTSC 2021 32 bits / 64 bits Windows 10 IoT Entreprise version 1607 32 bits / 64 bits Windows 10 TH1 Famille/Pro pour les Stations de travail/Entreprise/Éducation 32 bits / 64 bits Windows 10 TH2 Famille/Pro pour les Stations de travail/Entreprise/Éducation 32 bits / 64 bits Windows 10 RS1 Famille/Pro pour les Stations de travail/Entreprise/Éducation 32 bits / 64 bits Windows 10 RS2 Famille/Pro pour les Stations de travail/Entreprise/Éducation 32 bits / 64 bits Windows 10 RS3 Famille/Pro pour les Stations de travail/Entreprise/Éducation 32 bits / 64 bits Windows 10 RS4 Famille/Pro pour les Stations de travail/Entreprise/Éducation 32 bits / 64 bits Windows 10 RS5 Famille/Pro pour les Stations de travail/Entreprise/Éducation 32 bits / 64 bits Windows 10 RS6 Famille/Pro pour les Stations de travail/Entreprise/Éducation 32 bits / 64 bits Windows 10 19H1 Famille/Pro pour les Stations de travail/Entreprise/Éducation 32 bits / 64 bits Windows 10 19H2 Famille/Pro pour les Stations de travail/Entreprise/Éducation 32 bits / 64 bits Windows 10 20H1 Famille/Pro pour les Stations de travail/Entreprise/Éducation 32 bits / 64 bits Windows 10 20H2 Famille/Pro pour les Stations de travail/Entreprise/Éducation 32 bits / 64 bits Windows 10 21H1 Famille/Pro pour les Stations de travail/Entreprise/Éducation 32 bits / 64 bits Windows 10 21H2 Famille/Pro pour les Stations de travail/Entreprise/Éducation 32 bits / 64 bits Windows 10 22H2 Famille/Pro pour les Stations de travail/Entreprise/Éducation 32 bits / 64 bits Windows 11 Famille/Pro pour Stations de travail/Entreprise/Éducation 64 bits Windows 11 22H2 Famille/Pro pour Stations de travail/Entreprise/Éducation 64 bits Windows 11 23H2 Famille/Pro pour Stations de travail/Entreprise/Éducation 64 bits Windows 11 24H2 Famille/Pro pour Stations de travail/Entreprise/Éducation 64 bits Windows 8 Pro/Entreprise 32 bits / 64 bits Windows 8.1 Pro/Entreprise 32 bits / 64 bits Windows 7 Home/Pro/Enterprise/Ultimate avec Service Pack 1 32 bits / 64 bits Microsoft Windows XP Professionnel avec Service Pack 2 32 bits/64 bits (uniquement pris en charge par l'Agent d'administration version 10.5.1781, que vous pouvez demander via le Support technique) Windows XP Professional avec Service Pack 3 et versions ultérieures 32 bits (pris en charge par l'Agent d'administration version 14.0.0.20023) Windows XP Professional for Embedded Systems avec Service Pack 3 32 bits (pris en charge par l'Agent d'administration version 14.0.0.20023) Windows MultiPoint Server 2011 Standard/Premium 64 bits Windows Server 2003 SP1 32 bits/64 bits (uniquement pris en charge par l'Agent d'administration version 10.5.1781) Windows Server 2003 SP2 Standard/Enterprise 32 bits/64 bits (uniquement pris en charge par l'Agent d'administration version 10.5.1781) Windows Server 2003 R2 Standard/Enterprise avec SP2 32 bits/64 bits (uniquement pris en charge par l'Agent d'administration version 10.5.1781) Windows Server 2008 Standard/Enterprise/Datacenter/Foundation avec Service Pack 2 32 bits / 64 bits Microsoft Windows Server 2008 R2 Standard/Datacenter/Enterprise/Foundation avec Service Pack 1 et versions ultérieures 64 bits Windows Server 2012 Standard/Datacenter/Essentials/Foundation/Server Core 64 bits

	Windows Server 2012 R2 Standard/Datacenter/Essentials/Foundation/Server Core 64 bits Windows Server 2016 Standard/Datacenter/Essentials/Server Core (option d'installation) (LTSB) 64 bits Windows Server 2019 Standard/Datacenter/Core 64 bits Windows Server 2019 RS5 Standard/Essentials 64 bits Windows Server 2022 Standard/Datacenter/Core 64 bits Windows Server 2022 21H2 Standard/Datacenter 64 bits Windows Server 2025 Standard/Datacenter/Core 64 bits Windows Storage Server 2019 64 bits
Systèmes d'exploitation. Linux	Debian GNU/Linux 10.x (Buster) 32 bits / 64 bits Debian GNU/Linux 11.x (Bullseye) 32 bits / 64 bits Debian GNU/Linux 12 (Bookworm) 32 bits / 64 bits Ubuntu Server 18.04 LTS (Bionic Beaver) 64 bits Ubuntu Server 20.04 LTS (Focal Fossa) 64 bits Ubuntu Server 22.04 LTS (Jammy Jellyfish) 64 bits Ubuntu Server 22.04 LTS ARM 64 bits Ubuntu Server 24.04 LTS (Noble Numbat) 64 bits CentOS 6.7 et versions ultérieures 32 bits CentOS 6.x (jusqu'à 6.6) 32 bits / 64 bits CentOS 7.x 64 bits CentOS Stream 8 64 bits CentOS Stream 9 64 bits CentOS Stream 9 ARM 64 bits Red Hat Enterprise Linux Server 6.x 32 bits / 64 bits Red Hat Enterprise Linux Server 7.x 64 bits Red Hat Enterprise Linux Server 8.x 64 bits Red Hat Enterprise Linux Server 9.x 64 bits SUSE Linux Enterprise Server 12 (Tous Service Packs) 64 bits SUSE Linux Enterprise Server 15 (Tous Service Packs) 64 bits SUSE Linux Enterprise Server 15 (Tous Service Packs) ARM 64 bits openSUSE 15 64 bits EulerOS 2.0 SP10 64 bits EulerOS 2.0 SP10 ARM 64 bits Astra Linux Special Edition RUSB.10015-01 (mise à jour opérationnelle 1.5) 64 bits Astra Linux Special Edition RUSB.10015-01 (mise à jour opérationnelle 1.6) 64 bits Astra Linux Special Edition RUSB.10015-16 (version 1) (mise à jour opérationnelle 1.6) 64 bits Astra Linux Special Edition RUSB.10015-17 (mise à jour opérationnelle 1.7.3) 64 bits Astra Linux Special Edition RUSB.10015-01 (mise à jour opérationnelle 1.7) 64 bits Astra Linux Special Edition RUSB.10015-01 (mise à jour opérationnelle 1.8) 64 bits Astra Linux Special Edition RUSB.10015-37 (mise à jour opérationnelle 7.7) 64 bits Astra Linux Special Edition RUSB.10152-02 (mise à jour opérationnelle 4.7) ARM 64 bits Astra Linux Common Edition (mise à jour opérationnelle 2.12) 64 bits ALT Workstation 10.1 64 bits ALT Server 10.1 64 bits ALT Education 10.1 64 bits ALT SP Server 10 32 bits/64 bits ALT SP Server 10 ARM 64 bits ALT SP Workstation 10 32 bits/64 bits ALT SP Workstation 10 ARM 64 bits ALT Server 10 64 bits ALT Server 10 ARM 64 bits ALT Workstation 10 32 bits / 64 bits ALT 8 SP Workstation (8.4) ARM 64 bits ALT 8 SP Server (8.4) ARM 64 bits ALT 8 SP Server (LKNV.11100-01) 32 bits / 64 bits ALT 8 SP Server (LKNV.11100-02) 32 bits / 64 bits ALT 8 SP Server (LKNV.11100-03) 32 bits/64 bits

	ALT 8 SP Workstation (LKNV.11100-01) 32 bits / 64 bits ALT 8 SP Workstation (LKNV.11100-02) 32 bits / 64 bits ALT 8 SP Workstation (LKNV.11100-03) 32 bits / 64 bits Mageia 4 32 bits Oracle Linux 7 64 bits Oracle Linux 8 64 bits Oracle Linux 9 64 bits Linux Mint 20.x 64 bits Linux Mint 21.1 et versions ultérieures 64 bits AlterOS 7.5 et suivant 64 bits GosLinux IC6/7.17 64 bits GosLinux IC6/7.2 64 bits SberOS 3.3.1 64 bits Platform V SberLinux OS Server (SLO) 8.8 64 bits Platform V SberLinux OS Server (SLO) 8.9.2 64 bits RED OS 7.3 ARM 64 bits RED OS 7.3 Server 64 bits RED OS 7.3 Édition certifiée 64 bits RED OS 8 Édition certifiée 64 bits ROSA Enterprise Linux Server 7.9 64 bits ROSA Enterprise Linux Desktop 7.9 64 bits ROSA COBALT 7.9 64 bits ROSA CHROME 12 64 bits AlmaLinux 8 et versions ultérieures 64 bits AlmaLinux 9 et versions ultérieures 64 bits Rocky Linux 8 et versions ultérieures 64 bits Rocky Linux 9 et versions ultérieures 64 bits Atlant, version Alcyone, version 2022.02 64 bits MSVSPHERE 9.2 SERVER 64 bits MSVSPHERE 9.2 ARM 64 bits SynthesisM Server 8.6 64 bits SynthesisM Client 8.6 64 bits OSnova 2.10 64 bits Kylin 10 64 bits EMIAS 1.0 64 bits Amazon Linux 2 64 bits MosOS 15.4 Arbat 64 bits OS MES (Moscow Electronic School) 64 bits
Systèmes d'exploitation. macOS	Pour obtenir la liste des systèmes d'exploitation pris en charge, consultez l'aide de Kaspersky Endpoint Security for Mac.

L'agent d'administration prend également en charge l'architecture Apple Silicon (M1), ainsi qu'Intel.

Plateformes de virtualisation prises en charge :

- VMware vSphere 6.7
- VMware vSphere 7.0
- VMware vSphere 8.0
- Parallels Desktop 18
- Oracle VM VirtualBox 7.x

- Citrix XenServer 7.1 LTSR
- Citrix XenServer 8.x
- Machine virtuelle basée sur le noyau (tous les systèmes d'exploitation Linux pris en charge par l'Agent d'administration)

Sur les appareils exécutant Windows 10 version RS4 ou RS5, Kaspersky Security Center peut être dans l'incapacité de détecter certaines vulnérabilités dans les dossiers où la sensibilité à la casse est activée.

Avant l'installation de l'Agent d'administration sur les appareils fonctionnant sous Windows 7, Windows Server 2008 ou Windows Server 2008 R2, assurez-vous que vous avez installé la mise à jour de sécurité KB3063858 pour le système d'exploitation Windows (Mise à jour de sécurité pour Windows 7 (KB3063858), Mise à jour de sécurité pour Windows 7 pour les systèmes x64 (KB3063858), Mise à jour de sécurité pour Windows Server 2008 (KB3063858), Mise à jour de sécurité pour Windows Server 2008 Édition x64 (KB3063858), Mise à jour de sécurité pour Windows Server 2008 R2 Édition x64 (KB3063858)).

Dans Microsoft Windows XP, l'Agent d'administration peut ne pas effectuer certaines opérations correctement.

Vous pouvez installer ou mettre à jour l'Agent d'administration pour Windows XP sous Microsoft Windows XP uniquement. Les éditions de Microsoft Windows XP prises en charge et les versions correspondantes de l'Agent d'Administration sont répertoriées dans la liste des systèmes d'exploitation pris en charge. Vous pouvez télécharger la version requise de l'Agent d'Administration pour Microsoft Windows XP depuis cette page.

Nous vous recommandons d'installer la même version de l'Agent d'administration que Kaspersky Security Center.

Kaspersky Security Center prend entièrement en charge l'Agent d'administration de la même version ou d'une version plus récente.

L'Agent d'administration pour macOS est fourni avec l'application de sécurité Kaspersky pour ce système d'exploitation.

Compatible avec les applications et les solutions de Kaspersky

Kaspersky Security Center prend en charge le déploiement et l'administration centralisés de toutes les applications et solutions Kaspersky actuellement prises en charge. Le tableau ci-dessous indique les applications et solutions Kaspersky prises en charge par la Console d'administration basée sur MMC et Kaspersky Security Center Web Console. Pour connaître les versions des applications et des solutions, reportez-vous à la page Internet de Product Support Lifecycle.

Nom de l'application ou de la solution Kaspersky	Pris en charge par la Console d'administration basée sur MMC	Pris en charge par Kaspersky Security Center Web Console
Pour les postes de travail :		
Kaspersky Endpoint Security for Windows	✓	✓
Kaspersky Endpoint Security for Linux	✓	✓
Kaspersky Endpoint Security for Linux Elbrus Edition	✓	✓
Kaspersky Endpoint Security for Mac	✓	✓
Kaspersky Endpoint Agent	✓	✓
Kaspersky Embedded Systems Security for Windows	✓	✓
Kaspersky Embedded Systems Security for Linux	—	✓
Pour les solutions industrielles		
Kaspersky Industrial CyberSecurity for Nodes	✓	✓
Kaspersky Industrial CyberSecurity for Linux Nodes	✓	✓
Kaspersky Industrial CyberSecurity for Networks (le déploiement centralisé n'est pas pris en charge)	✓	✓
Pour les appareils mobiles		
Kaspersky Endpoint Security for Android	✓	✓
Kaspersky Security for iOS	—	✓
Pour les serveurs de fichier		
Kaspersky Security for Windows Server	✓	✓
Kaspersky Endpoint Security for Windows	✓	✓
Kaspersky Endpoint Security for Linux	✓	✓
Pour les environnements virtuels		
Kaspersky Security for Virtualization Light Agent	✓	✓
Kaspersky Security for Virtualization Agentless	✓	—
Pour les serveurs de messagerie et de collaboration		
Kaspersky Security for Microsoft Exchange Servers	✓	—
Pour la détection d'attaques ciblées		
Kaspersky Sandbox Server	—	✓
Kaspersky Endpoint Detection and Response Optimum	—	✓
Kaspersky Managed Detection and Response	—	✓
Pour les appareils KasperskyOS		
Kaspersky IoT Secure Gateway	—	✓
Kaspersky Thin Client	—	✓
Bases de réputation		
Kaspersky Private Security Network	—	✓

Licence et fonctionnalités de Kaspersky Security Center 15.1

Kaspersky Security Center nécessite une licence pour certaines de ses fonctionnalités.

Le tableau ci-dessous indique les fonctionnalités de Kaspersky Security Center couvertes par les différentes licences.

Pour activer les fonctionnalités de Kaspersky Security Center, vous devez activer le Serveur d'administration en ajoutant une clé de licence du Serveur d'administration.

Vous devez ajouter manuellement une clé de licence pour chaque Serveur d'administration.

Licence et fonctionnalité de Kaspersky Security Center

Fonctionnalités de Kaspersky Security Center	Gestion des vulnérabilités et des correctifs de Kaspersky	Kaspersky Endpoint Security for Business Select	Kaspersky Endpoint Security for Business Advanced	Kaspersky Total Security for Business	Kaspersky Hybrid Cloud Security Standard	Kaspersky Hybrid Cloud Security Enterprise	Kaspersky EDR Optimum
Évaluation des vulnérabilités	✓	✓	✓	✓	✓	✓	✓
Gestion des correctifs	✓	–	✓	✓	–	✓	✓
Restriction d'accès selon un rôle	✓	✓	✓	✓	✓	✓	✓
Installation des systèmes d'exploitation et des applications	✓	–	✓	✓	–	✓	✓
Administration des appareils mobiles (c'est-à-dire la gestion des appareils iOS et Android des utilisateurs)	✓	✓	✓	✓	–	–	✓
Configurer l'environnement cloud pour travailler dans des environnements cloud, comme AWS, Microsoft Azure ou Google Cloud	–	–	–	–	✓	✓	–
Exportation des événements dans les systèmes SIEM : Syslog	✓	✓	✓	✓	✓	✓	✓
Exportation des événements dans les systèmes SIEM : QRadar par IBM et ArcSight par Micro Focus	✓	✓	✓	✓	✓	✓	✓

À propos de la compatibilité des modules de Kaspersky Security Center

Le tableau ci-dessous contient les informations sur la compatibilité des modules de Kaspersky Security Center.

Compatibilité des modules de Kaspersky Security Center

Module	Compatible avec
Serveur d'administration de Kaspersky Security Center 15.1	• Console d'administration de Kaspersky Security Center 15.1. • Kaspersky Security Center 15.1 Web Console. • L'Agent d'administration de Kaspersky Security Center des versions suivantes : 15.4, 15.1, 15, 14.2 et 14.
Kaspersky Security Center 15.1 Web Console	Le Serveur d'administration de Kaspersky Security Center des versions suivantes : 15.1 et 14.2.
Serveur d'administration principal de Kaspersky Security Center 15.1	Serveurs d'administration secondaires : • Kaspersky Security Center 14 Windows. • Kaspersky Security Center 14.2 Windows. • Kaspersky Security Center 15.1 Windows. • Kaspersky Security Center 14.2 Linux. • Kaspersky Security Center 15 Linux. • Kaspersky Security Center 15.1 Linux.
Serveur d'administration secondaire de Kaspersky Security Center 15.1	Serveurs d'administration principaux : • Kaspersky Security Center 14 Windows. • Kaspersky Security Center 14.2 Windows. • Kaspersky Security Center 15.1 Windows. • Kaspersky Security Center 14.2 Linux. • Kaspersky Security Center 15 Linux. • Kaspersky Security Center 15.1 Linux.

Nous vous recommandons d'utiliser la dernière version du Serveur d'administration de Kaspersky Security Center et de Kaspersky Security Center Web Console. Dans le cas contraire, les fonctionnalités de Kaspersky Security Center peuvent être limitées. Vous pouvez installer et mettre à niveau le Serveur d'administration de Kaspersky Security Center et Kaspersky Security Center Web Console indépendamment. Dans ce cas, vous devez vous assurer que la version de Kaspersky Security Center Web Console installée est compatible avec la version du Serveur d'administration auquel vous vous connectez.

Si vous disposez de la dernière version de Kaspersky Security Center Web Console et de la version précédente de Kaspersky Security Center et qu'une erreur se produit lors de l'authentification du domaine, le texte de l'erreur contient un message par défaut.

Comparaison de Kaspersky Security Center : basé sur Windows et basé sur Linux

Kaspersky propose Kaspersky Security Center en tant que solution sur site pour deux plates-formes : Windows et Linux. Dans la solution Windows, vous installez le Serveur d'administration sur un appareil Windows et la solution Linux dispose de la version du Serveur d'administration conçue pour être installée sur un appareil Linux. Cette aide en ligne contient des informations sur Kaspersky Security Center Windows. Pour obtenir des informations détaillées sur la solution Linux, consultez l'aide en ligne de Kaspersky Security Center Linux.

Le tableau ci-dessous permet de comparer les principales fonctionnalités de Kaspersky Security Center en tant que solution Windows et en tant que solution Linux.

Fonctionnalité ou propriété	Kaspersky Security Center	
	Solution basée sur Windows	Solution basée sur Linux
Serveur d'administration		
Emplacement du système de gestion de base de données (SGBD)	Sur site	Sur site (Microsoft SQL n'est pas pris en charge)
Système d'exploitation sur lequel installer le Serveur d'administration	Windows	Linux
Hiérarchie des Serveurs d'administration	✓	✓
Prise en charge des Serveurs d'administration virtuels	✓	✓
Utilisation de SNMP pour envoyer les statistiques du Serveur d'administration à des applications tierces	✓	* À mettre en œuvre en 2026
Serveur Web pour la publication des paquets d'installation et d'autres fichiers	✓	✓
Installation du Serveur d'administration sur un cluster de basculement Windows Server	✓	—
Console d'administration		
Type de Console d'administration	Basé sur MMC et sur le Web	Basé sur le Web
Système d'exploitation sur lequel installer la Console d'administration Web	Windows ou Linux	Linux
Se connecter à la console à l'aide de l'authentification de domaine	✓	✓ (l'authentification unique n'est pas prise en charge pour les versions 15.1–15.4 incluses)
Gestion des appareils clients et des groupes d'administration		
Nombre maximal d'appareils administrés (par Serveur d'administration)	100 000	50 000 (avec PostgreSQL et Postgres Pro)
Sondage réseau	✓	✓ À partir de la version 16, les contrôleurs de domaine FreeIPA et ALD Pro sont pris en charge)
Protection des appareils administrés Windows, macOS et Linux	✓	✓
Protection des appareils mobiles	✓ Administration de base des appareils mobiles	✓ MDM et utilisation de la fonctionnalité d'Administration de Kaspersky Secure Mobility (sous licence)
Gestion de la protection des machines virtuelles	✓	✓
Protection de l'infrastructure Cloud publique	✓	—
Connexion à distance au bureau d'un appareil client	✓	✓ (à partir de la version 15.3)
Chiffrement et protection des données	✓	✓ (sur les appareils administrés sous Windows équipés de Kaspersky Endpoint Security for Windows ou Kaspersky Endpoint Security for Mac)
Déploiement du cluster de basculement Kaspersky Security Center	✓	✓
Prise en charge des clusters et des matrices de serveurs dans les groupes d'administration	✓	✓
Hiérarchie du groupe d'administration	✓	✓
Ajout d'une passerelle de connexion dans la DMZ en tant que point de distribution	✓ (Console d'administration basée sur MMC)	* À mettre en œuvre en 2026

Fonctionnalité ou propriété	Kaspersky Security Center	
	Solution basée sur Windows	Solution basée sur Linux
Travail avec les utilisateurs		
Création et gestion des comptes utilisateurs	✓	✓
Gestion des applications Kaspersky		
Stratégies d'application	✓	✓
Tâches pour les applications Kaspersky	✓	✓
Kaspersky Security Network	✓	✓
Proxy KSN	✓	✓
Kaspersky Private Security Network	✓	✓
Déploiement centralisé des clés de licence pour les applications Kaspersky	✓	✓
Diagnostic à distance des appareils clients	✓	✓
Mise à jour automatique des applications Kaspersky	✓	✓
Prise en charge du Contrôle évolutif des anomalies	✓	✓
Administration de la sécurité centrée sur l'appareil	✓	✓
Administration de la sécurité centrée sur l'utilisateur	✓	✓
Administration des systèmes		
Déploiement des systèmes d'exploitation sur les appareils clients	✓	—
Administration des licences tierces	✓	—
Utilisation du Serveur d'administration comme serveur WSUS	✓	✓ (mode de recherche passif de mises à jour Windows uniquement)
Gestion des applications tierces sur les appareils client		
Installation des mises à jour du logiciel tiers et correction des vulnérabilités dans les applications tierces	✓	✓
Surveillance, reporting et audit		
Utilisation des révisions des objets	✓	✓
Comparaison des révisions d'une stratégie	✓	* À mettre en œuvre en 2026
Consultation et utilisation des alertes détectées par Kaspersky Endpoint Detection and Response Optimum	✓	✓
Notifications sur les événements survenus sur les appareils administrés	✓	✓
Surveillance de l'état des stratégies et des tâches	✓	✓
Intégrations		
Intégration avec Kaspersky Managed Detection and Response	✓	✓
Intégration avec les systèmes SIEM	✓	✓ (en utilisant Syslog uniquement)
Exportation des événements via les formats CEF et LEEF	✓	* À mettre en œuvre en 2026

À propos de Kaspersky Security Center Cloud Console

L'utilisation de Kaspersky Security Center en tant qu'application fonctionnant sur site signifie que vous installez Kaspersky Security Center, Serveur d'administration compris, sur un appareil local et vous administrez le système de sécurité du réseau via une Console d'administration basée sur Microsoft Management Console (disponible uniquement dans Kaspersky Security Center Windows) ou Kaspersky Security Center Web Console.

Cependant, vous pouvez utiliser Kaspersky Security Center en tant que service cloud à la place. Dans ce cas, Kaspersky Security Center est installé et maintenu pour vous par des experts de Kaspersky dans l'environnement cloud, et Kaspersky vous donne accès au Serveur d'administration en tant que service. Vous administrez le système de sécurité réseau via la Console d'administration dans le cloud nommée Kaspersky Security Center Cloud Console. Cette console dispose d'une interface semblable à l'interface de Kaspersky Security Center Web Console.

L'interface et la documentation de Kaspersky Security Center Cloud Console sont disponibles dans les langues suivantes :

- anglais
- français
- allemand
- italien
- japonais
- portugais (Brésil)
- russe
- Chinois simplifié
- espagnol
- espagnol (LATAM)
- Chinois traditionnel

Plus d'informations à propos de Kaspersky Security Center Cloud Console et ses caractéristiques sont disponibles dans la documentation de Kaspersky Security Center Cloud Console et dans la documentation de Kaspersky Endpoint Security for Business.

Kaspersky Security Center 15.1

Cette section fournit des informations sur l'utilisation de Kaspersky Security Center 15.1.

Les informations de Online Help peuvent différer de celles reprises dans les documents qui accompagnent l'application. Elles sont également à jour. Pour accéder à l'aide en ligne, cliquez sur les liens qui apparaissent dans l'interface de l'application ou dans la documentation. Le contenu de l'aide en ligne peut être mis à jour sans préavis. Vous pouvez basculer entre l'aide en ligne et l'aide hors ligne, si nécessaire.

Notions principales

Cette section contient les définitions détaillées des notions principales, concernant Kaspersky Security Center.

Serveur d'administration

Les modules de Kaspersky Security Center permettent d'effectuer l'administration centralisée des applications de Kaspersky installées sur les appareils clients.

Les appareils, sur lesquels le module Serveur d'administration est installé, s'appellent les *Serveurs d'administration* (ci-après aussi *Serveurs*). Les Serveurs d'administration doivent être protégés, y compris physiquement contre tout accès non autorisé.

Le Serveur d'administration s'installe sur l'appareil en qualité de service avec la sélection d'attributs suivante :

- Sous le nom « Serveur d'administration de Kaspersky Security Center »
- Configuré de manière à démarrer automatiquement au démarrage du système d'exploitation
- Avec le compte utilisateur **LocalSystem** ou le compte utilisateur selon la sélection effectuée lors de l'installation du Serveur d'administration

Le Serveur d'administration exécute les fonctions suivantes :

- Sauvegarde de la structure des groupes d'administration
- Sauvegarde des informations sur la configuration des appareils clients
- Administration des stockages des paquets de distribution des applications
- Installation à distance des applications sur les appareils clients et suppression des applications
- Mise à jour des bases de données et des modules des applications de Kaspersky
- Administration des stratégies et des tâches sur les appareils clients
- Sauvegarde des informations sur les événements survenus sur les appareils clients

- Formation des rapports sur le fonctionnement des applications de Kaspersky
- Déploiement de clés de licence sur des appareils clients et stockage d'informations relatives aux clés de licence
- Envoi des notifications sur l'exécution en cours des tâches (par exemple, des virus détectés sur un appareil client)

Attribution d'un nom aux Serveurs d'administration dans l'interface de l'application

Dans l'interface de la Console d'administration basée sur MMC et de Kaspersky Security Center Web Console, les Serveurs d'administration peuvent avoir les noms suivants :

- Nom du Serveur d'administration, par exemple : « *nom_appareil* » ou « Serveur d'administration : *nom_appareil* ».
- Adresse IP de l'appareil Serveur d'administration, par exemple : " *adresse_IP* " ou " Serveur d'administration : *adresse_IP* ".
- Les Serveurs d'administration secondaires et les Serveurs d'administration virtuels présentent des noms personnalisés que vous indiquez lorsque vous connectez un Serveur d'administration virtuel ou secondaire au Serveur d'administration principal.
- Si vous utilisez l'instance de Kaspersky Security Center Web Console installée sur un appareil Linux, l'application affiche les noms des Serveurs d'administration que vous avez indiqués comme étant approuvés dans le fichier de réponse.

Vous pouvez vous connecter au Serveur d'administration à l'aide de la Console d'administration ou de Kaspersky Security Center Web Console.

Hiérarchie des Serveurs d'administration

Les Serveurs d'administration peuvent être classés par ordre hiérarchique. Chaque Serveur d'administration peut avoir plusieurs Serveurs d'administration secondaires (ci-après *Serveurs secondaires*) aux différents niveaux hiérarchiques. Le niveau d'intégration des Serveurs secondaires n'est pas limité. Les appareils clients de tous les Serveurs d'administration secondaires feront partie des groupes d'administration du Serveur d'administration principal. De cette façon, les participants du réseau informatique indépendants peuvent être administrés par différents Serveurs d'administration qui, à leur tour, sont administrés par le Serveur principal.

Le cas particulier des Serveurs d'administration secondaires : les *Serveurs d'administration virtuels*.

La hiérarchie des Serveurs d'administration peut être utilisée pour remplir les objectifs suivants :

- Limiter la charge sur le Serveur d'administration (par rapport à un seul Serveur installé pour un réseau entier).
- Diminuer le trafic sur le réseau et simplifier le travail sur les bureaux distants. Il n'est pas nécessaire d'établir de connexion entre le Serveur d'administration principal et tous les appareils du réseau qui peuvent se trouver par exemple dans d'autres régions. Il suffit d'installer dans chaque segment du réseau un Serveur d'administration secondaire, de répartir les appareils dans les groupes d'administration des Serveurs secondaires et fournir aux Serveurs secondaires une connexion avec le Serveur principal par des canaux de liaisons rapides.

- La répartition des responsabilités entre les administrateurs de la sécurité antivirus. En outre, toutes les possibilités d'administration centralisée et de surveillance de la sécurité antivirus du réseau de l'entreprise seront maintenues.

- Utilisez Kaspersky Security Center par les fournisseurs de services. Il suffit au fournisseur de services d'installer Kaspersky Security Center et Kaspersky Security Center Web Console. Pour gérer un grand nombre d'appareils clients de diverses organisations, un fournisseur de services peut ajouter des Serveurs d'administration secondaires (y compris des Serveurs virtuels) à la hiérarchie des Serveurs d'administration.

Chaque appareil inclus dans la hiérarchie du groupe d'administration peut être connecté à un seul Serveur d'administration. Il vous faut vérifier la connexion des appareils aux Serveurs d'administration. Pour cela, vous pouvez utiliser la fonction de recherche d'appareils selon les attributs de réseau dans les groupes d'administration des Serveurs différents.

Serveur d'administration virtuel

Serveur d'administration virtuel (ci-après *Serveur virtuel*) – le module de l'application Kaspersky Security Center conçu pour l'administration du système de protection antivirus du réseau de l'entreprise cliente.

Le Serveur d'administration virtuel est un cas particulier du Serveur d'administration secondaire et, par rapport à un Serveur d'administration physique, est soumis aux restrictions suivantes :

- Le Serveur d'administration virtuel peut fonctionner uniquement s'il fait partie d'un Serveur d'administration principal.

- Le Serveur d'administration virtuel fonctionne à l'aide de la base de données du Serveur d'administration principal. Les tâches de sauvegarde et de restauration des données, ainsi que les tâches de recherche et de téléchargement des mises à jour, ne sont pas prises en charge sur un Serveur d'administration virtuel.

- La création des Serveurs d'administration secondaires (y compris les Serveurs virtuels) n'est pas prise en charge par le Serveur virtuel.

Outre cela, le Serveur d'administration virtuel possède des restrictions suivantes :

- Dans la fenêtre des propriétés du Serveur d'administration virtuel, l'ensemble de sections est limité.

- Pour installer à distance des applications de Kaspersky sur des appareils clients administrés par le Serveur d'administration virtuel, il faut que l'Agent d'administration soit installé sur un des appareils clients pour assurer la connexion au Serveur d'administration virtuel. Lors de la première connexion au Serveur d'administration virtuel, cet appareil est automatiquement désigné en tant que point de distribution et exécute le rôle de la passerelle des connexions des appareils clients avec le Serveur d'administration virtuel.

- Le Serveur virtuel peut sonder le réseau uniquement par les points de distribution.

- Pour relancer le Serveur virtuel dont la productivité a été perturbée, Kaspersky Security Center relance le Serveur d'administration principal et tous les Serveurs virtuels.
- Les utilisateurs créés sur un Serveur virtuel ne peuvent pas se voir attribuer un rôle sur le Serveur d'administration.

L'administrateur du Serveur d'administration virtuel possède tous les privilèges dans le cadre de ce Serveur virtuel.

Serveur des appareils mobiles

Le *Serveur des appareils mobiles* est un module de Kaspersky Security Center qui offre un accès aux appareils mobiles et permet de les administrer via la Console d'administration. Le Serveur des appareils mobiles obtient les informations sur les appareils mobiles et enregistre leurs profils.

Kaspersky Security Center inclut le serveur MDM iOS en tant que Serveur d'appareils mobiles. Ce Serveur des appareils mobiles est utilisé pour administrer les appareils mobiles qui prennent en charge le service Apple® Push Notification service (APNs).

Les Serveurs des appareils mobiles de Kaspersky Security Center permettent d'administrer les objets suivants :

- Appareil mobile distinct.
- Plusieurs appareils mobiles.
- Plusieurs appareils mobiles connectés au cluster de serveurs simultanément. Lors de la connexion au cluster des serveurs, le Serveur des appareils mobiles installé sur ce cluster s'affiche dans la Console d'administration comme un serveur.

Serveur Web

Le *Serveur Web* de Kaspersky Security Center (ci-après *Serveur Web*) est un module de Kaspersky Security Center qui s'installe avec le Serveur d'administration. Le Serveur Web est conçu pour transférer via réseau des paquets d'installation autonomes, des profils MDM iOS, ainsi que des fichiers du dossier partagé.

Lors de la création, le paquet d'installation autonome est automatiquement publié sur le Serveur Web. Le lien pour télécharger le paquet autonome s'affiche dans la liste des paquets d'installation autonomes créés. En cas de nécessité, vous pouvez annuler la publication du paquet autonome ou le publier de nouveau sur le Serveur Web.

Lors de la création, le profil MDM iOS pour l'appareil mobile de l'utilisateur est aussi automatiquement publié sur le Serveur Web. Le profil publié est supprimé automatiquement du Serveur Web après l'installation réussie sur l'appareil mobile de l'utilisateur.

Le dossier partagé est utilisé pour placer les informations accessibles à tous les utilisateurs dont les appareils sont administrés via le Serveur d'administration. Si l'utilisateur n'a pas d'accès direct au dossier partagé, il est possible de lui transférer les informations depuis ce dossier à l'aide du Serveur Web.

Pour transférer aux utilisateurs les informations depuis le dossier partagé à l'aide du Serveur Web, l'administrateur doit créer le sous-dossier public imbriqué dans le dossier partagé et y placer les informations.

La syntaxe du lien de transfert des informations à l'utilisateur ressemble à ceci :

```
https://<Web Server name>:<HTTPS port>/public/<object>
```

où :

- `<Web Server name>` est le nom du Serveur Web de Kaspersky Security Center.
- `<HTTPS port>` est le port HTTPS du Serveur Web défini par l'administrateur. Le port HTTPS peut être défini dans la section **Serveur Internet** de la fenêtre des propriétés du Serveur d'administration. Le numéro de port par défaut est 8061.
- `<object>` est le sous-dossier ou le fichier dont l'accès doit être ouvert à l'utilisateur.

L'administrateur peut transférer à l'utilisateur le lien formé à l'aide d'un moyen commode quelconque, par exemple, via email.

A l'aide du lien reçu, l'utilisateur peut télécharger les informations sur l'appareil local.

Agent d'administration

L'interaction entre le Serveur d'administration et l'appareil est confiée au module *Agent d'administration* de Kaspersky Security Center. L'Agent d'administration doit être installé sur tous les appareils où l'administration des applications de Kaspersky se réalise à l'aide de Kaspersky Security Center.

L'Agent d'administration s'installe sur l'appareil en tant que service avec la sélection d'attributs suivante :

- Sous le nom "Agent d'administration de Kaspersky Security Center"
- Configuré de manière à démarrer automatiquement au démarrage du système d'exploitation
- Utilisation du compte LocalSystem

Un appareil doté de l'Agent d'administration est un *appareil administré* ou un *appareil*.

Vous pouvez installer l'Agent d'administration sur un appareil Windows, Linux ou Mac. Vous pouvez activer l'module un des sources suivants :

- Paquet d'installation dans le stockage du Serveur d'administration (le Serveur d'administration doit être installé)
- Paquet d'installation situé sur les serveurs Web de Kaspersky

Il n'est pas nécessaire d'installer l'Agent d'administration sur l'appareil où vous avez installé un Serveur d'administration car la version serveur de l'Agent d'administration est automatiquement installée avec le Serveur d'administration.

Le processus lancé par l'Agent d'administration s'appelle *klnagent.exe*.

L'Agent d'administration synchronise l'appareil administré avec le serveur d'administration. Nous recommandons d'adopter un intervalle de synchronisation (désigné également par le terme *battement de cœur*) de 15 minutes pour 10 000 appareils administrés.

Groupes d'administration

Groupe d'administration (ci-après *groupe*) : c'est l'ensemble logique des appareils administrés, réunis selon un critère dans le but d'administrer les appareils en tant que groupe unique dans Kaspersky Security Center.

Pour tous les appareils administrés dans le groupe, les éléments suivants sont installés :

- Les paramètres uniques de fonctionnement des applications, à l'aide des stratégies de groupe ;
- Utiliser un mode de fonctionnement commun pour toutes les applications via la création de tâches de groupe avec des paramètres spécifiés. Parmi les exemples de tâches de groupe, citons la création et l'installation d'un paquet d'installation commun, la mise à jour des bases de l'application et des modules, l'analyse de l'appareil à la demande et l'activation de la protection en temps réel.

L'appareil administrées peut être inclus dans un seul groupe d'administration.

Vous pouvez créer des hiérarchies de n'importe quel degré d'imbrication pour les Serveurs d'administration et les groupes. Les Serveurs d'administration secondaires et virtuels, les groupes et les appareils administrés peuvent se trouver à un niveau de la hiérarchie. Vous pouvez déplacer les appareils d'un groupe à un autre sans les déplacer physiquement. Par exemple, si un employé de l'entreprise passe de la fonction de comptable à celle de développeur, vous pouvez bouger l'appareil de cet employé depuis le groupe d'administration Comptables vers le groupe d'administration Développeurs. L'appareil recevra automatiquement par la suite les paramètres des applications requis pour les développeurs.

Appareil administré

Un *appareil administré* est un appareil exécutant Windows, Linux ou macOS sur lequel l'Agent d'administration est installé, ou un appareil mobile sur lequel une application de sécurité Kaspersky est installée. Vous pouvez administrer ces appareils via la création de tâches et de stratégies pour les applications installées sur ces appareils. Vous pouvez également recevoir les rapports pour les appareils administrés.

Vous pouvez affecter à un appareil non mobile administré la fonction de point de distribution ou de passerelle de connexion.

Un appareil peut être administré uniquement par un Serveur d'administration. Un Serveur d'administration peut administrer jusqu'à 100 000 appareils, y compris des appareils mobiles.

Appareil non défini

Un *appareil non défini* est un appareil du réseau qui n'a été inclus dans aucun groupe d'administration. Vous pouvez effectuer des actions avec des appareils non définis, par exemple, les déplacer vers des groupes d'administration et installer des applications sur ces appareils.

Quand un sondage du réseau trouve un nouvel appareil sur votre réseau, cet appareil est ajouté au groupe d'administration **Appareils non définis**. Vous pouvez configurer les règles pour les appareils qui devront être déplacés automatiquement dans d'autres groupes d'administration après la découverte des appareils.

Poste de travail de l'administrateur

Le *poste de travail de l'administrateur* est un appareil sur lequel la Console d'administration est installée ou que vous utilisez pour ouvrir Kaspersky Security Center Web Console. A partir de ces appareils, les administrateurs peuvent administrer à distance de manière centralisée les applications de Kaspersky installées sur les appareils clients.

Une fois que la Console d'administration a été installée sur votre appareil, son icône apparaît, ce qui vous permet de lancer la Console d'administration. Vous la trouverez dans **Démarrer** → **Applications** → **Kaspersky Security Center**.

Aucune restriction n'est imposée sur le nombre de postes de travail de l'administrateur. Depuis chaque poste de travail de l'administrateur, il est possible d'administrer les groupes d'administration de plusieurs Serveurs d'administration dans le réseau. Le poste de travail de l'administrateur peut être connecté au Serveur d'administration (physique et virtuel) de n'importe quel niveau de la hiérarchie.

Le poste de travail de l'administrateur peut être inclus dans le groupe d'administration en tant qu'appareil client.

Dans le cadre des groupes d'administration de n'importe quel Serveur d'administration, le même appareil peut être simultanément client du Serveur d'administration, Serveur d'administration et poste de travail de l'administrateur.

Plug-in d'administration

L'administration des applications Kaspersky via la Console d'administration est exécutée à l'aide d'un module dédié appelé *plug-in d'administration*. Chaque application de Kaspersky qui peut être administrée via Kaspersky Security Center possède un plug-in d'administration.

À l'aide du plug-in d'administration des applications, il est possible d'exécuter les actions suivantes dans la Console d'administration :

- Créer et modifier les stratégies et les paramètres de l'application, ainsi que les paramètres des tâches de cette application.
- Obtenir les informations sur les tâches de l'application, sur les événements dans son fonctionnement, et sur les statistiques de fonctionnement de l'application obtenues depuis les appareils clients.

Vous pouvez télécharger des plug-ins d'administration à partir de la page Web du Support Technique de Kaspersky.

Plug-in Web d'administration

Un module spécial, le *plug-in Web d'administration*, permet de réaliser l'administration à distance des logiciels de Kaspersky via Kaspersky Security Center Web Console. Ci-après, un plug-in Web d'administration est également appelé *plug-in d'administration*. Un plug-in d'administration est une interface entre Kaspersky Security Center Web Console et une application spécifique de Kaspersky. Un plug-in d'administration permet de configurer des tâches et des stratégies pour l'application.

Vous pouvez télécharger les plug-ins Web de gestion à partir de la page Web du Support Technique de Kaspersky.

Le plug-in d'administration offre les éléments suivants :

- Interface pour la création et la modification des tâches et des paramètres de l'application
- Interface pour la création et la modification de stratégies et de profils de stratégie pour la configuration centralisée et à distance d'applications et d'appareils de Kaspersky
- Transmission des événements créés par l'application
- Fonctions de Kaspersky Security Center Web Console pour l'affichage des données opérationnelles et des événements de l'application et des statistiques transmises par les appareils client

Stratégies

Une *stratégie* est un ensemble de paramètres d'application Kaspersky qui sont appliqués à un groupe d'administration et à ses sous-groupes. Vous pouvez installer plusieurs applications Kaspersky sur les appareils d'un groupe d'administration. Kaspersky Security Center fournit une stratégie propre à chaque application Kaspersky d'un groupe d'administration. La stratégie possède un des états suivants (voir le tableau ci-dessous) :

L'état de la stratégie

État	Description
Actif	La stratégie actuelle appliquée à l'appareil. Une seule stratégie peut être active pour une application Kaspersky dans chaque groupe d'administration. Les appareils appliquent les valeurs de paramètres d'une stratégie active pour une application Kaspersky.
Inactive	Une stratégie qui n'est actuellement pas appliquée à un appareil.
Pour les utilisateurs itinérants	Si cette option a été sélectionnée, la stratégie agit lorsque l'appareil est déconnecté du réseau de l'entreprise.

Le fonctionnement des stratégies obéit aux règles suivantes :

- Il est possible de configurer plusieurs stratégies avec différentes valeurs pour une seule application.
- Une seule stratégie peut être active pour l'application actuelle.
- Vous pouvez activer une stratégie inactive lorsqu'un événement en particulier se produit. Par exemple, vous pouvez mettre en œuvre des paramètres d'Endpoint Protection plus stricts en cas de propagation de virus.
- Une stratégie peut comporter des stratégies enfants.

En règle générale, vous pouvez utiliser des stratégies pour vous préparer aux situations d'urgence, telles qu'une propagation de virus. Par exemple, en cas d'attaque via les clés USB, vous pouvez activer une stratégie bloquant l'accès aux clés USB. Dans ce cas, la stratégie active actuelle devient automatiquement inactive.

Afin d'éviter une multiplicité de stratégies, par exemple, lorsque des circonstances diverses impliquent la seule modification de plusieurs paramètres, vous pouvez utiliser des profils de stratégie.

Un *profil de stratégie* est un sous-ensemble nommément désigné de valeurs de paramètres de stratégie qui remplace les valeurs de paramètres d'une stratégie. Un profil de stratégie affecte la formation effective des paramètres sur un appareil administré. *Les paramètres effectifs* sont un ensemble de paramètres de stratégie, de paramètres de profil de stratégie et de paramètres d'application locale actuellement appliqués à l'appareil.

Les profils de stratégie fonctionnent conformément aux règles suivantes :

- Un profil de stratégie prend effet lorsqu'une condition d'activation particulière est réalisée.
- Les profils de stratégie contiennent des valeurs de paramètres qui diffèrent des paramètres de stratégie.
- L'activation d'un profil de stratégie modifie les paramètres effectifs de l'appareil administré.
- Une stratégie ne peut pas compter plus de 100 profils de stratégie.

Profils de stratégie

Il peut être parfois nécessaire de créer plusieurs instances d'une seule stratégie pour différents groupes d'administration. Vous pouvez également modifier les paramètres de ces stratégies de manière centralisée. Ces instances peuvent différer uniquement sur un ou deux paramètres. Par exemple, tous les comptables d'une entreprise sont soumis à la même stratégie, mais les comptables avec plus de responsabilités sont autorisés à utiliser des clés USB, à la différence du reste. Dans ce cas, l'application de stratégies aux appareils uniquement via la hiérarchie des groupes d'administration peut être ardue.

Pour vous éviter la création de plusieurs instances d'une seule stratégie, Kaspersky Security Center permet de créer des *profils des stratégies*. Les profils de stratégie sont nécessaires pour que les appareils à l'intérieur d'un groupe d'administration puissent avoir différents paramètres de stratégie.

Un profil de stratégie est un sous-ensemble nommé de paramètres de stratégie. Un profil de stratégie est un sous-ensemble nommé de paramètres de stratégie qui est diffusé sur les appareils avec la stratégie et qui vient compléter la stratégie quand une condition définie, la *condition d'activation du profil*, est remplie. Les profils contiennent uniquement les paramètres qui se distinguent de la stratégie " de base " en vigueur sur l'appareil administré (ordinateur, appareil mobile). L'activation d'un profil modifie les paramètres dans la stratégie " de base " active à l'origine sur l'appareil. La modification paramètres prennent alors les valeurs reprises dans le profil.

Tâches

Kaspersky Security Center gère le fonctionnement des protection applications Kaspersky installées sur les appareils par la création et l'exécution des *tâches*. Les tâches permettent d'exécuter l'installation, le lancement et l'arrêt des applications, l'analyse des fichiers, la mise à jour des bases de données et des modules des applications, les autres actions avec les applications.

Des tâches pour une application définie peuvent être créées uniquement si le plug-in d'administration pour cette application est installé.

Les tâches peuvent être exécutées sur le Sur le Serveur d'administration et sur les appareils.

Tâches exécutées sur le Serveur d'administration :

- Diffusion automatique des rapports
- Téléchargement des mises à jour dans le stockage du Serveur d'administration
- Sauvegarde des données du Serveur d'administration

- Maintenance de la base de données
- Synchronisation de Windows Update
- Création du paquet d'installation sur la base de l'image du système d'exploitation de l'appareil de référence

Les types de tâche suivants sont réalisés sur les appareils :

- *Tâches* exécutées sur un appareil particulier

  Les tâches locales peuvent être modifiées non seulement par l'administrateur via la Console d'administration, mais aussi par l'utilisateur de l'appareil distant (par exemple, dans l'interface de l'application de sécurité). Si la tâche locale a été modifiée simultanément par l'administrateur et l'utilisateur sur l'appareil administré, ce sont les modifications introduites par l'administrateur qui sont retenues car elles ont une priorité supérieure.

- *Tâches de groupe* : tâches qui sont réalisées sur tous les appareils d'un groupe particulier

  Sauf indication contraire dans les propriétés de la tâche, une tâche de groupe peut également avoir un impact sur les sous-groupes du groupe sélectionné. Une tâche de groupe agit aussi (de manière facultative) sur les appareils connectés aux Serveurs d'administration virtuels et secondaires placés dans ce groupe et ses sous-groupes.

- *Tâches* — Tâches exécutées sur les appareils un ensemble de peu importe leur inclusion dans les groupes d'administration.

Pour chaque application vous pouvez créer n'importe quel nombre de tâches de groupe, de tâches globales et des tâches locales.

Vous pouvez modifier les paramètres des tâches en l'exécution des tâches, copier, exporter ou importer, ainsi que supprimer les Tâches.

Les tâches ne sont lancées sur un appareil que lorsque l'application pour laquelle les tâches ont été créées est lancée.

Les résultats des tâches sont enregistrés dans les journaux des événements Microsoft Windows et Kaspersky Security Center d'une manière centralisée sur le Serveur d'administration et d'une manière locale sur chaque appareil.

N'incluez pas de données confidentielles dans les paramètres des tâches. Par exemple, le mot de passe de l'administrateur de domaine.

Zone d'action d'une tâche

La *zone d'action d'une tâche* est l'ensemble d'appareils sur lesquels la tâche est réalisée. Voici les types de zone d'action :

- Pour une *tâche locale*, la zone d'action est l'appareil en lui-même.
- Pour une *tâche du Serveur d'administration*, la zone d'action est le Serveur d'administration.
- Pour une *tâche de groupe*, la zone d'action est la liste des appareils inclus dans le groupe.

Lors de la création d'une *tâche globale*, vous pouvez utiliser les méthodes suivantes afin de définir la zone d'action :

- Désignation manuelle de certains appareils.

  Vous pouvez utiliser l'adresse IP (ou l'intervalle IP), le nom NetBIOS ou le nom DNS en tant que l'adresse de l'appareil.

- Importer la liste des appareils depuis le fichier au format TXT, contenant la les adresses des appareils ajoutés (chaque adresse doit se trouver dans une ligne séparée).

  Si la liste des appareils est importée depuis le fichier ou formée manuellement et les appareils sont identifiés selon le nom, uniquement les appareils dont les informations sont déjà enregistrées dans la base de données du Serveur d'administration peuvent être ajoutés dans la liste lors de la connexion des appareils ou lors du. De plus, l'information doit avoir été saisie quand ces appareils étaient connectés ou lors de la recherche d'appareils.

- Indiquer une sélection d'appareils.

  Au fil du temps, la zone d'action de la tâche change au fur et à mesure que change la quantité d'appareils qui figurent dans la sélection. La sélection d'appareils peut s'opérer sur la base des attributs des appareils, notamment sur la base du logiciel installé sur l'appareil, ainsi que sur la base des tags attribués à l'appareil. La sélection d'appareils est la méthode la plus flexible pour définir la zone d'action d'une tâche.

  Le Serveur d'administration se charge toujours de la programmation des tâches pour les sélections d'appareils. Ces tâches ne seront pas lancées sur les appareils qui ne communiquent pas avec le Serveur d'administration. Les tâches dont la zone d'action est définie à l'aide d'autres méthodes sont exécutées directement sur les appareils et par conséquent, elles ne dépendent pas de la connexion de l'appareil au Serveur d'administration.

  Les tâches pour les sélections d'appareils sont lancées non selon l'heure locale de l'appareil, mais bien selon l'heure locale du Serveur d'administration. Les tâches dont la zone d'action est définie par d'autres méthodes sont exécutées à l'heure locale de l'appareil.

Corrélation de la stratégie et des paramètres locaux de l'application

A l'aide des stratégies, les mêmes valeurs des paramètres de fonctionnement de l'application peuvent être installées pour tous les appareils inclus dans le groupe.

Vous pouvez redéfinir les valeurs des paramètres définies par une stratégie pour les appareils individuels dans le groupe à l'aide des paramètres locaux de l'application. Avec cela, vous pouvez établir les valeurs des paramètres, dont la modification n'est pas interdite par la stratégie (le paramètre n'est pas fermé par le cadenas).

La valeur du paramètre, utilisée par l'application sur l'appareil client est définie par la position du cadenas (🔒) dans le paramètre de la stratégie :

- Si la modification du paramètre est interdite, la même valeur est utilisée sur tous les appareils clients : définie par la stratégie.

- Si ce n'est pas interdit, l'application n'utilise alors pas la valeur qui est indiquée dans la stratégie sur chaque appareil client, mais la valeur locale du paramètre. Cela dit, la valeur du paramètre peut être modifiée par les paramètres locaux de l'application.

De cette façon, lorsque la tâche est en exécution sur un appareil client, l'application utilise les paramètres définis selon deux manières différentes :

- Par les paramètres de la tâche et les paramètres locaux de l'application, si l'interdiction de modifier le paramètre n'était pas établie dans la stratégie.
- Par la stratégie du groupe, si l'interdiction de modifier le paramètre était établie dans la stratégie.

Les paramètres locaux de l'application sont modifiés après la première utilisation de la stratégie conformément aux paramètres de la stratégie.

Point de distribution

Le point de distribution (connu comme l'agent de mises à jour) est un appareil avec un Agent d'administration installé qui sert à la diffusion des mises à jour, à installer les applications à distance et à recevoir des informations sur les appareils du réseau. Les points de distribution accélèrent la diffusion des mises à jour et permettent d'économiser les ressources du Serveur d'administration.

Les fonctionnalités et les cas d'utilisation de l'Agent d'administration installé sur un appareil utilisé comme point de distribution varient en fonction du système d'exploitation.

Un point de distribution peut remplir les fonctions suivantes :

- Distribuer les fichiers reçus du Serveur d'administration aux appareils clients au sein du groupe (y compris la distribution via la multidiffusion à l'aide d'UDP).

  La liste des fichiers pouvant être transférés par les points de distribution comprend :

  - Mises à jour des bases de données et des modules logiciels de Kaspersky
  - Mises à jour du logiciel tiers
  - Paquets d'installation
  - Mises à jour Windows lorsque vous utilisez le Serveur d'administration comme serveur WSUS

  Les mises à jour peuvent être obtenues à partir du Serveur d'administration comme à partir des serveurs de mise à jour de Kaspersky. Dans ce dernier cas, une tâche de mise à jour doit être créée pour le point de distribution. Les appareils de points de distribution exécutant macOS ne peuvent pas télécharger les mises à jour à partir des serveurs de mises à jour de Kaspersky.

  Si un ou plusieurs appareils exécutant macOS sont inclus dans la zone d'action de la tâche *Télécharger les mises à jour sur les stockages des points de distribution*, la tâche reçoit l'état *Échec*, même si elle s'est terminée avec succès sur tous les appareils Windows.

- Diffuser les stratégies et les tâches de groupe à l'aide d'une diffusion de type multidiffusion via le protocole UDP.

- Agit en tant que passerelle pour la connexion au Serveur d'administration pour les appareils d'un groupe d'administration.

  Lorsqu'il est impossible d'établir une connexion directe entre les appareils administrés du groupe et le serveur d'administration, le point de distribution peut être désigné comme passerelle de connexion de ce groupe au Serveur d'administration. Dans ce cas, les appareils administrés se connectent à la passerelle qui se connecte à son tour au Serveur d'administration.

  La présence d'un point de distribution qui fonctionne en mode passerelle de connexions n'empêche pas la connexion directe des appareils administrés au Serveur d'administration. Si la passerelle de connexion n'est pas disponible et qu'une connexion directe au Serveur d'administration est possible sur le plan technique, les appareils administrés se connectent directement au Serveur.

- Sonder le réseau dans le but de détecter de nouveaux appareils et de mettre à jour les informations sur les appareils détectés. Un point de distribution peut exécuter les mêmes méthodes de recherche d'appareils que le Serveur d'administration.

- Effectuez l'installation à distance de logiciels tiers et d'applications Kaspersky à l'aide des outils du système d'exploitation du point de distribution. Notez que le point de distribution peut effectuer l'installation sur les appareils clients sans Agent d'administration.

  Cette fonction permet de transmettre à distance les paquets d'installation de l'Agent d'administration sur les appareils clients du réseau auxquels le Serveur d'administration n'a pas d'accès direct.

- Agir comme un serveur proxy qui participe à Kaspersky Security Network (KSN).

  Vous pouvez activer le serveur proxy KSN du côté du point de distribution pour que l'appareil agisse comme le serveur proxy KSN. Dans ce cas, le service KSN proxy (ksnproxy) est exécuté sur l'appareil.

La transmission des fichiers au point de distribution par le Serveur d'administration s'effectue via le protocole HTTP ou, si une connexion SSL est configurée, via le protocole HTTPS. L'utilisation du protocole HTTP ou HTTPS assure une performance plus élevée par rapport au protocole SOAP grâce à la réduction du trafic.

Les appareils sur lesquels l'Agent d'administration est installé peuvent être assignés comme points de distribution manuellement par l'administrateur ou automatiquement par le Serveur d'administration. Pour obtenir la liste complète des points de distribution pour les groupes d'administration indiqués, il faut créer un rapport sur la liste des points de distribution.

La zone d'action du point de distribution est le groupe d'administration dont il est assigné administrateur et dans les sous-groupes, quel que soit le niveau d'intégration. Si la hiérarchie des groupes d'administration compte plusieurs points de distribution, l'Agent d'administration de l'appareil administré se connecte au point de distribution le plus proche dans la hiérarchie.

L'emplacement réseau peut aussi être une zone d'action des points de distribution. L'emplacement réseau s'utilise pour la création en mode manuel d'un ensemble d'appareils sur lesquels le point de distribution déploiera les mises à jour. La définition de l'emplacement réseau est accessible seulement pour les appareils administrés sous le système d'exploitation Windows.

Si les points de distribution sont assignés automatiquement par le Serveur d'administration, le serveur assigne ces points de distribution par domaines multicast, et non par groupes d'administration. Cela se produit dès que les domaines multicast sont connus. L'Agent d'administration communique avec les autres Agents d'administration de son réseau par messages et envoie au Serveur d'administration des informations sur lui-même et de brèves informations sur les autres Agents d'administration. Sur la base de ces informations, le Serveur d'administration peut regrouper des Agents d'administration par domaines multicast. Les domaines multicast deviennent connus du Serveur d'administration dès que plus de 70 % des Agents d'administration ont été sondés dans les groupes d'administration. Le Serveur d'administration sonde les domaines de diffusion toutes les deux heures. Dès que les points de distribution ont été désignés par domaine de diffusion, il est impossible de les désigner à nouveau par groupes d'administration.

Si l'administrateur attribue manuellement des points de distribution, ils peuvent être affectés à des groupes d'administration ou à des emplacements réseau.

Les Agents d'administration avec un profil actif de connexion ne participent pas à la définition d'un domaine multicast.

Kaspersky Security Center attribue à chaque Agent d'administration une adresse de diffusion IP multiple unique qui ne recoupe pas les autres adresses. Cela permet d'éviter un excès de charge sur le réseau, ce qui se produirait en cas d'interaction des adresses.

Si sur une seule parcelle de réseau ou dans un groupe d'administration, au moins deux points de distribution sont désignés, l'un d'entre eux devient le point de distribution actif et les autres sont nommés points de distribution de réserve. Le point de distribution actif télécharge les mises à jour et les paquets d'installation directement à partir du serveur d'administration, tandis que les points de distribution de réserve reçoivent les mises à jour à partir du point de distribution actif, uniquement. Dans ce cas, les fichiers sont téléchargés une seule fois à partir du Serveur d'administration, puis répartis entre les points de distribution. Si le point de distribution actif est indisponible pour quelque raison, l'un des points de distribution en attente s'active. Le Serveur d'administration désigne automatiquement le point de distribution comme point de distribution de réserve.

L'état du point de distribution (*Actif* / *De réserve*) est indiqué par une case à cocher dans le rapport de l'utilitaire klnagchk.

Un point de distribution nécessite au moins 4 Go d'espace libre sur le disque. Si l'espace libre disponible sur le disque du point de distribution est inférieur à 2 Go, Kaspersky Security Center crée un problème de sécurité avec le niveau d'importance *Avertissement*. L'incident sera publié dans les propriétés de l'appareil dans la section **Problèmes de sécurité**.

Il faut de l'espace libre sur le disque en cas d'utilisation de tâches d'installation à distance sur un appareil désigné comme point de distribution. L'espace libre sur le disque doit être supérieur à la taille de l'ensemble des paquets d'installation à installer.

L'utilisation de la tâche d'installation des mises à jour (correctifs) et de correction des vulnérabilités sur un appareil désigné comme point de distribution requiert de l'espace libre sur le disque. Cet espace libre doit être au moins le double du volume de l'ensemble des correctifs à installer.

Les appareils fonctionnant comme points de distribution doivent être protégés, y compris physiquement contre tout accès non autorisé.

Passerelle des connexions

Une *passerelle de connexion* est un Agent d'administration fonctionnant dans un mode spécial. Une passerelle de connexion accepte les connexions d'autres Agents d'administration et les achemine vers le Serveur d'administration par sa propre connexion avec le serveur. Contrairement à un Agent d'administration ordinaire, une passerelle de connexion attend les connexions du Serveur d'administration au lieu d'établir des connexions avec le Serveur d'administration.

Une passerelle de connexion peut recevoir les connexions de jusqu'à 10 000 appareils.

Vous avez deux options pour utiliser des passerelles de connexion :

- Nous vous recommandons d'installer une passerelle de connexion dans une zone démilitarisée (DMZ). Pour les autres Agents d'administration installés sur des appareils itinérants, vous devez configurer spécialement une connexion au Serveur d'administration via la passerelle de connexion.

  Une passerelle de connexion ne modifie ni ne traite en aucune façon les données transmises des Agents d'administration au Serveur d'administration. De plus, elle n'écrit ces données dans aucun tampon et ne peut donc pas accepter les données d'un Agent d'administration et les transmettre ultérieurement au Serveur d'administration. Si l'Agent d'administration tente de se connecter au Serveur d'administration via la passerelle de connexion, mais que la passerelle de connexion ne peut pas se connecter au Serveur d'administration, l'Agent d'administration interprète cela comme si le Serveur d'administration était inaccessible. Toutes les données restent sur l'Agent d'administration (et non sur la passerelle de connexion).

  Une passerelle de connexion ne peut pas se connecter au Serveur d'administration via une autre passerelle de connexion. Cela signifie que l'Agent d'administration ne peut pas être simultanément une passerelle de connexion et utiliser une passerelle de connexion pour se connecter au Serveur d'administration.

  Toutes les passerelles de connexion sont incluses dans la liste des points de distribution dans les propriétés du Serveur d'administration.

- Vous pouvez également utiliser des passerelles de connexion au sein du réseau. Par exemple, les points de distribution attribués automatiquement deviennent également des passerelles de connexion dans leur propre zone d'action. Cependant, au sein d'un réseau interne, les passerelles de connexion n'offrent pas d'avantages considérables. Elles réduisent le nombre de connexions réseau reçues par le Serveur d'administration, mais ne réduisent pas le volume des données entrantes. Même sans passerelles de connexion, tous les appareils peuvent toujours se connecter au Serveur d'administration.

Principal scénario d'installation

Grâce à ce scénario, vous pouvez déployer le Serveur d'administration et installer l'Agent d'administration et les applications de sécurité sur les appareils du réseau. Vous pouvez utiliser ce scénario pour découvrir l'application et pour l'installer en vue d'une utilisation ultérieure.

L'installation de Kaspersky Security Center comprend les étapes suivantes :

1. Préparatifs
2. Installation de Kaspersky Security Center et d'une application de sécurité Kaspersky sur l'appareil du Serveur d'administration
3. Déploiement centralisé des applications de sécurité Kaspersky sur les appareils clients

Le déploiement de Kaspersky Security Center dans le cloud et le déploiement de Kaspersky Security Center pour les prestataires de services sont décrits dans les sections d'aide.

Nous vous recommandons de consacrer au moins une heure à l'installation du Serveur d'administration et au moins une journée de travail à l'exécution du scénario. Nous vous conseillons également d'installer une application de sécurité, telle que Kaspersky Security for Windows Server ou Kaspersky Endpoint Security, sur l'appareil qui fera office de Serveur d'administration de Kaspersky Security Center.

Une fois le scénario terminé, la protection est déployée dans le réseau de l'entreprise de la façon suivante :

- Le SGBD sera installé pour le Serveur d'administration.
- Le Serveur d'administration de Kaspersky Security Center est installé.

- Les stratégies et les tâches requises seront créées, et les paramètres de stratégie et de tâches par défaut sont indiqués.
- Les applications de sécurité (par exemple, Kaspersky Endpoint Security for Windows) et l'Agent d'administration sont installées sur les appareils administrés.
- Les groupes d'administration sont créés (éventuellement liés à la hiérarchie).
- Le cas échéant, la protection des appareils mobiles est déployée.
- Les points de distribution sont affectés le cas échéant.

L'installation de Kaspersky Security Center se déroule par étapes :

Préparatifs

1. **Obtention des fichiers nécessaires**

   Assurez-vous que vous disposez d'une clé de licence (code d'activation) pour Kaspersky Security Center ou de clés de licence (codes d'activation) pour les applications de sécurité Kaspersky.

   Décompressez l'archive que vous avez reçue de la part de votre fournisseur. Cette archive contient les clés de licence (fichiers KEY), codes d'activation, et la liste des applications Kaspersky pouvant être activées par chaque clé de licence.

   Si vous souhaitez d'abord essayer Kaspersky Security Center, vous pouvez obtenir une évaluation gratuite de 30 jours sur le site Web de Kaspersky.

   Pour obtenir des informations détaillées sur les licences des applications de sécurité Kaspersky qui ne sont pas incluses dans Kaspersky Security Center, vous pouvez vous reporter à la documentation de ces applications.

2. **Sélection de la structure de protection d'une organisation**

   Prenez connaissance des modules de Kaspersky Security Center. Choisissez la structure de la protection et la configuration du réseau les mieux adaptées à votre organisation. En fonction de la configuration du réseau et de la bande passante des canaux de communication, définissez le nombre de Serveurs d'administration à utiliser et leur répartition entre les bureaux, (si vous utilisez un réseau distribué).

   Pour atteindre et conserver les performances optimales dans les conditions d'utilisation les plus diverses, tenez compte du nombre d'appareils protégés dans le réseau, de la topologie du réseau et des fonctions de Kaspersky Security Center dont vous avez besoin (pour en savoir plus, consultez le Guide de dimensionnement de Kaspersky Security Center).

   Déterminez si votre organisation va utiliser une hiérarchie des Serveurs d'administration. Pour cela, il faut savoir s'il est possible et utile de couvrir tous les appareils client à l'aide d'un Serveur d'administration ou s'il faut élaborer une hiérarchie des Serveurs d'administration. Il faudra peut-être aussi organiser une hiérarchie des Serveurs d'administration conforme à la structure organisationnelle de l'organisation dont vous souhaitez protéger le réseau.

   Si vous devez garantir la protection des appareils mobiles, exécutez les actions préalables de configuration d'un Serveur MDM iOS.

   Confirmez que les appareils que vous avez sélectionnés en vue d'une utilisation en tant que Serveurs d'administration et pour l'installation de la Console d'administration répondent à la configuration matérielle et logicielle.

3. **Préparation à l'utilisation de certificats personnalisés**

   Si l'infrastructure à clé publique (PKI) de votre organisation nécessite que vous utilisiez des certificats personnalisés émis par une autorité de certification (CA) en particulier, préparez ces certificats et assurez-vous qu'ils répondent à toutes les exigences.

4. **Préparation de la licence de Kaspersky Security Center**

   Si vous envisagez d'utiliser une version de Kaspersky Security Center avec administration des appareils mobiles, intégration aux systèmes SIEM et/ou prise en charge de la fonction de Gestion des vulnérabilités et des correctifs, confirmez que vous possédez un fichier clé ou un code d'activation pour la licence de l'application.

5. **Préparation de la licence des applications de sécurité administrées**

   Pendant le déploiement de la protection il est nécessaire de fournir à Kaspersky les clés de licence actives des applications que vous envisagez d'administrer à l'aide de Kaspersky Security Center (voir la liste des applications de sécurité pouvant être administrées). Pour plus d'informations sur l'obtention d'une licence pour chacune des applications de sécurité, vous pouvez consulter la documentation qui les accompagne.

6. **Sélection de la configuration matérielle du Serveur d'administration et du SGBD**

   Prévoyez la configuration matérielle pour le SGBD et le Serveur d'administration en tenant compte du nombre d'appareils dans votre réseau.

7. **Choix d'un SGBD**

   Au moment de choisir le SGBD, tenez compte du nombre d'appareils administrés qui seront couverts par le Serveur d'administration. Si votre réseau compte moins de 10 000 appareils et que vous n'envisagez pas d'augmenter ce nombre, vous pouvez utiliser un SGBD gratuit comme SQL Express ou MySQL et l'installer sur un appareil doté du Serveur d'administration. Vous pouvez également choisir le SGBD MariaDB qui vous permet d'administrer jusqu'à 20 000 appareils. Si votre réseau compte plus de 10 000 appareils (ou si vous avez l'intention d'élargir votre réseau jusqu'à atteindre une telle quantité), il est conseillé d'utiliser une version payante du SGBD SQL et de l'installer sur un appareil distinct. Un SGBD payant peut fonctionner avec plusieurs Serveurs d'administration, tandis qu'un SGBD gratuit ne fonctionne qu'avec un seul serveur.

   Si vous sélectionnez SQL Server DBMS, notez que vous pouvez migrer les données stockées dans la base de données vers MySQL, MariaDB ou Azure SQL DBMS. Pour effectuer la migration, sauvegardez vos données et restaurez-les dans le nouveau DBMS.

8. **Installation du SGBD et création d'une base de données**

   Renseignez-vous sur les comptes pour le travail avec le SGBD et installez votre SGBD.

   Avant l'installation, choisissez un SGBD pris en charge. Vous pouvez sélectionner, par exemple, PostgreSQL, Postgres Pro, Microsoft SQL Server, MySQL, ou MariaDB.

   Pour en savoir plus sur l'installation du SGBD sélectionné, consultez sa documentation.

   Si vous installez MariaDB, MySQL, PostgreSQL ou Postgres Pro, utilisez les paramètres recommandés pour garantir le bon fonctionnement du SGBD.

   Notez et conservez les paramètres du SGBD car vous en aurez besoin lors de l'installation du Serveur d'administration. Ces paramètres reprennent le nom du serveur SQL, le numéro de port pour la connexion au serveur SQL, le nom du compte et le mot de passe d'accès au serveur SQL.

   > Si vous décidez d'installer le SGBD PostgreSQL ou Postgres Pro, assurez-vous d'avoir indiqué un mot de passe de superutilisateur. Si le mot de passe n'est pas indiqué, le Serveur d'administration risque de ne pas pouvoir se connecter à la base de données.

   Par défaut, le programme d'installation de Kaspersky Security Center crée la base de données pour le placement des informations du Serveur d'administration, mais vous pouvez refuser sa création et utiliser une autre base de données. Dans ce cas, assurez-vous que la base de données a été créée, que vous connaissez son nom, et que le compte sous lequel le Serveur d'administration accédera à cette base de données a le rôle db_owner correspondant.

   En cas de nécessité, contactez l'administrateur SGBD pour plus d'informations.

9. **Configuration des ports**

Assurez-vous que, pour l'interaction des modules selon la structure de protection choisie par vous, les ports nécessaires sont ouverts.

S'il faut accorder l'accès au Serveur d'administration depuis Internet, configurez les ports et les paramètres de connexion, en fonction de la configuration du réseau.

10. **Contrôle des comptes utilisateurs**

Vérifiez que vous disposez des droits d'administrateur local pour une installation réussie du Serveur d'administration de Kaspersky Security Center et le déploiement de la protection sur les appareils. Les droits d'administrateur local sur les appareils client sont nécessaires pour l'installation de l'Agent d'administration sur ces appareils. Après l'installation de l'Agent d'administration, vous pourrez l'utiliser afin d'installer à distance les applications sur les appareils, sans passer par le compte utilisateur disposant des droits d'administrateur de ces appareils.

Par défaut, le programme d'installation de Kaspersky Security Center crée sur l'appareil sélectionné pour l'installation du Serveur d'administration, trois comptes utilisateur locaux, sous lesquels seront lancés le Serveur d'administration et les services de Kaspersky Security Center :

- KL-AK-* : compte utilisateur du service du Serveur d'administration.
- NT Service/KSC* : compte utilisateur pour les autres services compris dans le Serveur d'administration.
- KlPxeUser : compte utilisateur pour le déploiement des systèmes d'exploitation.

Vous pouvez ne pas créer de compte pour les services du Serveur d'administration et les autres services. Utilisez vos comptes existants à la place, par exemple les comptes de domaine si vous prévoyez d'installer le Serveur d'administration sur un cluster haute disponibilité ou d'utiliser des comptes de domaine au lieu de comptes locaux pour toute autre raison. Dans ce cas, assurez-vous que les comptes utilisateur pour le lancement du Serveur d'administration et des services de Kaspersky Security Center sont créés, ne sont pas des comptes privilégiés et possèdent les droits nécessaires à l'accès au SGBD. (Si vous envisagez par la suite de déployer les systèmes d'exploitation sur des appareils Kaspersky Security Center, ne refusez pas la création de comptes utilisateur.)

Installation de Kaspersky Security Center et d'une application de sécurité Kaspersky sur l'appareil du Serveur d'administration

1. **Installation du Serveur d'administration, de la Console d'administration, de Kaspersky Security Center Web Console et des plug-ins d'administration pour les applications de sécurité**

Téléchargez Kaspersky Security Center depuis le site Web de Kaspersky. Vous pouvez télécharger le paquet complet, la Web Console uniquement ou la Console d'administration uniquement.

Installez le Serveur d'administration sur l'appareil sélectionné (ou les appareils, s'il vous est nécessaire d'utiliser plusieurs Serveurs d'administration). Vous avez le choix entre une installation standard ou une installation personnalisée du Serveur d'administration. La Console d'administration est installée avec le Serveur d'administration. Il est recommandé d'installer le Serveur d'administration sur un serveur dédié au lieu d'un contrôleur de domaine.

L'installation standard est recommandée si vous voulez découvrir l'application Kaspersky Security Center, par exemple, tester son fonctionnement sur un petit segment de votre réseau. Dans le cadre de l'installation standard, vous configurez uniquement les paramètres de la base de données. Vous pouvez également installer uniquement l'ensemble par défaut de plug-ins d'administration des applications de Kaspersky. Vous pouvez aussi vous servir de l'installation standard si vous avez déjà l'habitude d'utiliser Kaspersky Security Center et pouvez spécifier tous les paramètres nécessaires après l'installation standard.

L'installation personnalisée est recommandée si vous envisagez de modifier les paramètres de Kaspersky Security Center, comme un chemin vers le dossier partager, les comptes utilisateurs et les ports de connexion au Serveur d'administration, ainsi que les paramètres de la base de données. L'installation personnalisée vous permet de désigner les plug-ins d'administration des applications de Kaspersky à installer. En cas de nécessité, vous pouvez lancer l'installation personnalisée en mode silencieux.

La Console d'administration et la version serveur de l'Agent d'administration sont également installées avec le Serveur d'administration. Vous pouvez aussi choisir d' Installer Kaspersky Security Center Web Console lors de l'installation.

En cas de besoin, installez la Console d'administration et/ou la Kaspersky Security Center Web Console séparément sur le poste de travail de l'administrateur pour gérer le Serveur d'administration par le réseau.

2. **Configuration initiale et licence**

   Après l'achèvement de l'installation du Serveur d'administration lors de la première connexion au Serveur d'administration, l'Assistant de configuration initiale de l'application est automatiquement lancé. Exécutez la configuration initiale du Serveur d'administration conformément à vos exigences. Lors de la configuration initiale, l'Assistant crée les stratégies indispensables au déploiement de la protection et les tâches selon les paramètres par défaut. Il se peut que ces paramètres ne soient pas parfaits pour les besoins de votre entreprise. Si nécessaire, vous pouvez modifier les paramètres des stratégies et des tâches (Configuration de la protection sur le réseau d'une entreprise cliente, Scénario de configuration de la protection réseau).

   Si vous envisagez d'utiliser les fonctions situées hors de la fonctionnalité de base, mettez l'application sous licence. Pour cela, vous pouvez effectuer une des étapes de l'Assistant de configuration initiale de l'application.

3. **Analyse du succès de l'installation du Serveur d'administration**

   Après l'exécution fructueuse des étapes précédentes, le Serveur d'administration est installé et prêt pour une utilisation ultérieure.

   Assurez-vous que la Console d'administration fonctionne et que vous pouvez vous connecter via la Console au Serveur d'administration. Assurez-vous également que la tâche de téléchargement des mises à jour du stockage du Serveur d'administration se trouve bien sur le Serveur d'administration (dans le dossier **Tâches** de l'arborescence de la console), ainsi que la stratégie pour Kaspersky Endpoint Security (dans le dossier **Stratégies** de l'arborescence de la console).

   Une fois la vérification terminée, suivez les étapes ci-après.

Déploiement centralisé des applications de sécurité Kaspersky sur les appareils clients

1. **Recherche d'appareils en réseau**

   Cette étape se trouve dans l'Assistant de configuration initiale de l'application. Vous pouvez aussi commencer la Recherche d'appareils manuellement. Suite à cela, Kaspersky Security Center obtient les adresses et les noms de tous les appareils détectés sur le réseau. Ensuite, vous pouvez installer à l'aide de Kaspersky Security Center des applications de Kaspersky et d'autres éditeurs sur les appareils détectées. Kaspersky Security Center lance la recherche d'appareils régulièrement. Par conséquent, si de nouveaux appareils apparaissent sur le réseau, ils seront détectés automatiquement.

2. **Installation de l'Agent d'administration et des applications de sécurité sur les appareils du réseau**

   Le déploiement de la protection (Configuration de la protection sur le réseau d'une entreprise cliente, Scénario de configuration de la protection réseau) sur le réseau d'une entreprise suppose l'installation de l'Agent d'administration et des applications de sécurité (par exemple, Kaspersky Endpoint Security) sur les appareils qui ont été détectés par le Serveur d'administration lors de la recherche d'appareils.

   Les applications de sécurité protègent les appareils contre les virus et / ou d'autres applications présentant la menace. L'Agent d'administration assure le lien entre l'appareil et le Serveur d'administration. Les paramètres de l'Agent d'administration sont automatiquement configurés par défaut.

   Si vous le souhaitez, vous pouvez installer l'Agent d'administration en mode silencieux avec un fichier de réponses ou sans fichier de réponses.

   Avant d'installer l'Agent d'administration et les applications de sécurité sur les appareils du réseau, confirmez la disponibilité de ces appareils (ils sont activés). Vous pouvez installer Agent d'administration sur les machines virtuelles ainsi que sur les appareils physiques.

   Il est possible d'installer une application de sécurité et l'Agent d'administration à distance ou localement.

Installation à distance : l'Assistant de déploiement de la protection permet d'installer à distance une application de sécurité (par exemple, Kaspersky Endpoint Security for Windows) et l'Agent d'administration sur les appareils dotés d'un Serveur d'administration détectés dans le réseau de l'organisation. En temps normal, la tâche d'installation à distance déploie la protection sur la majorité des appareils en réseau. Toutefois, elle peut recevoir une erreur de certains appareils si, par exemple, un appareil est éteint u n'est pas accessible pour une raison quelconque. Dans ce cas, il est recommandé de se connecter manuellement à l'appareil et utiliser l'installation locale.

Installation locale : utilisée sur les appareils du réseau où le déploiement de la protection via une tâche d'installation à distance a échoué. Pour installer la protection sur de tels appareils, créez le paquet d'installation autonome à lancer sur ces appareils localement.

L'installation de l'Agent d'administration sur des appareils fonctionnant sous Linux et macOS est décrite dans la documentation de Kaspersky Endpoint Security for Linux et Kaspersky Endpoint Security for Mac, respectivement. Malgré le fait que les appareils sous les systèmes d'exploitation Linux et macOS soient considérés comme moins vulnérables que les appareils sous Windows, il est également recommandé d'installer des applications de sécurité sur ces appareils.

Après l'installation, assurez-vous que l'application de sécurité est installée sur les appareils administrés. Lancez pour cela le Rapport sur les versions des applications de Kaspersky et prenez connaissance de ses résultats.

3. **Diffusion des clés de licence sur les appareils clients**

   Diffusez les clés de licence sur les appareils client pour activer les applications de sécurité administrées sur ces appareils.

4. **Configuration de la protection des appareils mobiles**

   Cette étape se trouve dans l'Assistant de configuration initiale de l'application.

   Si vous souhaitez gérer les appareils mobiles d'entreprise, suivez les étapes nécessaires pour préparer et déployer l'Administration des appareils mobiles.

5. **Création de la structure des groupes d'administration**

   Dans certains cas, pour garantir le déploiement optimal de la protection sur les appareils du réseau, il faut répartir les appareils en groupes d'administration en tenant compte de la structure organisationnelle de la société. Vous pouvez créer des règles de déplacement pour la répartition des appareils par groupes ou répartir manuellement les appareils. Il est possible d'assigner des tâches de groupe aux groupes d'administration, de définir la zone d'action des stratégies et d'assigner les points de distribution.

   Assurez-vous que tous les appareils administrés sont correctement répartis entre les groupes d'administration correspondants et que tous les appareils ont bien été définis.

6. **Assignation des points de distribution**

   Kaspersky Security Center attribue points de distribution aux groupes d'administration automatiquement, mais vous pouvez les affecter manuellement, si nécessaire. Il est recommandé d'utiliser les points de distribution dans les grands réseaux afin de réduire la charge sur le Serveur d'administration, ainsi que dans les réseaux à structure distribuée afin d'octroyer au Serveur d'administration un accès aux appareils ou aux groupes d'appareils reliés par des canaux à faible bande passante. Vous pouvez utiliser des appareils fonctionnant sous Linux comme points de distribution ainsi que des appareils fonctionnant sous Windows.

Ports utilisés par Kaspersky Security Center

Les tableaux ci-dessous indiquent les ports par défaut utilisés par les Serveurs d'administration et par les appareils clients. Si vous le souhaitez, vous pouvez modifier les numéros de port par défaut.

Si vous installez le Serveur d'administration et la base de données sur des appareils différents, vous devez mettre à disposition les ports nécessaires sur l'appareil où se trouve la base de données (par exemple, le port 3306 pour le serveur MySQL Server, le port 1433 pour Microsoft SQL Server ou le port 5432 pour PostgreSQL et Postgres Pro). Veuillez vous référer à la documentation du SGBD pour les informations pertinentes.

Ports utilisés par le Serveur d'administration

Numéro de port	Nom du processus qui a ouvert le port	Protocole	Destination du port	Zone de fonctionnement
8060	klcsweb	TCP	Transfert des paquets d'installation publiés aux appareils client.	Publication des paquets d'installation. Vous pouvez modifier le numéro de port par défaut dans la section **Serveur Web** de la fenêtre des propriétés du Serveur d'administration dans la Console d'administration ou dans Kaspersky Security Center Web Console. Ce port est facultatif. Pour des raisons de sécurité, nous vous recommandons d'utiliser le port TCP 8061.
8061	klcsweb	TCP (TLS)	Transfert des paquets d'installation publiés aux appareils client.	Publication des paquets d'installation. Vous pouvez modifier le numéro de port par défaut dans la section **Serveur Web** de la fenêtre des propriétés du Serveur d'administration dans la Console d'administration ou dans Kaspersky Security Center Web Console.
13000	klserver	TCP (TLS)	Réception des connexions des Agents d'administration et des Serveurs d'administration secondaires : intervient également sur les Serveurs d'administration secondaires pour recevoir les connexions du Serveur d'administration principal (par exemple, le Serveur d'administration secondaire se trouve dans la zone démilitarisée)	Administration des appareils client et des Serveurs d'administration secondaires. Vous pouvez modifier le numéro du port par défaut pour recevoir les connexions des Agents d'administration lors de la configuration des ports de connexion ; vous pouvez modifier le nombre de ports par défaut pour recevoir les connexions des Serveurs d'administration secondaires lors de la création d'une hiérarchie de Serveurs d'administration dans la Console d'administration ou dans Kaspersky Security Center Web Console.
13000	klserver	UDP	Réception des informations des Agents d'administration sur l'arrêt des appareils	Administration des appareils clients. Vous pouvez modifier le numéro de port par défaut dans les paramètres de stratégie de l'Agent d'administration dans la Console d'administration ou dans Kaspersky Security Center Web Console.
13291	klserver	TCP (TLS)	Réception des connexions de la Console d'administration au Serveur d'administration	Administration du Serveur d'administration. Vous pouvez modifier le numéro de port par défaut dans la fenêtre des propriétés du Serveur d'administration de la Console d'administration.
13299	klserver	TCP (TLS)	Réception des connexions de la Kaspersky Security Center Web Console au Serveur d'administration ; Réception des connexions au Serveur d'administration via OpenAPI	Tutoriel de Kaspersky Security Center Web Console, OpenAPI. Vous pouvez modifier le numéro de port par défaut dans la fenêtre des propriétés du Serveur d'administration (section **Paramètres de connexion au Serveur d'administration** → sous-section **Ports de connexion**) dans la Console d'administration, ou lors de la création d'une hiérarchie de Serveurs d'administration dans la Console d'administration ou dans Kaspersky Security Center Web Console.
14000	klserver	TCP	Réception des connexions des Agents d'administration	Administration des appareils clients. Vous pouvez modifier le numéro de port par défaut lors de la configuration des ports de connexion lors de l'installation de Kaspersky Security Center ou lors de la connexion manuelle d'un appareil client au Serveur d'administration. Ce port est facultatif. Pour des raisons de sécurité, nous vous recommandons d'utiliser le port TCP 1300.
13111 (uniquement si le service KSN Proxy est exécuté sur l'appareil)	ksnproxy	TCP	Réception des requêtes des appareils administrés au serveur proxy KSN	Serveur proxy KSN. Vous pouvez modifier le numéro de port par défaut dans la fenêtre des propriétés du Serveur d'administration.

Numéro de port	Nom du processus qui a ouvert le port	Protocole	Destination du port	Zone de fonctionnement
15111 (uniquement si le service KSN Proxy est exécuté sur l'appareil)	ksnproxy	UDP	Réception des requêtes des appareils administrés au serveur proxy KSN	Serveur proxy KSN. Vous pouvez modifier le numéro de port par défaut dans la fenêtre des propriétés du Serveur d'administration.
17000	klactprx	TCP (TLS)	Réception des connexions pour l'activation de l'application depuis les appareils administrés (sauf les appareils mobiles)	Serveur proxy d'activation utilisé par les appareils non mobiles pour activer les applications Kaspersky avec des codes d'activation. Vous pouvez modifier le numéro de port par défaut dans la fenêtre des propriétés du Serveur d'administration.
17100 (uniquement si vous administrez des appareils mobiles)	klactprx	TCP (TLS)	Réception des connexions pour l'activation de l'application depuis les appareils mobiles	Serveur proxy d'activation pour les appareils mobiles. Vous pouvez modifier le numéro de port par défaut dans la fenêtre des propriétés du Serveur d'administration.
19170	klserver	HTTPS (TLS)	Connexion en tunnel aux appareils administrés à l'aide de l'utilitaire klsctunnel	Connexion à distance aux appareils administrés à l'aide de Kaspersky Security Center Web Console. Vous pouvez modifier le numéro de port par défaut uniquement dans la fenêtre des propriétés du Serveur d'administration (section **Paramètres de connexion au Serveur d'administration** → sous-section **Ports de connexion** → **option Ouvrir le port RDP pour Kaspersky Security Center Web Console**).
13292 (uniquement si vous administrez des appareils mobiles)	klserver	TCP (TLS)	Réception des connexions des appareils mobiles	Administration des appareils mobiles. Vous pouvez modifier le numéro de port par défaut dans la fenêtre des propriétés du Serveur d'administration de la Console d'administration ou de Kaspersky Security Center Web Console.
13294 (uniquement si vous administrez des appareils mobiles)	klserver	TCP (TLS)	Réception des connexions des appareils protégés au niveau UEFI	Administration des appareils client protégés au niveau UEFI. Vous pouvez modifier le numéro de port par défaut lors de la connexion d'appareils mobiles, ou ultérieurement dans la fenêtre des propriétés du Serveur d'administration (section **Paramètres de connexion au Serveur d'administration** → sous-section **Ports de connexion**) dans la Console d'administration ou dans Kaspersky Security Center Web Console.
13296	klserver	TCP (TLS)	Publication des métriques de Kaspersky Security Center for Prometheus	La publication des métriques de Kaspersky Security Center qui seront ensuite obtenues par Prometheus. Vous pouvez consulter les métriques via le lien suivant : https://<`server_address`>:13296/metrics. Dans <`server_address`>, indiquez l'adresse IP ou le nom de domaine de votre Serveur d'administration. Vous pouvez modifier le numéro de port par défaut dans la fenêtre des propriétés du Serveur d'administration de la Console d'administration.
30522, 30523 (ports sur l'interface localhost)	klnagent	TCP	Réception des mises à jour des applications Kaspersky à partir du Serveur d'administration à l'aide du module FileTransferBridge	Appareil du Serveur d'administration qui reçoit les mises à jour des applications Kaspersky.

Le tableau ci-dessous indique le port utilisé par le serveur MDM iOS (uniquement si vous administrez des appareils mobiles).

Port utilisé par le serveur MDM iOS

Numéro de port	Nom du processus qui a ouvert le port	Protocole	Destination du port	Zone de fonctionnement
443	kliosmdmservicesrv	TCP (TLS)	Réception des connexions des appareils mobiles iOS	Administration des appareils mobiles. Vous pouvez modifier le numéro de port par défaut lors de l'installation du Serveur MDM iOS.

Le tableau ci-dessous indique le port utilisé par le Serveur de Kaspersky Security Center Web Console. Il peut s'agir du même appareil sur lequel le Serveur d'administration est installé ou d'un autre appareil.

Ports utilisés par le serveur de Kaspersky Security Center Web Console

Numéro de port	Nom du processus qui a ouvert le port	Protocole	Destination du port	Zone de fonctionnement
8080	Node.js : JavaScript côté serveur	TCP (TLS)	Réception des connexions du navigateur vers Kaspersky Security Center Web Console	Kaspersky Security Center Web Console. Vous pouvez modifier le numéro de port par défaut lors de l'installation de Kaspersky Security Center Web Console sur un appareil fonctionnant sous Windows ou sur une plateforme Linux. Si vous installez Kaspersky Security Center Web Console sur le système d'exploitation Linux ALT, vous devez préciser un numéro de port différent de 8080, car le port 8080 est utilisé par le système d'exploitation.

Le tableau ci-dessous indique le port utilisé par les appareils administrés sur lesquels l'Agent d'administration est installé.

Ports utilisés par l'Agent d'administration

Numéro de port	Nom du processus qui a ouvert le port	Protocole	Destination du port	Zone de fonctionnement
15000	klnagent	UDP	Signaux d'administration du Serveur d'administration ou du Point de distribution aux Agents d'administration	Administration des appareils clients. Vous pouvez modifier le numéro de port par défaut dans les paramètres de stratégie de l'Agent d'administration dans la Console d'administration ou dans Kaspersky Security Center Web Console.
15000	klnagent	Diffusion UDP	Collecte de données sur d'autres Agents d'administration dans le même domaine de diffusion (les données sont ensuite envoyées au Serveur d'administration)	Remise des mises à jour et des paquets d'installation.
15001	klnagent	UDP	Réception des demandes de multidiffusion d'un point de distribution (si utilisé)	Réception des mises à jour et des paquets d'installation à partir d'un point de distribution. Vous pouvez modifier le numéro de port par défaut dans la fenêtre des propriétés du point de distribution dans la Console d'administration ou dans Kaspersky Security Center Web Console.
30522, 30523 (ports sur l'interface localhost)	klnagent	TCP	Réception des mises à jour des applications Kaspersky à partir du Serveur d'administration à l'aide du module FileTransferBridge	Appareils administrés qui reçoivent les mises à jour des applications Kaspersky à partir du Serveur d'administration spécifié comme source de mise à jour des bases de données.
161	klnagent	SNMP	Surveillance et détection des appareils en réseau.	Découvrabilité des appareils.

Veuillez noter que le processus klnagent peut également demander des ports libres à partir de la plage de ports dynamique d'un système d'exploitation d'extrémité. Ces ports sont attribués automatiquement au processus klnagent par le système d'exploitation, de sorte que le processus klnagent peut utiliser certains ports qui sont utilisés par un autre logiciel. Si le processus klnagent affecte le fonctionnement de ce logiciel, modifiez les paramètres du port dans ce logiciel ou modifiez la plage de ports dynamique par défaut dans votre système d'exploitation pour exclure le port utilisé par le logiciel concerné.

Notez également que les recommandations sur la compatibilité de Kaspersky Security Center avec les logiciels tiers sont décrites à titre d'information uniquement et peuvent ne pas être applicables aux nouvelles versions des logiciels tiers. Les recommandations décrites pour la configuration des ports sont basées sur l'expérience du Support technique et sur nos meilleures pratiques.

Le tableau ci-dessous indique les ports utilisés par un appareil administré sur lequel l'Agent d'administration est installé et agit en tant que point de distribution. Les ports répertoriés sont utilisés par les appareils du point de distribution en plus des ports utilisés par les Agents d'administration (cf. tableau ci-dessus).

Ports utilisés par l'Agent d'administration fonctionnant comme point de distribution

Numéro de port	Nom du processus qui a ouvert le port	Protocole	Destination du port	Zone de fonctionnement
13000	klnagent	TCP (TLS)	Réception des connexions depuis les Agents d'administration et depuis Kaspersky Security Center quand le point de distribution agit comme passerelle de connexion dans la DMZ. Si un appareil avec le Serveur d'administration installé est défini comme point de distribution, le port 13001 est utilisé pour la connexion SSL par défaut au lieu de 13000.	Administration des appareils client, remise des mises à jour et des paquets d'installation. Pour plus de détails, voir la rubrique suivante : un Serveur d'administration, une passerelle de connexion dans un segment du réseau et un appareil client. Vous pouvez modifier le numéro de port par défaut dans la fenêtre des propriétés du point de distribution dans la Console d'administration ou dans Kaspersky Security Center Web Console.
13111 (uniquement si le service KSN Proxy est exécuté sur l'appareil)	ksnproxy	TCP	Réception des requêtes des appareils administrés au serveur proxy KSN	Serveur proxy KSN. Vous pouvez modifier le numéro de port par défaut dans la fenêtre des propriétés du point de distribution dans la Console d'administration ou dans Kaspersky Security Center Web Console.
15111 (uniquement si le service KSN Proxy est exécuté sur l'appareil)	ksnproxy	UDP	Réception des requêtes des appareils administrés au serveur proxy KSN	Serveur proxy KSN. Vous pouvez modifier le numéro de port par défaut dans la fenêtre des propriétés du point de distribution dans la Console d'administration ou dans Kaspersky Security Center Web Console.
17111 (uniquement si le service KSN Proxy est exécuté sur l'appareil)	ksnproxy	HTTPS	Réception des requêtes des appareils administrés au serveur proxy KSN	Serveur proxy KSN. Vous pouvez modifier le numéro de port par défaut dans la fenêtre des propriétés du point de distribution dans la Console d'administration ou dans Kaspersky Security Center Web Console.
13295 (uniquement si vous utilisez le point de distribution comme serveur push)	klnagent	TCP (TLS)	Réception des connexions des appareils mobiles	Serveur push. Vous pouvez modifier le numéro de port par défaut dans la fenêtre des propriétés du point de distribution dans la Console d'administration ou dans Kaspersky Security Center Web Console.

Le tableau ci-dessous indique les ports utilisés par un contrôleur de domaine.

Ports utilisés par un contrôleur de domaine

Numéro de port	Protocole	Destination du port	Zone de fonctionnement
389	LDAP sur TCP ou UDP	Connexion à un serveur LDAP	Sondage du contrôleur de domaine
636	LDAP sur TLS	Connexion à un serveur LDAP	Sondage du contrôleur de domaine

Certificats pour l'utilisation de Kaspersky Security Center

Cette section contient des informations sur les certificats de Kaspersky Security Center et décrit comment émettre un certificat personnalisé pour le Serveur d'administration.

À propos des certificats de Kaspersky Security Center

Kaspersky Security Center utilise les types de certificats suivants pour permettre une interaction sécurisée entre les modules de l'application :

- Certificat du Serveur d'administration
- Certificat mobile
- Certificat du serveur MDM iOS
- Certificat de serveur Web de Kaspersky Security Center
- Certificat de Kaspersky Security Center Web Console

Par défaut, Kaspersky Security Center utilise des certificats auto-signés (c'est-à-dire émis par Kaspersky Security Center lui-même), mais vous pouvez les remplacer par des certificats personnalisés pour mieux répondre aux exigences du réseau de votre organisation et respecter les normes de sécurité. Une fois que le Serveur d'administration a vérifié si un certificat personnalisé répond à toutes les exigences applicables, ce certificat a la même zone de fonction qu'un certificat auto-signé. La seule différence réside dans le fait qu'un certificat personnalisé n'est pas réémis automatiquement à son expiration. Vous remplacez les certificats par des certificats personnalisés à l'aide de l'utilitaire klsetsrvcert ou par la section des propriétés du Serveur d'administration dans la Console d'administration, en fonction du type de certificat. Lorsque vous utilisez l'utilitaire klsetsrvcert, vous devez spécifier un type de certificat à l'aide de l'une des valeurs suivantes :

- C—certificat commun pour les ports 13000 et 13291.
- CR—certificat commun de réserve pour les ports 13000 et 13291.
- M—certificat mobile pour le port 13292.
- MR—certificat mobile de réserve pour le port 13292.
- MCA—autorité de certification mobile pour les certificats utilisateur générés automatiquement.

> Vous n'avez pas besoin de télécharger l'utilitaire klsetsrvcert. Il figure dans le kit de distribution de Kaspersky Security Center. L'utilitaire n'est pas compatible avec les versions précédentes de Kaspersky Security Center.

La période de validité maximale des certificats du Serveur d'administration ne doit pas dépasser 397 jours.

Certificats du Serveur d'administration

Un certificat de Serveur d'administration est requis pour procéder à l'authentification du Serveur d'administration ainsi que pour assurer une interaction sécurisée entre le Serveur d'administration et l'Agent d'administration sur les appareils administrés ou entre le Serveur d'administration principal et les Serveurs d'administration secondaires. Lorsque vous connectez la Console d'administration au Serveur d'administration pour la première fois, vous êtes invité à confirmer l'utilisation du certificat actuel du Serveur d'administration. Une telle confirmation est également requise chaque fois que le certificat du Serveur d'administration est remplacé, après chaque réinstallation du Serveur d'administration et lors de la connexion d'un Serveur d'administration secondaire au Serveur d'administration principal. Ce certificat est appelé certificat commun ("C").

Le certificat commun ("C") est créé automatiquement lors de l'installation du module Serveur d'administration. Le certificat est composé de deux parties :

- fichier klserver.cer ; par défaut, il se trouve sur l'appareil où le module Serveur d'administration est installé dans le dossier C:\ProgramData\KasperskyLab\adminkit\1093\cert.

- Clé secrète située dans le Stockage protégé Windows.

Il existe également un certificat commun de réserve ("CR"). Kaspersky Security Center génère automatiquement ce certificat 90 jours avant l'expiration du certificat commun. Le certificat commun de réserve est ensuite utilisé pour remplacer facilement le certificat du Serveur d'administration. Lorsque le certificat commun est sur le point d'expirer, le certificat commun de réserve est utilisé pour maintenir la connexion avec les instances d'Agent d'administration installées sur les appareils administrés. Ainsi, le certificat commun de réserve remplace automatiquement le nouveau certificat commun 24 heures avant l'expiration de l'ancien certificat commun.

Vous pouvez également sauvegarder le certificat du Serveur d'administration séparément des autres paramètres du Serveur d'administration afin de déplacer le Serveur d'administration d'un appareil à un autre sans aucune perte de données.

Certificats mobiles

Un certificat mobile ("M") est requis pour assurer l'authentification du Serveur d'administration sur les appareils mobiles. Vous configurez l'utilisation du certificat mobile à l'étape dédiée de l'Assistant de configuration initiale de l'application.

Il existe également un certificat mobile de réserve ("MR") : il est utilisé pour remplacer facilement le certificat mobile. Kaspersky Security Center génère automatiquement ce certificat 60 jours avant l'expiration du certificat commun. Lorsque le certificat mobile est sur le point d'expirer, le certificat mobile de réserve est utilisé pour maintenir la connexion avec les instances d'Agent d'administration installées sur les appareils mobiles administrés. Ainsi, le certificat mobile de réserve remplace automatiquement le nouveau certificat mobile 24 heures avant l'expiration de l'ancien certificat mobile.

Si le scénario de connexion nécessite l'utilisation d'un certificat client sur les appareils mobiles (connexion impliquant une authentification SSL bidirectionnelle), vous pouvez générer ces certificats au moyen de l'autorité de certification pour les certificats utilisateur générés automatiquement ("MCA"). En outre, l'Assistant de configuration initiale de l'application vous permet de commencer à utiliser des certificats clients personnalisés émis par une autre autorité de certification, tandis que l'intégration avec l'infrastructure à clés publiques (PKI) de domaine de votre organisation vous permet d'émettre des certificats clients au moyen de votre autorité de certification de domaine.

Certificat du serveur MDM iOS

Un certificat de serveur MDM iOS est requis pour assurer l'authentification du Serveur d'administration sur les appareils mobiles fonctionnant sous le système d'exploitation iOS. L'interaction avec ces appareils est effectuée via le protocole d'administration des appareils mobiles Apple (MDM) qui n'implique aucun Agent d'administration. Au lieu de cela, vous installez un profil MDM iOS spécial, contenant un certificat client, sur chaque appareil, pour assurer une authentification SSL bidirectionnelle.

En outre, l'Assistant de configuration initiale de l'application vous permet de commencer à utiliser des certificats clients personnalisés émis par une autre autorité de certification, tandis que l'intégration avec l'infrastructure à clés publiques (PKI) de domaine de votre organisation vous permet d'émettre des certificats clients au moyen de votre autorité de certification de domaine.

Les certificats clients sont transmis aux appareils iOS lorsque vous téléchargez ces profils MDM iOS. Un certificat client du serveur MDM iOS est unique pour chaque appareil iOS administré. Vous générez tous les certificats clients du serveur MDM iOS au moyen de l'autorité de certification pour les certificats utilisateur générés automatiquement ("MCA").

Certificat de serveur Web de Kaspersky Security Center

Kaspersky Security Center Web Server (ci-après dénommé Serveur Web), un composant du Serveur d'administration de Kaspersky Security Center, utilise un type de certificat particulier. Ce certificat est requis pour la publication des paquets d'installation de l'Agent d'administration que vous téléchargez par la suite sur les appareils administrés, ainsi que pour la publication des profils MDM iOS, des applications iOS et des paquets d'installation de Kaspersky Security for Mobile. Pour cela, le Serveur Web peut utiliser différents certificats.

Si la prise en charge des appareils mobiles est désactivée, le Serveur Web utilise l'un des certificats suivants, par ordre de priorité :

1. Certificat de serveur Web personnalisé que vous avez précisé manuellement par la Console d'administration
2. Certificat commun du Serveur d'administration ("C")

Si la prise en charge des appareils mobiles est activée, le Serveur Web utilise l'un des certificats suivants, par ordre de priorité :

1. Certificat de serveur Web personnalisé que vous avez précisé manuellement par la Console d'administration
2. Certificat mobile personnalisé
3. Certificat mobile auto-signé ("M")
4. Certificat commun du Serveur d'administration ("C")

Certificat de Kaspersky Security Center Web Console

Kaspersky Security Center Web Console Server (ci-après Web Console) possède son propre certificat. Lorsque vous ouvrez un site, un navigateur vérifie si votre connexion est fiable. Le certificat de Web Console permet d'authentifier Web Console et sert à chiffrer le trafic entre un navigateur et Web Console.

Lorsque vous ouvrez Web Console, le navigateur peut vous informer que la connexion à Web Console n'est pas privée et que le certificat de Web Console n'est pas valide. Cet avertissement apparaît car le certificat de la Console Web est auto-signé et généré automatiquement par Kaspersky Security Center. Pour supprimer cet avertissement, vous pouvez effectuer une des actions suivantes :

- Remplacez le certificat de Web Console par un certificat personnalisé (option recommandée). Créez un certificat de confiance dans votre infrastructure et qui répond aux exigences des certificats personnalisés.
- Ajoutez le certificat de Web Console à la liste des certificats de navigateur de confiance. Nous vous recommandons d'utiliser cette option uniquement si vous ne pouvez pas créer de certificat personnalisé.

À propos du certificat du Serveur d'administration

Deux opérations sont effectuées en fonction du *Certificat du Serveur d'administration :* authentification du Serveur d'administration lors de la connexion par la Console d'administration et échange de données avec les appareils. Le certificat est utilisé pour l'authentification lorsque les Serveurs d'administration principaux sont connectés aux Serveurs d'administration secondaires.

Certificat émis par Kaspersky

Le certificat de Serveur d'administration est automatiquement créé en cours de l'installation du module Serveur d'administration et sauvegardé dans le dossier %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert.

Le certificat du Serveur d'administration est valable cinq ans si le certificat a été généré par le Serveur d'administration 12.2 ou antérieure. Dans le cas contraire, la durée de validité du certificat est limitée à 397 jours. Un nouveau certificat est généré par le Serveur d'administration sous forme de certificat de réserve 90 jours avant la date d'expiration du certificat en cours. Ensuite, le nouveau certificat remplace automatiquement le certificat en cours un jours avant sa date d'expiration. Tous les Agents d'administration sur les appareils clients sont reconfigurés automatiquement afin d'authentifier le Serveur d'administration à l'aide du nouveau certificat.

Certificats personnalisés

Le cas échéant, vous pouvez attribuer un certificat personnalisé au Serveur d'administration. Une telle mesure peut se justifier par l'amélioration de l'intégration avec la PKI en place de votre entreprise ou pour personnaliser la configuration des champs du certificat.

La période de validité maximale des certificats du Serveur d'administration ne doit pas dépasser 397 jours.

Lors du remplacement du certificat, tous les Agents d'administration déjà connectés au Serveur d'administration via SSL se déconnectent du Serveur avec l'erreur « Erreur d'authentification du Serveur d'administration ». Pour éliminer cette erreur, il faudra restaurer la connexion après le remplacement du certificat.

Dans le cas où le certificat du Serveur d'administration serait perdu, il est nécessaire pour le restaurer de réinstaller le module du Serveur d'administration, puis de restaurer les données.

Si vous ouvrez Kaspersky Security Center Web Console dans différents navigateurs et que vous téléchargez le fichier de certificat du Serveur d'administration dans la fenêtre des propriétés du Serveur d'administration, les fichiers téléchargés portent des noms différents.

Conditions requises pour les certificats personnalisés utilisés dans Kaspersky Security Center

Le tableau ci-dessous présente les conditions requises pour les certificats personnalisés définis pour les différents modules de Kaspersky Security Center.

Conditions requises pour les certificats de Kaspersky Security Center

Type de certificat	Conditions	Commentaires
Certificat commun, certificat de réserve commun ("C", "CR")	Longueur de clé minimale : 2 048. Contraintes de base : • Contrainte de longueur de chemin : aucune Utilisation des clés : • Signature numérique • Signature du certificat • Chiffrement de clé • Signature CRL Utilisation de clés étendues (facultatif) : authentification du serveur, authentification du client.	Le paramètre Utilisation de clés étendues est facultatif. La valeur Contrainte de longueur de chemin peut varier d'un nombre entier de "Aucune", mais ne peut pas être inférieure à 1.
Certificat mobile, certificat de réserve mobile ("M", "MR")	Longueur de clé minimale : 2 048. Contraintes de base : • Autorité de certification : vrai • Contrainte de longueur de chemin : aucune Utilisation des clés : • Signature numérique • Signature du certificat • Chiffrement de clé • Signature CRL Utilisation de clés étendues (facultatif) : authentification du serveur.	Le paramètre Utilisation de clés étendues est facultatif. La valeur Contrainte de longueur de chemin peut varier d'un nombre entier de "Aucune" si le certificat commun a une valeur Contrainte de longueur de chemin non inférieure à 1.
Certificat d'autorité de certification pour les certificats utilisateur générés automatiquement ("MCA")	Longueur de clé minimale : 2 048. Contraintes de base : • Autorité de certification : vrai • Contrainte de longueur de chemin : aucune Utilisation des clés : • Signature numérique • Signature du certificat • Chiffrement de clé • Signature CRL Utilisation de clés étendues (facultatif) : authentification du serveur, authentification du client.	Le paramètre Utilisation de clés étendues est facultatif. La valeur Contrainte de longueur de chemin peut varier d'un nombre entier de "Aucune" si le certificat commun a une valeur Contrainte de longueur de chemin non inférieure à 1.

Type de certificat	Conditions	Commentaires
Certificat du Serveur Web	Utilisation de clés étendues : authentification du serveur. Le conteneur PKCS #12 / PEM à partir duquel le certificat est indiqué comprend la chaîne entière de clés publiques. Le nom alternatif de l'objet (SAN) du certificat est présent, autrement dit, la valeur du champ `subjectAltName` est valide. Le certificat répond aux exigences réelles des navigateurs imposées aux certificats de serveur ainsi qu'aux exigences de base actuelles du Forum CA/Browser.	—
Certificat de Kaspersky Security Center Web Console	Le conteneur PEM à partir duquel le certificat est indiqué inclut la chaîne entière de clés publiques. Le nom alternatif de l'objet (SAN) du certificat est présent, autrement dit, la valeur du champ `subjectAltName` est valide. Le certificat répond aux exigences réelles des navigateurs imposées aux certificats de serveur ainsi qu'aux exigences de base actuelles du Forum CA/Browser.	Les certificats chiffrés ne sont pas pris en charge par Kaspersky Security Center Web Console.

Scénario : Spécifier le certificat personnalisé du Serveur d'administration

Vous pouvez attribuer le certificat personnalisé du Serveur d'administration, par exemple, pour une meilleure intégration avec l'infrastructure à clé publique (PKI) existante de votre entreprise ou pour une configuration personnalisée des champs du certificat. Il est conseillé de remplacer le certificat directement après l'installation du Serveur d'administration, avant la fin de l'Assistant de configuration initiale de l'application.

La période de validité maximale des certificats du Serveur d'administration ne doit pas dépasser 397 jours.

Prérequis

Les conditions suivantes doivent être remplies :

- Le nouveau certificat doit être créé au format PKCS#12 (par exemple, au moyen de l'ICP de l'entreprise).
- Pour le nouveau certificat, les exigences énumérées dans le tableau ci-dessous doivent être remplies.

  Dans le tableau ci-dessous, faites attention à la mention " CA: true ", qui signifie que le nouveau certificat doit être émis par une autorité de certification (CA) de confiance. Le nouveau certificat portant la mention " CA: true " doit inclure toute la chaîne de confiance et une clé privée, qui doit être stockée dans un fichier avec l'extension pfx ou p12.

  Conditions requises pour les certificats du Serveur d'administration

Type de certificat	Conditions
Certificat commun, certificat de réserve commun ("C", "CR")	Longueur de clé minimale : 2 048. Contraintes de base : • Contrainte de longueur de chemin : aucune La valeur Contrainte de longueur de chemin peut varier d'un nombre entier de "Aucune", mais ne peut pas être inférieure à 1. Utilisation des clés : • Signature numérique • Signature du certificat • Chiffrement de clé • Signature CRL Utilisation de clés étendues (EKU) : authentification du serveur, authentification du client. L'EKU est facultative, mais si votre certificat la contient, les données d'authentification du serveur et du client doivent être spécifiées dans l'EKU.
Certificat mobile, certificat de réserve mobile ("M", "MR")	Longueur de clé minimale : 2 048. Contraintes de base : • Autorité de certification : vrai • Contrainte de longueur de chemin : aucune La valeur Contrainte de longueur de chemin peut varier d'un nombre entier de "Aucune" si le certificat commun a une valeur Contrainte de longueur de chemin non inférieure à 1. Utilisation des clés : • Signature numérique • Signature du certificat • Chiffrement de clé • Signature CRL Utilisation de clés étendues (EKU) : authentification du serveur. L'EKU est facultative, mais si votre certificat la contient, les données d'authentification du serveur doivent être spécifiées dans l'EKU.
Certificat d'autorité de certification pour les certificats utilisateur générés automatiquement ("MCA")	Longueur de clé minimale : 2 048. Contraintes de base : • Autorité de certification : vrai • Contrainte de longueur de chemin : aucune La valeur Contrainte de longueur de chemin peut varier d'un nombre entier de "Aucune" si le certificat commun a une valeur Contrainte de longueur de chemin non inférieure à 1. Utilisation des clés : • Signature numérique • Signature du certificat • Chiffrement de clé • Signature CRL Utilisation de clés étendues (EKU) : authentification du serveur. L'EKU est facultative, mais si votre certificat la contient, les données d'authentification du client doivent être spécifiées dans l'EKU.

Les certificats émis par une autorité de certification publique ne disposent pas de l'autorisation de signature de certificat. Pour utiliser ces certificats, assurez-vous d'avoir installé la version 13 ou supérieure de l'Agent d'administration sur les points de distribution ou les passerelles de connexion de votre réseau. Sinon, vous ne pourrez pas utiliser de certificats sans l'autorisation de signature.

Étapes

La spécification du certificat du Serveur d'administration se déroule par étapes :

1. **Remplacement du certificat du Serveur d'administration**

   Utiliser la ligne de commande utilitaire klsetsrvcert dans ce but.

2. **Spécification d'un nouveau certificat et rétablissement de la connexion des Agents d'administration au Serveur d'administration**

   Lors du remplacement du certificat, tous les Agents d'administration déjà connectés au Serveur d'administration via SSL se déconnectent du Serveur avec l'erreur "Erreur d'authentification du Serveur d'administration". Pour désigner le nouveau certificat et rétablir la connexion, utilisez la ligne ce commande utilitaire klmover.

3. **Spécification d'un nouveau certificat dans les paramètres de Kaspersky Security Center Web Console**

   Après que vous avez remplacé le certificat, renseignez-le dans les paramètres de Kaspersky Security Center Web Console. Sinon, Kaspersky Security Center Web Console ne pourra pas se connecter au serveur d'administration.

Résultats

Lorsque vous avez terminé le scénario, le certificat du Serveur d'administration est remplacé et le serveur est authentifié par les Agents d'administration sur les appareils administrés.

Remplacement du certificat du Serveur d'administration à l'aide de l'utilitaire klsetsrvcert

Pour remplacer le certificat du Serveur d'administration, procédez comme suit :

Dans la ligne de commande, exécutez l'utilitaire suivant :

```
klsetsrvcert [-t <type de certificat> {-i <chemin vers le nouveau certificat> [-p <mot de passe>] [-o <paramètres>] | -g <nom DNS>}][-f <temps de remplacement>][-r <certificats racines>][-l <chemin du fichier journal>]
```

Vous n'avez pas besoin de télécharger l'utilitaire klsetsrvcert. Il figure dans le kit de distribution de Kaspersky Security Center. Il n'est pas compatible avec les versions précédentes de Kaspersky Security Center.

La description des paramètres de l'utilitaire klsetsrvcert est présentée dans le tableau ci-dessous.

Valeurs des paramètres de l'utilitaire klsetsrvcert

Paramètre	Valeur
`-t < type de certificat >`	Le type de certificat à remplacer. Valeurs possibles du paramètre `< type de certificat >` : • `C` : remplacer le certificat commun pour les ports 13000 et 13291. • `CR` : remplacer le certificat de réserve commun pour les ports 13000 et 13291. • `M` : remplacer le certificat pour les appareils mobiles du port 13292. • `MR` : remplacer le certificat mobile de réserve pour le port 13292. • `MCA` : autorité de certification de client mobile pour les certificats utilisateur générés automatiquement.
`-f < temps de remplacement >`	Calendrier de changement de certificat, format "JJ-MM-AAAA hh:mm" (pour les ports 13000 et 13291). Utilisez ce paramètre si vous souhaitez remplacer le certificat commun par le certificat commun de réserve avant l'expiration du certificat commun. Spécifiez l'heure à laquelle les appareils administrés doivent se synchroniser avec le Serveur d'administration sur un nouveau certificat.
`-i < chemin vers le nouveau certificat >`	Le conteneur où se trouve le certificat et une clé privée au format PKCS#12 (fichier avec extension .p12 ou .pfx).
`-p < mot de passe >`	Le mot de passe qui protège le conteneur p12. Le certificat et une clé privée sont stockés dans le conteneur, par conséquent, le mot de passe est requis pour déchiffrer le fichier avec le conteneur.
`-o < paramètres de validation >`	Paramètres de validation du certificat (séparés par des points-virgules). Pour utiliser un certificat personnalisé sans autorisation de signature, spécifiez `-o NoCA` dans l'utilitaire klsetsrvcert. Ceci est utile pour les certificats émis par une autorité de certification publique. Pour modifier la longueur de la clé de chiffrement pour les certificats de type C ou CR, spécifiez `-o RsaKeyLen: < longueur de clé >` dans l'utilitaire klsetsrvcert, où le paramètre `< longueur de clé >` correspond à la valeur de la longueur de clé requise. Sinon, la longueur de clé actuelle du certificat est utilisée.
`-g < nom DNS >`	Un certificat est créé pour le nom DNS indiqué.
`-r < certificats racine >`	Liste des autorités de certification racine de confiance, format PEM.
`-l < chemin du fichier journal >`	Le fichier contenant les résultats. Par défaut l'affichage se réalise dans le flux standard d'affichage.

Par exemple, pour spécifier le certificat personnalisé du Serveur d'administration, utilisez la commande suivante :

```
klsetsrvcert -t C -i <chemin vers le nouveau certificat> -p <mot de passe> -o NoCA
```

Une fois le certificat remplacé, tous les Agents d'administration connectés au Serveur d'administration via SSL perdent leur connexion. Pour la restaurer, utilisez la ligne de commande utilitaire klmover.

Pour éviter de perdre les connexions des Agents d'administration, utilisez la commande suivante :

1. Pour installer le nouveau certificat,

   ```
   klsetsrvcert.exe -t CR -i <chemin vers le nouveau certificat> -p <mot de passe> -o NoCA
   ```

2. Pour préciser la date d'application du nouveau certificat,

   ```
   klsetsrvcert.exe -f "DD-MM-YYYY hh:mm"
   ```

où "`DD-MM-YYYY hh:mm`" est la date 3 à 4 semaines plus tard que la date actuelle. Le décalage horaire nécessaire au remplacement du certificat par le nouveau permettra au nouveau certificat d'être distribué à tous les Agents d'administration.

Connexion des Agents réseau au Serveur d'administration à l'aide de l'utilitaire klmover

Après avoir remplacé le certificat du Serveur d'administration à l'aide de la ligne de commande utilitaire klsetsrvcert, vous devez établir la connexion SSL entre les Agents d'administration et le Serveur d'administration car la connexion est interrompue.

Pour indiquer le nouveau certificat du Serveur d'administration et restaurer la connexion, procédez comme suit :

Dans la ligne de commande, exécutez l'utilitaire suivant :

```
klmover [-address <adresse du serveur>] [-pn <numéro de port>] [-ps <numéro de port SSL>] [-nossl] [-cert <chemin vers le fichier du certificat>]
```

Les droits d'administrateur sont requis pour exécuter l'utilitaire.

Cet utilitaire est automatiquement copié dans le dossier d'installation de l'Agent d'administration lorsque l'Agent d'administration est installé sur un appareil client.

Pour éviter que des intrus ne puissent déplacer des appareils hors du contrôle de votre Serveur d'administration, nous vous recommandons vivement d'activer la protection par mot de passe pour le lancement de l'utilitaire klmover. Pour activer la protection par mot de passe, sélectionnez l'option **Utiliser un mot de passe de désinstallation** dans les paramètres de stratégie de l'Agent d'Administration.

L'utilitaire klmover requiert des droits d'administrateur local. La protection par mot de passe pour le fonctionnement de l'utilitaire klmover peut être omise pour les appareils administrés sans les droits d'administrateur local.

L'activation de l'option **Utiliser un mot de passe de désinstallation** active également la protection par un mot de passe du nettoyage (cleaner.exe).

Vous ne pouvez pas utiliser l'utilitaire klmover pour les appareils clients connectés au Serveur d'administration via des passerelles de connexion. Pour de tels appareils, vous devez soit reconfigurer l'Agent d'administration, soit réinstaller l'Agent d'administration et indiquer la passerelle de connexion.

La description des paramètres de l'utilitaire klmover est présentée dans le tableau ci-dessous.

Valeurs des paramètres de l'utilitaire klmover

Paramètre	Valeur
`-address <adresse du serveur>`	Adresse du Serveur d'administration pour la connexion. Vous pouvez spécifier une adresse IP, un nom NetBIOS ou un nom DNS.
`-pn <numéro de port>`	Numéro de port à utiliser pour une connexion non sécurisée au Serveur d'administration. Le numéro de port par défaut est 14000.
`-ps <numéro de port SSL>`	Numéro de port SSL à utiliser pour une connexion sécurisée au Serveur d'administration sous protocole SSL. Le numéro de port par défaut est 13000.

Paramètre	Valeur
`-nossl`	Utilise une connexion non sécurisée au Serveur d'administration. Si aucune clé n'est utilisée, la connexion de l'Agent d'administration au Serveur d'administration est établie à l'aide du protocole sécurisé SSL.
`-cert < chemin d'accès au fichier de certificat >`	Utilise le fichier de certificat spécifié pour l'authentification, afin d'accéder au Serveur d'administration.
`-virtserv`	Nom du Serveur d'administration virtuel.
`-cloningmode`	Mode de clonage du disque de l'Agent d'administration Utilisez l'un des paramètres suivants pour configurer le mode de clonage du disque : • `-cloningmode` : demande l'état du mode de clonage du disque. • `-cloningmode 1` : active le mode de clonage du disque. • `-cloningmode 0` : désactive le mode de clonage du disque.
`-nauninstpwd < mot de passe >`	Utilisez ce paramètre pour spécifier le mot de passe de désinstallation de l'Agent d'administration. Ce paramètre n'est pas obligatoire.

Par exemple, pour connecter l'Agent d'administration au Serveur d'administration, exécutez la commande suivante :

```
klmover -address kscserver.mycompany.com -logfile klmover.log
```

Réémettre le certificat du Serveur Web

Le certificat de serveur Web utilisé dans Kaspersky Security Center est requis pour la publication des paquets d'installation de l'Agent d'administration que vous téléchargez ensuite sur les appareils administrés, ainsi que pour la publication des profils MDM iOS, des applications iOS et des paquets d'installation de Kaspersky Endpoint Security for Mobile. En fonction de la configuration actuelle de l'application, différents certificats peuvent faire office de certificat de serveur Web (pour plus de détails, voir À propos des certificats de Kaspersky Security Center).

Vous devrez peut-être réémettre le certificat de serveur Web pour satisfaire aux exigences en termes de sécurité propres à votre organisation ou pour maintenir une connexion continue de vos appareils administrés avant de commencer à mettre à niveau l'application. Kaspersky Security Center propose deux méthodes pour réémettre le certificat du serveur Web ; le choix entre elles dépend de la connexion d'appareils mobiles et de leur administration via le protocole mobile (c'est-à-dire avec le certificat mobile).

Si vous n'avez jamais spécifié votre propre certificat personnalisé comme certificat de serveur Web dans la section **Serveur Internet** de la fenêtre des propriétés du Serveur d'administration, le certificat mobile fait office de certificat du serveur Web. Dans ce cas, la réémission du certificat du serveur Web s'effectue via celle du protocole mobile lui-même.

Pour réémettre le certificat du serveur Web lorsque vous n'avez aucun appareil mobile administré via le protocole mobile :

1. dans l'arborescence de la console, cliquez avec le bouton droit sur le nom du Serveur d'administration concerné et dans le menu contextuel, sélectionnez **Propriétés**.

2. Dans la fenêtre des propriétés du Serveur d'administration qui s'ouvre, dans le volet de gauche, sélectionnez la section **Paramètres de connexion au Serveur d'administration**.

3. Dans la liste des sous-sections, sélectionnez **Certificats**.

4. Si vous prévoyez de continuer à utiliser le certificat émis par Kaspersky Security Center, procédez comme suit :

   a. Dans le volet droit, dans le groupe de paramètres de l'**Authentification du Serveur d'administration par les appareils mobiles**, sélectionnez l'option **Le certificat a été émis via le Serveur d'administration** puis cliquez sur le bouton **Réémettre**.

   b. Dans la fenêtre **Réémettre le certificat** qui s'ouvre, dans les groupes de paramètres **Adresse de connexion** et **Délai d'activation**, sélectionnez les options appropriées puis cliquez sur **OK**.

   c. Dans la fenêtre de confirmation, cliquez sur **Oui**.

   Lorsque vous prévoyez d'utiliser votre propre certificat personnalisé, procédez comme suit :

   a. assurez-vous que votre certificat personnalisé satisfait aux exigences de Kaspersky Security Center, ainsi qu'à celles applicables aux certificats approuvés par Apple. S'il y a lieu, modifiez le certificat.

   b. Sélectionnez l'option **Autre certificat**, puis cliquez sur le bouton **Parcourir**.

   c. Dans la fenêtre **Certificat** qui s'ouvre alors, dans le **Type de certificat**, sélectionnez le type de votre certificat, puis spécifiez l'emplacement et les paramètres du certificat :

      - si vous avez sélectionné **Conteneur PKCS#12**, cliquez sur le bouton **Parcourir** à côté du **Fichier du certificat** puis spécifiez le fichier de certificat sur votre disque dur. Si le fichier de certificat est protégé par mot de passe, entrez le mot de passe dans le champ **Mot de passe (s'il existe)**.

      - Si vous avez sélectionné **Certificat X.509**, cliquez sur le bouton **Parcourir** à côté du champ **Clé privée (.prk, .pem)** et spécifiez la clé privée sur votre disque dur. Si la clé privée est protégée par mot de passe, saisissez le mot de passe dans le champ **Mot de passe (s'il existe)**. Cliquez ensuite sur le bouton **Parcourir** à côté du champ **Clé publique (.cer)** et spécifiez la clé privée sur votre disque dur.

   d. Dans la fenêtre **Certificat**, cliquez sur **OK**.

   e. Dans la fenêtre de confirmation, cliquez sur **Oui**.

   Le certificat mobile est réémis pour être utilisé comme certificat de serveur Web.

Pour réémettre le certificat de serveur Web lorsque des appareils mobiles sont administrés via le protocole mobile :

1. générez votre certificat personnalisé et préparez-le pour l'utiliser dans Kaspersky Security Center. assurez-vous que votre certificat personnalisé satisfait aux exigences de Kaspersky Security Center, ainsi qu'à celles applicables aux certificats approuvés par Apple. S'il y a lieu, modifiez le certificat.

   > Vous pouvez utiliser l'utilitaire kliossrvcertgen.exe pour la génération de certificats.

2. dans l'arborescence de la console, cliquez avec le bouton droit sur le nom du Serveur d'administration concerné et dans le menu contextuel, sélectionnez **Propriétés**.

3. Dans la fenêtre des propriétés du Serveur d'administration qui s'ouvre, dans le volet de gauche, sélectionnez la section **Serveur Internet**.

4. Dans le menu **Par le protocole HTTPS**, sélectionnez l'option **Définir un autre certificat**.

5. Dans le menu **Par le protocole HTTPS**, cliquez sur le bouton **Modifier**.

6. Dans la fenêtre **Certificat** qui s'ouvre, sélectionnez dans le **Type de certificat** champ le type de votre certificat :

   - si vous avez sélectionné **Conteneur PKCS#12**, cliquez sur le bouton **Parcourir** à côté du **Fichier du certificat** puis spécifiez le fichier de certificat sur votre disque dur. Si le fichier de certificat est protégé par mot de passe, entrez le mot de passe dans le champ **Mot de passe (s'il existe)**.

   - Si vous avez sélectionné **Certificat X.509**, cliquez sur le bouton **Parcourir** à côté du champ **Clé privée (.prk, .pem)** et spécifiez la clé privée sur votre disque dur. Si la clé privée est protégée par mot de passe, saisissez le mot de passe dans le champ **Mot de passe (s'il existe)**. Cliquez ensuite sur le bouton **Parcourir** à côté du champ **Clé publique (.cer)** et spécifiez la clé privée sur votre disque dur.

7. Dans la fenêtre **Certificat**, cliquez sur **OK**.

8. Si nécessaire, dans la fenêtre des propriétés du Serveur d'administration, dans le champ **Port HTTPS du serveur Internet**, modifiez le numéro du port HTTPS pour le serveur Web. Cliquez sur le bouton **OK**.

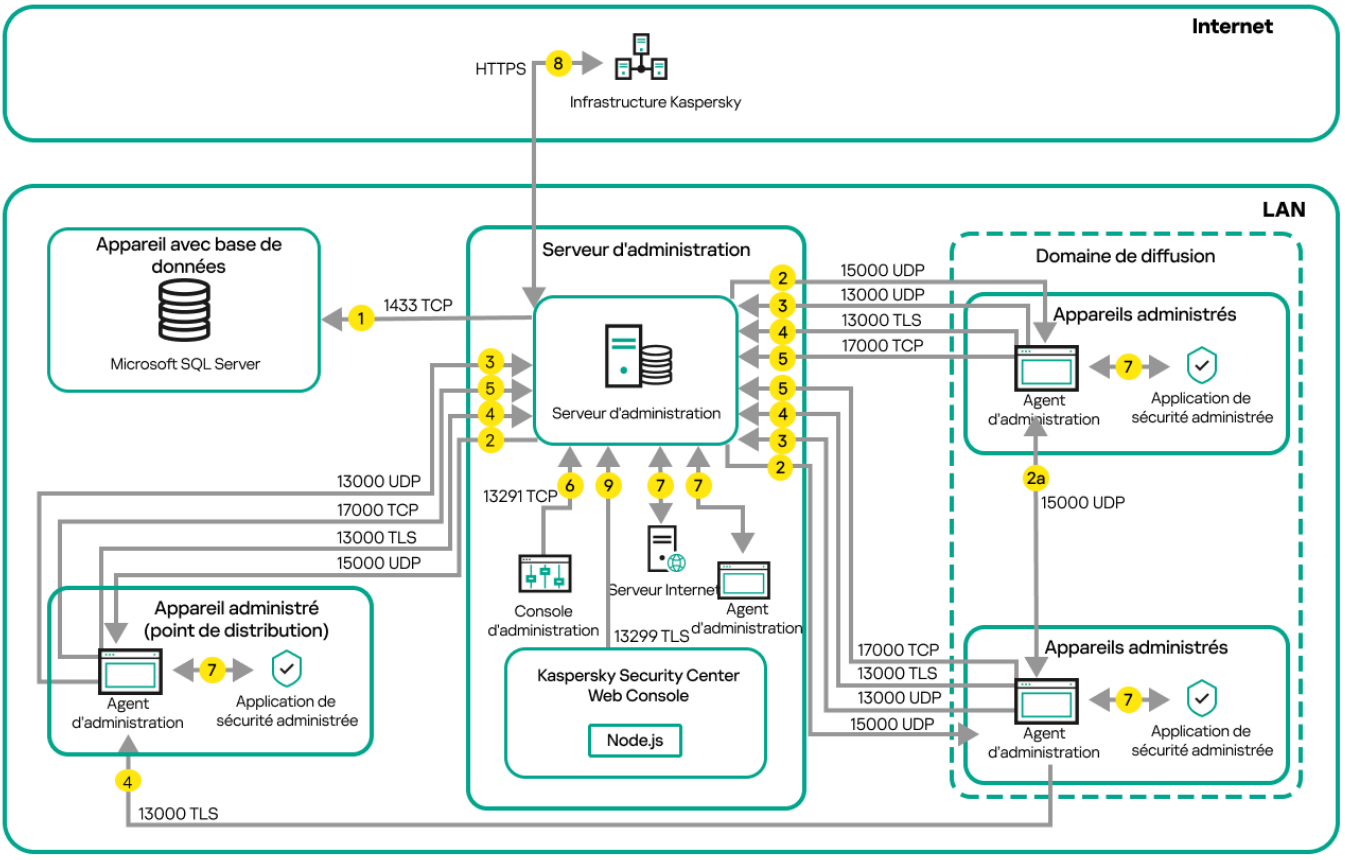
   Le certificat du serveur Web est réémis.

Schémas pour le trafic de données et l'utilisation du port

Cette section présente des schémas pour le trafic de données entre les modules de Kaspersky Security Center, les applications de sécurité administrées et les serveurs externes sous différentes configurations. Les schémas fournis indiquent les numéros des ports qui doivent être disponibles sur les appareils locaux.

Serveur d'administration et appareils administrés sur le LAN

La figure ci-dessous montre le trafic des données si Kaspersky Security Center n'est déployé que sur un réseau local (LAN).



Serveur d'administration et appareils administrés sur un réseau local (LAN)

La figure montre comment les différents appareils administrés se connectent au Serveur d'administration de plusieurs façons : directement ou via un point de distribution. Les points de distribution réduisent la surcharge sur le Serveur d'administration lors de la diffusion des mises à jour et optimisent le trafic sur le réseau. Cependant, les points de distribution ne sont nécessaires que si le nombre d'appareils administrés est assez grand. S'il y a peu d'appareils administrés, ils peuvent tous recevoir directement les mises à jour du Serveur d'administration.

Les flèches indiquent l'ouverture du trafic : chaque flèche relie l'appareil qui initie la connexion à celui qui " répond " à l'appel. Le numéro du port et le nom du protocole utilisés pour le transfert de données sont fournis. Chaque flèche porte une étiquette numérique et les informations sur le trafic de données sont :

1. Le Serveur d'administration envoie des données à la base de données. Si vous installez le Serveur d'administration et la base de données sur des appareils différents, vous devez mettre à disposition les ports nécessaires sur l'appareil où se trouve la base de données (par exemple, le port 3306 pour MySQL Server ou le port 1433 pour Microsoft SQL Server). Veuillez vous référer à la documentation du SGBD pour les informations pertinentes.

2. Les demandes de communication du Serveur d'administration sont transférés à tous les appareils non mobiles administrés par le port UDP 15000.

   Les Agents d'administration s'envoient des requêtes entre eux au sein d'un domaine de diffusion. Les données sont ensuite envoyées au Serveur d'administration et sont utilisées pour définir les limites du domaine de diffusion et pour l'attribution automatique des points de distribution (si cette option est activée).

   Si le Serveur d'administration n'a pas d'accès direct aux appareils administrés, les requêtes de communication du Serveur d'administration vers ces appareils ne sont pas envoyées directement.

3. Les informations sur l'arrêt des appareils administrés sont transférées de l'agent d'administration au Serveur d'administration via le port UDP 13000.

4. Le Serveur d'administration reçoit une connexion des Agents d'administration et des Serveurs d'administration secondaires via le port TLS 13000.

   Si vous avez utilisé une des versions précédentes de Kaspersky Security Center dans votre réseau, le Serveur d'administration peut accepter les connexions depuis les Agents d'administration par le port non-TLS 14000. Kaspersky Security Center prend aussi en charge la connexion depuis les Agents d'administration par le port 14000. Cependant, il est recommandé d'utiliser le port TLS 13000.

   > Le point de distribution s'appelait "Agent de mise à jour" dans les versions antérieures de Kaspersky Security Center.

5. Les appareils administrés (sauf les appareils mobiles) demandent l'activation via le port TCP 17000. Ce n'est pas nécessaire si l'appareil dispose de son propre accès à Internet. Dans ce cas, l'appareil envoie directement les données aux serveurs de Kaspersky via Internet.

6. Les données de la Console d'administration basée sur MMC sont transférées au Serveur d'administration via le port 13291. (La Console d'administration peut être installée sur le même appareil ou sur un autre.)

7. Les applications sur un seul appareil échangent du trafic local (sur le Serveur d'administration ou sur un appareil administré). Aucun port externe ne doit être ouvert.

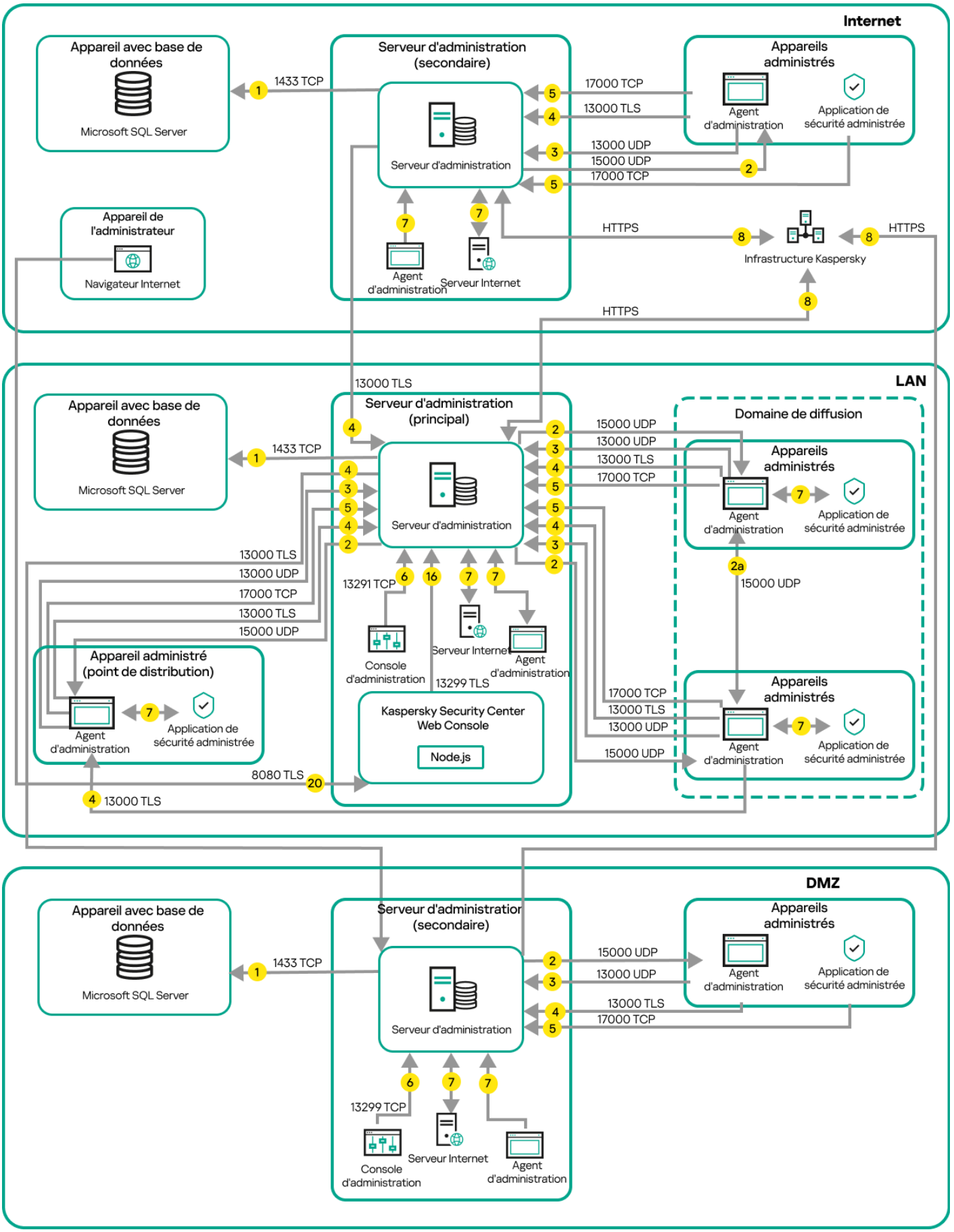
8. Le transfert des données du Serveur d'administration aux serveurs Kaspersky (telles que les données KSN ou les informations sur les licences) et le transfert des données des serveurs Kaspersky au Serveur d'administration (telles que les mises à jour d'applications et les mises à jour de bases de données antivirus), sont effectués via le protocole HTTPS.

   Si vous ne voulez pas que votre Serveur d'administration accède à Internet, vous devez gérer ces données manuellement.

9. Kaspersky Security Center Web Console Server envoie des données au Serveur d'administration, qui peut être installé sur le même appareil ou sur un autre, via le port TLS 13299.

Serveur d'administration principal sur LAN et deux Serveurs d'administration secondaires

La figure ci-dessous représente la hiérarchie des Serveurs d'administration : le Serveur d'administration principal est sur un réseau local (LAN). Un Serveur d'administration secondaire se trouve dans la zone démilitarisée (DMZ) ; un autre Serveur d'administration secondaire est sur Internet.



Hiérarchie des Serveurs d'administration : Serveur d'administration principal et deux Serveurs d'administration secondaires

Les flèches indiquent l'ouverture du trafic : chaque flèche relie l'appareil qui initie la connexion à celui qui " répond " à l'appel. Le numéro du port et le nom du protocole utilisés pour le transfert de données sont fournis. Chaque flèche porte une étiquette numérique et les informations sur le trafic de données sont :

1. Le Serveur d'administration envoie des données à la base de données. Si vous installez le Serveur d'administration et la base de données sur des appareils différents, vous devez mettre à disposition les ports nécessaires sur l'appareil où se trouve la base de données (par exemple, le port 3306 pour MySQL Server ou le port 1433 pour Microsoft SQL Server). Veuillez vous référer à la documentation du SGBD pour les informations pertinentes.

2. Les demandes de communication du Serveur d'administration sont transférés à tous les appareils non mobiles administrés par le port UDP 15000.

   Les Agents d'administration s'envoient des requêtes entre eux au sein d'un domaine de diffusion. Les données sont ensuite envoyées au Serveur d'administration et sont utilisées pour définir les limites du domaine de diffusion et pour l'attribution automatique des points de distribution (si cette option est activée).

   Si le Serveur d'administration n'a pas d'accès direct aux appareils administrés, les requêtes de communication du Serveur d'administration vers ces appareils ne sont pas envoyées directement.

3. Les informations sur l'arrêt des appareils administrés sont transférées de l'agent d'administration au Serveur d'administration via le port UDP 13000.

4. Le Serveur d'administration reçoit une connexion des Agents d'administration et des Serveurs d'administration secondaires via le port TLS 13000.

   Si vous avez utilisé une des versions précédentes de Kaspersky Security Center dans votre réseau, le Serveur d'administration peut accepter les connexions depuis les Agents d'administration par le port non-TLS 14000. Kaspersky Security Center prend aussi en charge la connexion depuis les Agents d'administration par le port 14000. Cependant, il est recommandé d'utiliser le port TLS 13000.

   > Le point de distribution s'appelait "Agent de mise à jour" dans les versions antérieures de Kaspersky Security Center.

5. Les appareils administrés (sauf les appareils mobiles) demandent l'activation via le port TCP 17000. Ce n'est pas nécessaire si l'appareil dispose de son propre accès à Internet. Dans ce cas, l'appareil envoie directement les données aux serveurs de Kaspersky via Internet.

6. Les données de la Console d'administration basée sur MMC sont transférées au Serveur d'administration via le port 13291. (La Console d'administration peut être installée sur le même appareil ou sur un autre.)

7. Les applications sur un seul appareil échangent du trafic local (sur le Serveur d'administration ou sur un appareil administré). Aucun port externe ne doit être ouvert.

8. Le transfert des données du Serveur d'administration aux serveurs Kaspersky (telles que les données KSN ou les informations sur les licences) et le transfert des données des serveurs Kaspersky au Serveur d'administration (telles que les mises à jour d'applications et les mises à jour de bases de données antivirus), sont effectués via le protocole HTTPS.

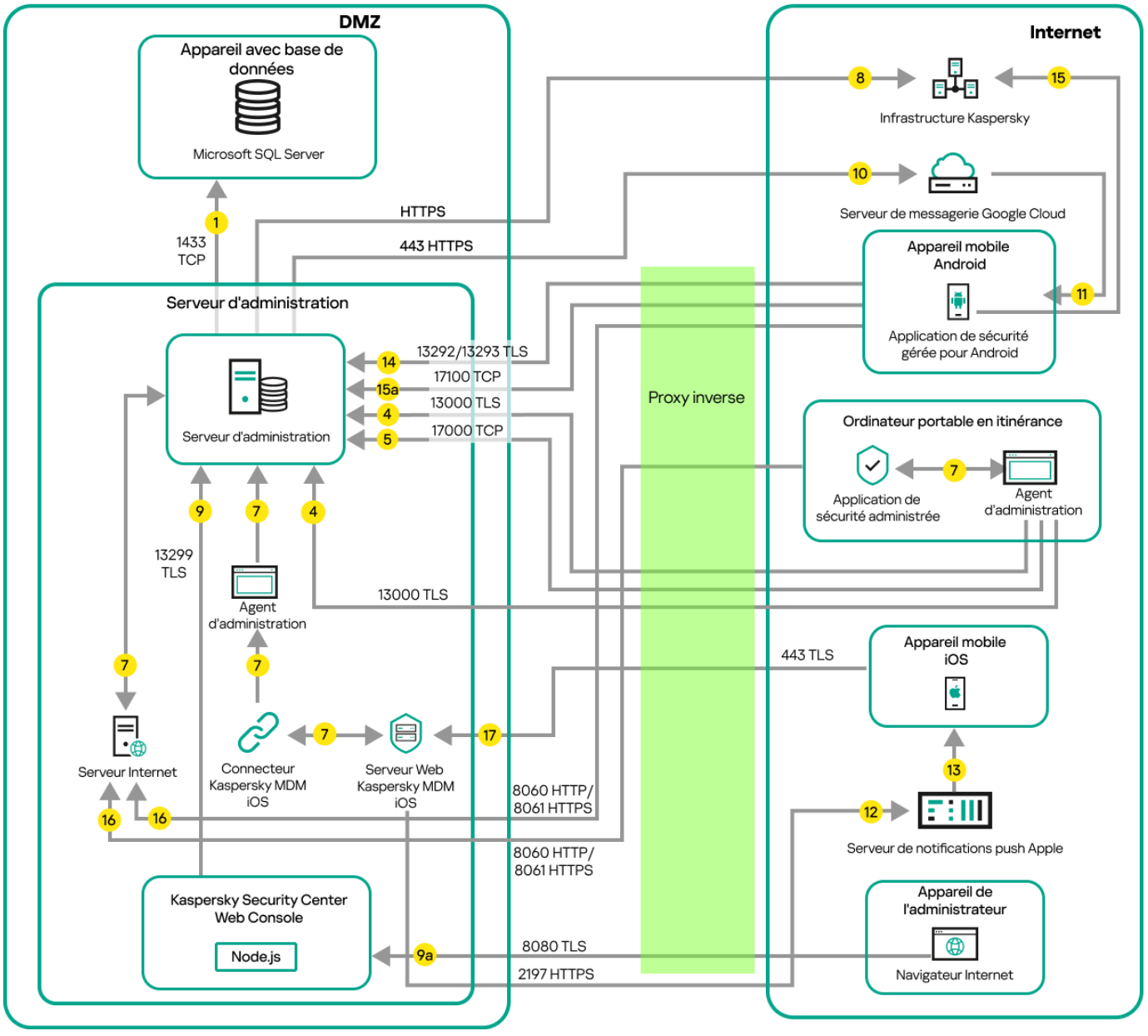
   Si vous ne voulez pas que votre Serveur d'administration accède à Internet, vous devez gérer ces données manuellement.

9. Kaspersky Security Center Web Console Server envoie des données au Serveur d'administration, qui peut être installé sur le même appareil ou sur un autre, via le port TLS 13299.

   9a. Les données du navigateur, installées sur un appareil séparé de l'administrateur, sont transférées sur Kaspersky Security Center Web Console Server (par le port TLS 8080). Le serveur Kaspersky Security Center Web Console peut être installé sur le Serveur d'administration ou sur un autre appareil.

Serveur d'administration sur réseau local, appareils administrés sur Internet, proxy inversé en cours d'utilisation

La figure ci-dessous représente le trafic des données si le Serveur d'administration est sur un réseau local (LAN) et les appareils administrés, dont les appareils mobiles, sont sur Internet. Dans cette figure, le proxy d'entreprise inversé de votre choix est utilisé. Reportez-vous à la documentation de l'application pour plus de détails.



Serveur d'administration sur un réseau local ; les appareils administrés se connectent au Serveur d'administration via un proxy d'entreprise inversé

Ce schéma de déploiement est recommandé si vous ne voulez pas que les appareils mobiles se connectent directement au Serveur d'administration et si vous ne voulez pas assigner une passerelle de connexion dans le DMZ.

Les flèches indiquent l'ouverture du trafic : chaque flèche relie l'appareil qui initie la connexion à celui qui " répond " à l'appel. Le numéro du port et le nom du protocole utilisés pour le transfert de données sont fournis. Chaque flèche porte une étiquette numérique et les informations sur le trafic de données sont :

1. Le Serveur d'administration envoie des données à la base de données. Si vous installez le Serveur d'administration et la base de données sur des appareils différents, vous devez mettre à disposition les ports nécessaires sur l'appareil où se trouve la base de données (par exemple, le port 3306 pour MySQL Server ou le port 1433 pour Microsoft SQL Server). Veuillez vous référer à la documentation du SGBD pour les informations pertinentes.

2. Les demandes de communication du Serveur d'administration sont transférés à tous les appareils non mobiles administrés par le port UDP 15000.

   Les Agents d'administration s'envoient des requêtes entre eux au sein d'un domaine de diffusion. Les données sont ensuite envoyées au Serveur d'administration et sont utilisées pour définir les limites du domaine de diffusion et pour l'attribution automatique des points de distribution (si cette option est activée).

   Si le Serveur d'administration n'a pas d'accès direct aux appareils administrés, les requêtes de communication du Serveur d'administration vers ces appareils ne sont pas envoyées directement.

3. Les informations sur l'arrêt des appareils administrés sont transférées de l'agent d'administration au Serveur d'administration via le port UDP 13000.

4. Le Serveur d'administration reçoit une connexion des Agents d'administration et des Serveurs d'administration secondaires via le port TLS 13000.

   Si vous avez utilisé une des versions précédentes de Kaspersky Security Center dans votre réseau, le Serveur d'administration peut accepter les connexions depuis les Agents d'administration par le port non-TLS 14000. Kaspersky Security Center prend aussi en charge la connexion depuis les Agents d'administration par le port 14000. Cependant, il est recommandé d'utiliser le port TLS 13000.

   > Le point de distribution s'appelait "Agent de mise à jour" dans les versions antérieures de Kaspersky Security Center.

5. Les appareils administrés (sauf les appareils mobiles) demandent l'activation via le port TCP 17000. Ce n'est pas nécessaire si l'appareil dispose de son propre accès à Internet. Dans ce cas, l'appareil envoie directement les données aux serveurs de Kaspersky via Internet.

6. Les données de la Console d'administration basée sur MMC sont transférées au Serveur d'administration via le port 13291. (La Console d'administration peut être installée sur le même appareil ou sur un autre.)

7. Les applications sur un seul appareil échangent du trafic local (sur le Serveur d'administration ou sur un appareil administré). Aucun port externe ne doit être ouvert.

8. Le transfert des données du Serveur d'administration aux serveurs Kaspersky (telles que les données KSN ou les informations sur les licences) et le transfert des données des serveurs Kaspersky au Serveur d'administration (telles que les mises à jour d'applications et les mises à jour de bases de données antivirus), sont effectués via le protocole HTTPS.

   Si vous ne voulez pas que votre Serveur d'administration accède à Internet, vous devez gérer ces données manuellement.

9. Kaspersky Security Center Web Console Server envoie des données au Serveur d'administration, qui peut être installé sur le même appareil ou sur un autre, via le port TLS 13299.

   9a. Les données du navigateur, installées sur un appareil séparé de l'administrateur, sont transférées sur Kaspersky Security Center Web Console Server (par le port TLS 8080). Le serveur Kaspersky Security Center Web Console peut être installé sur le Serveur d'administration ou sur un autre appareil.

10. Pour les appareils mobiles Android uniquement : les données du Serveur d'administration sont transférées aux serveurs Google. Cette connexion sert à notifier aux appareils mobiles Android qu'ils doivent se connecter au Serveur d'administration. Ensuite, les notifications push sont envoyées aux appareils mobiles.

11. Pour les appareils mobiles Android uniquement : les notifications push des serveurs Google sont envoyées à l'appareil mobile. Cette connexion sert à notifier aux appareils mobiles qu'ils doivent se connecter au Serveur d'administration.

12. Pour les appareils mobiles iOS uniquement : les données du serveur MDM iOS sont transférées aux serveurs de notifications Apple Push. Ensuite, les notifications push sont envoyées aux appareils mobiles.

13. Pour les appareils mobiles iOS uniquement : les notifications push des serveurs Apple sont envoyées à l'appareil mobile. Cette connexion sert à notifier aux appareils mobiles iOS qu'ils doivent se connecter au Serveur d'administration.

14. Pour les appareils mobiles uniquement : les données de l'application administrée sont transférées vers le Serveur d'administration (ou à la passerelle de connexion) via le port TLS 13292 / 13293 : directement ou via un proxy inversé.

15. Pour les appareils mobiles uniquement : les données de l'appareil mobile sont transférées vers l'infrastructure de Kaspersky.

    Si un appareil mobile n'a pas accès à Internet, les données sont transférées vers le Serveur d'administration via le port 17100, et le Serveur d'administration les envoie à l'infrastructure de Kaspersky. Cependant, ce scénario s'applique très rarement.

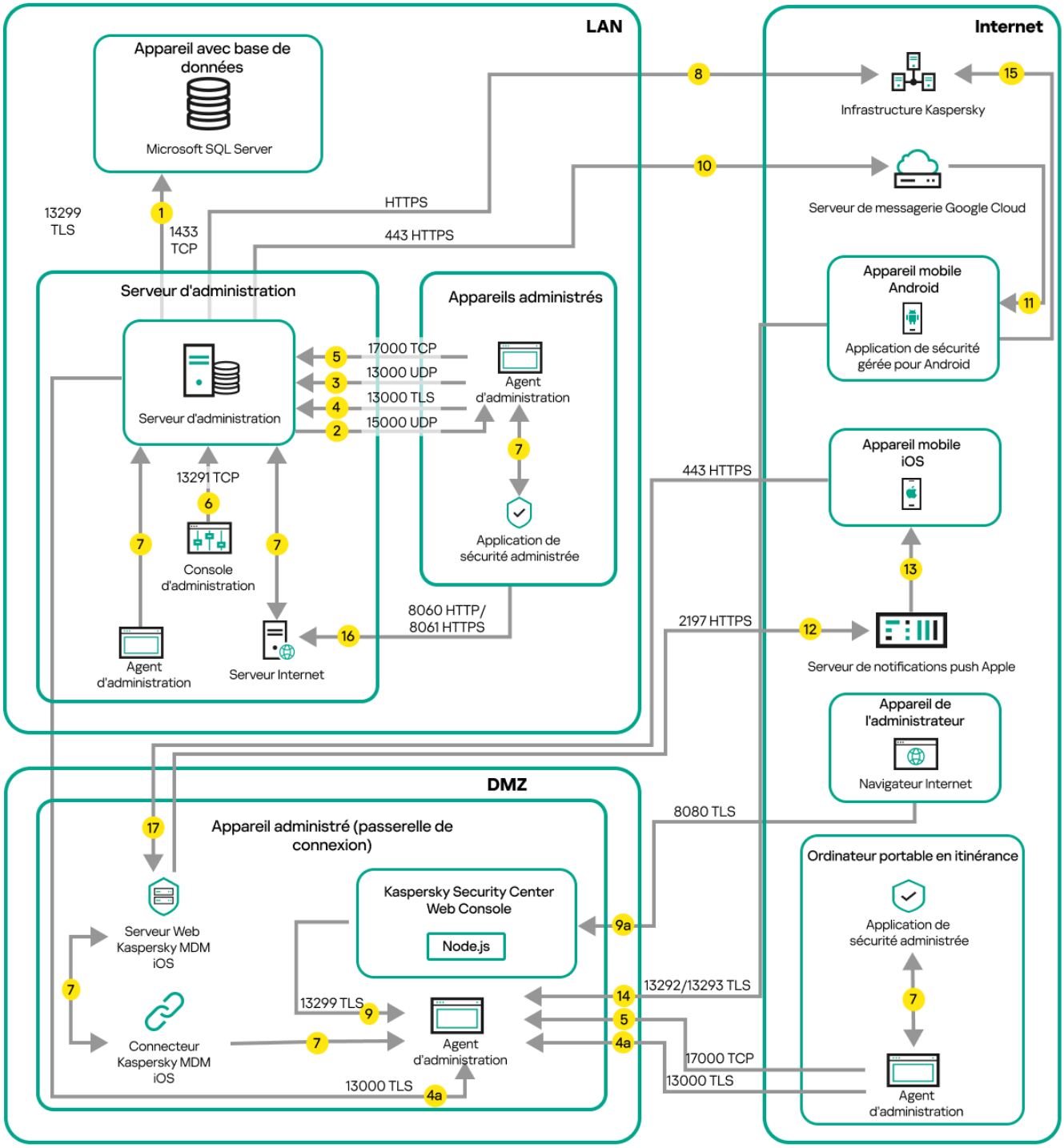
16. Les demandes de paquets provenant d'appareils administrés, y compris d'appareils mobiles, sont transférées sur le serveur Web, qui se trouve sur le même appareil que le Serveur d'administration.

17. Pour les appareils mobiles iOS uniquement : les données de l'appareil mobile sont transférées sur le serveur MDM iOS via le port TLS 443, qui se trouve sur le même appareil que le Serveur d'administration ou sur la passerelle de connexion.

Le Serveur d'administration sur LAN, les appareils administrés sur Internet, la passerelle de connexion en cours d'utilisation

La figure ci-dessous représente le trafic des données si le Serveur d'administration est sur un réseau local (LAN) et les appareils administrés, dont les appareils mobiles, sont sur Internet. Une passerelle de connexion est en cours d'utilisation.

Ce schéma de déploiement est recommandé si vous ne souhaitez pas que les appareils mobiles se connectent directement au Serveur d'administration et si vous ne souhaitez pas utiliser de proxy inversé ou de pare-feu d'entreprise.



Les appareils mobiles administrés sont connectés au Serveur d'administration par une passerelle de connexion

Dans cette figure, les appareils administrés sont connectés au Serveur d'administration par une passerelle de connexion située dans le DMZ. Aucun proxy inversé ou pare-feu d'entreprise n'est utilisé.

Les flèches indiquent l'ouverture du trafic : chaque flèche relie l'appareil qui initie la connexion à celui qui " répond " à l'appel. Le numéro du port et le nom du protocole utilisés pour le transfert de données sont fournis. Chaque flèche porte une étiquette numérique et les informations sur le trafic de données sont :

1. Le Serveur d'administration envoie des données à la base de données. Si vous installez le Serveur d'administration et la base de données sur des appareils différents, vous devez mettre à disposition les ports nécessaires sur l'appareil où se trouve la base de données (par exemple, le port 3306 pour MySQL Server ou le port 1433 pour Microsoft SQL Server). Veuillez vous référer à la documentation du SGBD pour les informations pertinentes.

2. Les demandes de communication du Serveur d'administration sont transférés à tous les appareils non mobiles administrés par le port UDP 15000.

   Les Agents d'administration s'envoient des requêtes entre eux au sein d'un domaine de diffusion. Les données sont ensuite envoyées au Serveur d'administration et sont utilisées pour définir les limites du domaine de diffusion et pour l'attribution automatique des points de distribution (si cette option est activée).

   Si le Serveur d'administration n'a pas d'accès direct aux appareils administrés, les requêtes de communication du Serveur d'administration vers ces appareils ne sont pas envoyées directement.

3. Les informations sur l'arrêt des appareils administrés sont transférées de l'agent d'administration au Serveur d'administration via le port UDP 13000.

4. Le Serveur d'administration reçoit une connexion des Agents d'administration et des Serveurs d'administration secondaires via le port TLS 13000.

   Si vous avez utilisé une des versions précédentes de Kaspersky Security Center dans votre réseau, le Serveur d'administration peut accepter les connexions depuis les Agents d'administration par le port non-TLS 14000. Kaspersky Security Center prend aussi en charge la connexion depuis les Agents d'administration par le port 14000. Cependant, il est recommandé d'utiliser le port TLS 13000.

   > Le point de distribution s'appelait "Agent de mise à jour" dans les versions antérieures de Kaspersky Security Center.

   4a. Une passerelle de connexion dans la DMZ reçoit également la connexion du Serveur d'administration par le port TLS 13000. Étant donné qu'une passerelle de connexion dans la DMZ ne peut pas atteindre les ports du Serveur d'administration, le Serveur d'administration crée et maintient une connexion de signal permanente avec une passerelle de connexion. La connexion de signal n'est pas utilisée pour le transfert de données ; elle n'est utilisée que pour envoyer une invitation à l'interaction réseau. Lorsque la passerelle de connexion doit se connecter au Serveur, elle avertit le Serveur par cette connexion de signal, puis le Serveur crée la connexion requise pour procéder au transfert de données.

   Les appareils itinérants se connectent également à la passerelle de connexion par le port TLS 13000.

5. Les appareils administrés (sauf les appareils mobiles) demandent l'activation via le port TCP 17000. Ce n'est pas nécessaire si l'appareil dispose de son propre accès à Internet. Dans ce cas, l'appareil envoie directement les données aux serveurs de Kaspersky via Internet.

6. Les données de la Console d'administration basée sur MMC sont transférées au Serveur d'administration via le port 13291. (La Console d'administration peut être installée sur le même appareil ou sur un autre.)

7. Les applications sur un seul appareil échangent du trafic local (sur le Serveur d'administration ou sur un appareil administré). Aucun port externe ne doit être ouvert.

8. Le transfert des données du Serveur d'administration aux serveurs Kaspersky (telles que les données KSN ou les informations sur les licences) et le transfert des données des serveurs Kaspersky au Serveur d'administration (telles que les mises à jour d'applications et les mises à jour de bases de données antivirus), sont effectués via le protocole HTTPS.

   Si vous ne voulez pas que votre Serveur d'administration accède à Internet, vous devez gérer ces données manuellement.

9. Kaspersky Security Center Web Console Server envoie des données au Serveur d'administration, qui peut être installé sur le même appareil ou sur un autre, via le port TLS 13299.

   9a. Les données du navigateur, installées sur un appareil séparé de l'administrateur, sont transférées sur Kaspersky Security Center Web Console Server (par le port TLS 8080). Le serveur Kaspersky Security Center Web Console peut être installé sur le Serveur d'administration ou sur un autre appareil.

10. Pour les appareils mobiles Android uniquement : les données du Serveur d'administration sont transférées aux serveurs Google. Cette connexion sert à notifier aux appareils mobiles Android qu'ils doivent se connecter au Serveur d'administration. Ensuite, les notifications push sont envoyées aux appareils mobiles.

11. Pour les appareils mobiles Android uniquement : les notifications push des serveurs Google sont envoyées à l'appareil mobile. Cette connexion sert à notifier aux appareils mobiles qu'ils doivent se connecter au Serveur d'administration.

12. Pour les appareils mobiles iOS uniquement : les données du serveur MDM iOS sont transférées aux serveurs de notifications Apple Push. Ensuite, les notifications push sont envoyées aux appareils mobiles.

13. Pour les appareils mobiles iOS uniquement : les notifications push des serveurs Apple sont envoyées à l'appareil mobile. Cette connexion sert à notifier aux appareils mobiles iOS qu'ils doivent se connecter au Serveur d'administration.

14. Pour les appareils mobiles uniquement : les données de l'application administrée sont transférées vers le Serveur d'administration (ou à la passerelle de connexion) via le port TLS 13292 / 13293 : directement ou via un proxy inversé.

15. Pour les appareils mobiles uniquement : les données de l'appareil mobile sont transférées vers l'infrastructure de Kaspersky.

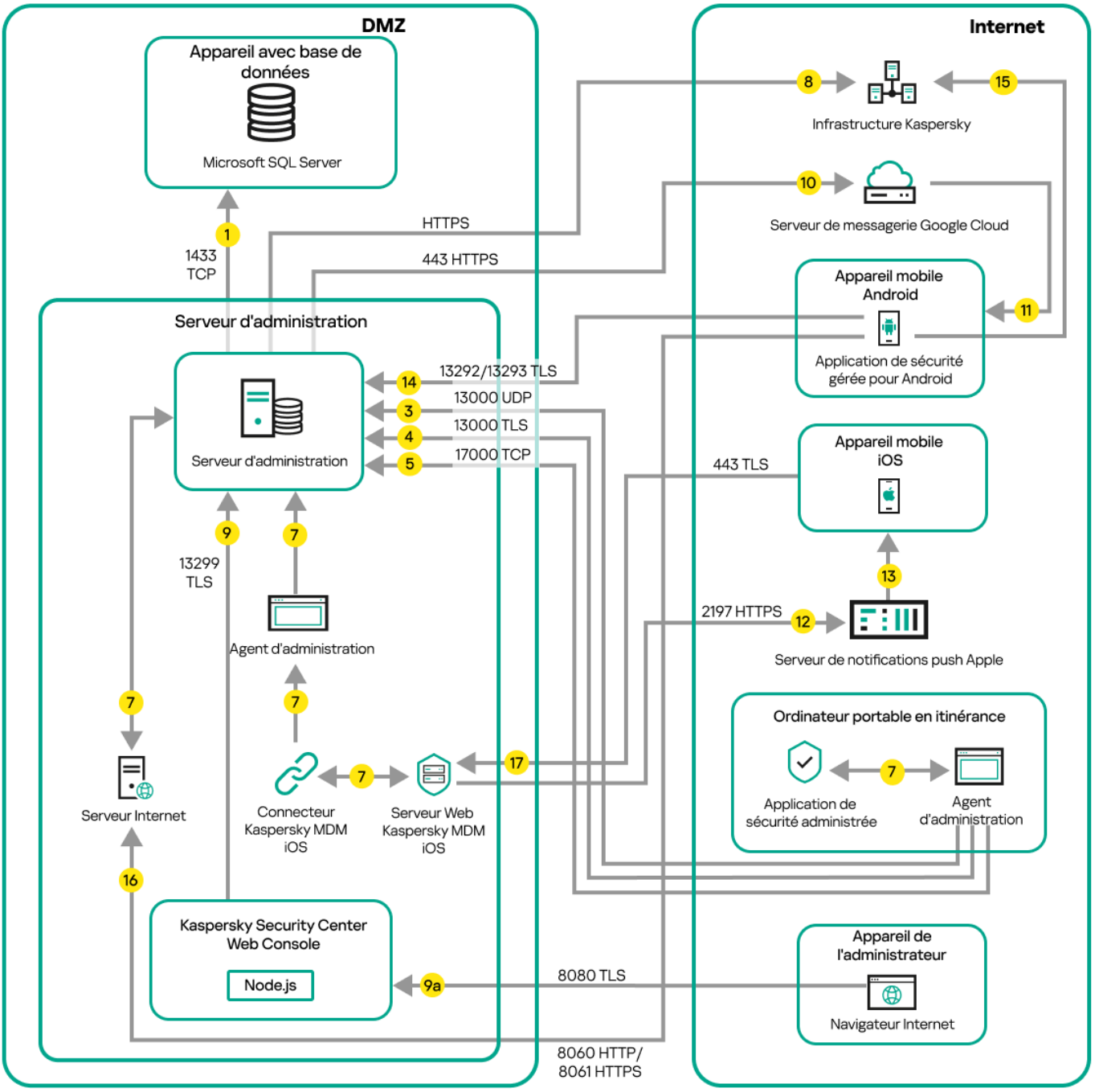
    Si un appareil mobile n'a pas accès à Internet, les données sont transférées vers le Serveur d'administration via le port 17100, et le Serveur d'administration les envoie à l'infrastructure de Kaspersky. Cependant, ce scénario s'applique très rarement.

16. Les demandes de paquets provenant d'appareils administrés, y compris d'appareils mobiles, sont transférées sur le serveur Web, qui se trouve sur le même appareil que le Serveur d'administration.

17. Pour les appareils mobiles iOS uniquement : les données de l'appareil mobile sont transférées sur le serveur MDM iOS via le port TLS 443, qui se trouve sur le même appareil que le Serveur d'administration ou sur la passerelle de connexion.

Serveur d'administration en DMZ, appareils administrés sur Internet

La figure ci-dessous représente le trafic des données si le Serveur d'administration est sur un DMZ et les appareils administrés, dont les appareils mobiles, sont sur Internet.



Serveur d'administration dans DMZ, appareils mobiles administrés sur Internet

Sur cette figure, aucune passerelle de connexion n'est utilisée : les appareils mobiles se connectent directement au Serveur d'administration.

Les flèches indiquent l'ouverture du trafic : chaque flèche relie l'appareil qui initie la connexion à celui qui " répond " à l'appel. Le numéro du port et le nom du protocole utilisés pour le transfert de données sont fournis. Chaque flèche porte une étiquette numérique et les informations sur le trafic de données sont :

1. Le Serveur d'administration envoie des données à la base de données. Si vous installez le Serveur d'administration et la base de données sur des appareils différents, vous devez mettre à disposition les ports nécessaires sur l'appareil où se trouve la base de données (par exemple, le port 3306 pour MySQL Server ou le port 1433 pour Microsoft SQL Server). Veuillez vous référer à la documentation du SGBD pour les informations pertinentes.

2. Les demandes de communication du Serveur d'administration sont transférés à tous les appareils non mobiles administrés par le port UDP 15000.

   Les Agents d'administration s'envoient des requêtes entre eux au sein d'un domaine de diffusion. Les données sont ensuite envoyées au Serveur d'administration et sont utilisées pour définir les limites du domaine de diffusion et pour l'attribution automatique des points de distribution (si cette option est activée).

   Si le Serveur d'administration n'a pas d'accès direct aux appareils administrés, les requêtes de communication du Serveur d'administration vers ces appareils ne sont pas envoyées directement.

3. Les informations sur l'arrêt des appareils administrés sont transférées de l'agent d'administration au Serveur d'administration via le port UDP 13000.

4. Le Serveur d'administration reçoit une connexion des Agents d'administration et des Serveurs d'administration secondaires via le port TLS 13000.

   Si vous avez utilisé une des versions précédentes de Kaspersky Security Center dans votre réseau, le Serveur d'administration peut accepter les connexions depuis les Agents d'administration par le port non-TLS 14000. Kaspersky Security Center prend aussi en charge la connexion depuis les Agents d'administration par le port 14000. Cependant, il est recommandé d'utiliser le port TLS 13000.

   > Le point de distribution s'appelait "Agent de mise à jour" dans les versions antérieures de Kaspersky Security Center.

5. Les appareils administrés (sauf les appareils mobiles) demandent l'activation via le port TCP 17000. Ce n'est pas nécessaire si l'appareil dispose de son propre accès à Internet. Dans ce cas, l'appareil envoie directement les données aux serveurs de Kaspersky via Internet.

6. Les données de la Console d'administration basée sur MMC sont transférées au Serveur d'administration via le port 13291. (La Console d'administration peut être installée sur le même appareil ou sur un autre.)

7. Les applications sur un seul appareil échangent du trafic local (sur le Serveur d'administration ou sur un appareil administré). Aucun port externe ne doit être ouvert.

8. Le transfert des données du Serveur d'administration aux serveurs Kaspersky (telles que les données KSN ou les informations sur les licences) et le transfert des données des serveurs Kaspersky au Serveur d'administration (telles que les mises à jour d'applications et les mises à jour de bases de données antivirus), sont effectués via le protocole HTTPS.

   Si vous ne voulez pas que votre Serveur d'administration accède à Internet, vous devez gérer ces données manuellement.

9. Kaspersky Security Center Web Console Server envoie des données au Serveur d'administration, qui peut être installé sur le même appareil ou sur un autre, via le port TLS 13299.

   9a. Les données du navigateur, installées sur un appareil séparé de l'administrateur, sont transférées sur Kaspersky Security Center Web Console Server (par le port TLS 8080). Le serveur Kaspersky Security Center Web Console peut être installé sur le Serveur d'administration ou sur un autre appareil.

10. Pour les appareils mobiles Android uniquement : les données du Serveur d'administration sont transférées aux serveurs Google. Cette connexion sert à notifier aux appareils mobiles Android qu'ils doivent se connecter au Serveur d'administration. Ensuite, les notifications push sont envoyées aux appareils mobiles.

11. Pour les appareils mobiles Android uniquement : les notifications push des serveurs Google sont envoyées à l'appareil mobile. Cette connexion sert à notifier aux appareils mobiles qu'ils doivent se connecter au Serveur d'administration.

12. Pour les appareils mobiles iOS uniquement : les données du serveur MDM iOS sont transférées aux serveurs de notifications Apple Push. Ensuite, les notifications push sont envoyées aux appareils mobiles.

13. Pour les appareils mobiles iOS uniquement : les notifications push des serveurs Apple sont envoyées à l'appareil mobile. Cette connexion sert à notifier aux appareils mobiles iOS qu'ils doivent se connecter au Serveur d'administration.

14. Pour les appareils mobiles uniquement : les données de l'application administrée sont transférées vers le Serveur d'administration (ou à la passerelle de connexion) via le port TLS 13292 / 13293 : directement ou via un proxy inversé.

15. Pour les appareils mobiles uniquement : les données de l'appareil mobile sont transférées vers l'infrastructure de Kaspersky.

    Si un appareil mobile n'a pas accès à Internet, les données sont transférées vers le Serveur d'administration via le port 17100, et le Serveur d'administration les envoie à l'infrastructure de Kaspersky. Cependant, ce scénario s'applique très rarement.

16. Les demandes de paquets provenant d'appareils administrés, y compris d'appareils mobiles, sont transférées sur le serveur Web, qui se trouve sur le même appareil que le Serveur d'administration.

17. Pour les appareils mobiles iOS uniquement : les données de l'appareil mobile sont transférées sur le serveur MDM iOS via le port TLS 443, qui se trouve sur le même appareil que le Serveur d'administration ou sur la passerelle de connexion.

Schémas d'interaction des modules de Kaspersky Security Center et des applications de sécurité : plus d'informations

Cette section présente les schémas d'interaction entre les modules figurant dans Kaspersky Security Center et les applications de sécurité administrées. Les schémas présentent les numéros des ports qui doivent être disponibles, et les noms des processus ouvrant les ports.

Conventions utilisées dans les schémas d'interaction

Le tableau ci-dessous présente les conventions utilisées dans les schémas.

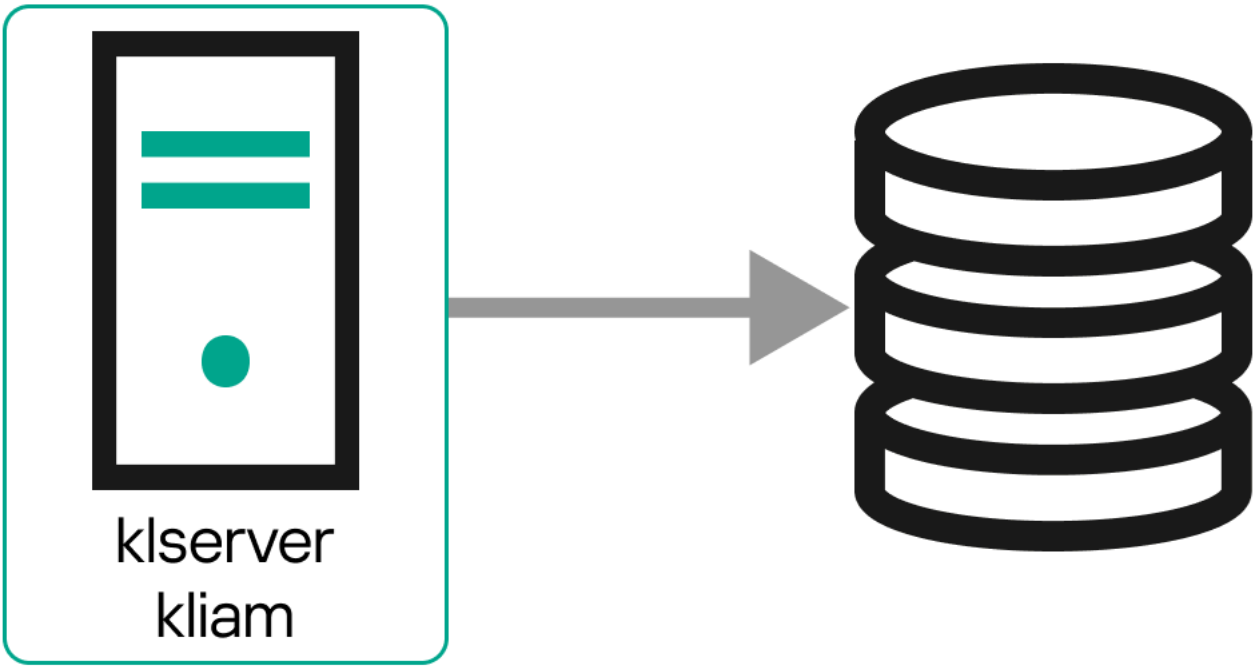
Conventions

Icône	Explication
	Serveur d'administration

	Serveur d'administration secondaire
	SGBD
	Appareil client sur lequel sont installés l'Agent d'administration et l'application de la série Kaspersky Endpoint Security (ou une autre application de sécurité pouvant être administrée par Kaspersky Security Center)
	Passerelle des connexions
	Point de distribution
	Appareil client mobile avec l'application Kaspersky Security for Mobile
	Navigateur sur l'appareil de l'utilisateur
	Processus exécuté sur l'appareil et ouvrant un port, quel qu'il soit
	Port et son numéro
	Trafic TCP (le sens de la flèche indique le sens du trafic)
	Trafic UDP (le sens de la flèche indique le sens du trafic)
	Appel COM
	Transport du SGBD
	Frontière de la zone démilitarisée

Serveur d'administration et SGBD

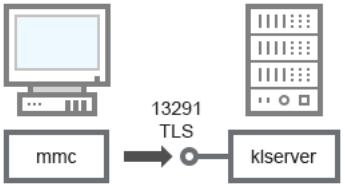
Les données du Serveur d'administration alimentent la base de données SQL Server, MySQL ou MariaDB.



Serveur d'administration et SGBD

Si vous installez le Serveur d'administration et la base de données sur des appareils différents, vous devez mettre à disposition les ports nécessaires sur l'appareil où se trouve la base de données (par exemple, le port 3306 pour MySQL Server ou le port 1433 pour Microsoft SQL Server). Veuillez vous référer à la documentation du SGBD pour les informations pertinentes.

Serveur d'administration et la Console d'administration



Serveur d'administration et la Console d'administration

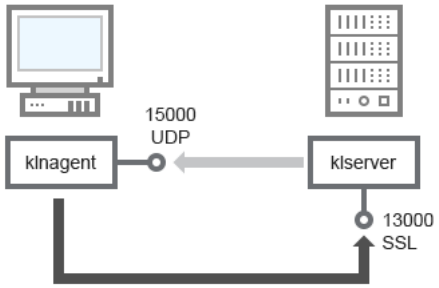
Pour avoir des explications sur le schéma, cf. tableau ci-après.

Serveur d'administration et la Console d'administration (trafic)

Appareil	Numéro de port	Nom du processus qui a ouvert le port	Protocole	TLS	Destination du port
Serveur d'administration	13291	klserver	TCP	Oui	Réception des connexions depuis la Console d'administration

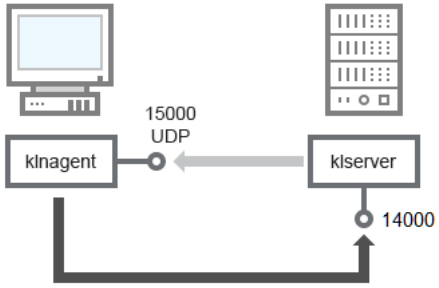
Serveur d'administration et appareil client : administration de l'application de sécurité

Le Serveur d'administration accepte la connexion depuis les Agents d'administration par le port protégé 13000 (cf. fig. ci-après).



Serveur d'administration et appareil client : administration de l'application de sécurité, connexion par le port 13000 (recommandée)

Si vous avez utilisé une des versions précédentes de Kaspersky Security Center, le Serveur d'administration sur votre réseau peut accepter les connexions depuis les Agents d'administration par le port non protégé 14000 (cf. fig. ci-après). Kaspersky Security Center 15.1 prend aussi en charge la connexion depuis les Agents d'administration par le port 14000. Cependant, il est recommandé d'utiliser le port protégé 13000.



Serveur d'administration et appareil client : administration de l'application de sécurité, connexion par le port 14000 (moins sûre)

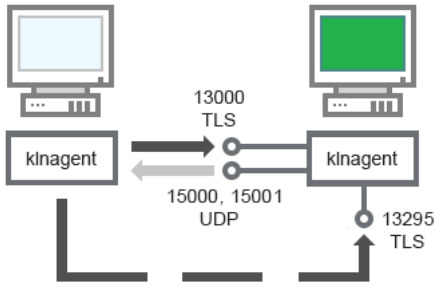
Pour avoir des explications sur les schémas, cf. tableau ci-après.

Serveur d'administration et appareil client : administration de l'application de sécurité (trafic)

Appareil	Numéro de port	Nom du processus qui a ouvert le port	Protocole	TLS (pour TCP uniquement)	Destination du port
Agent d'administration	15000	klnagent	UDP	Aucune valeur	Diffusion multicast vers les Agents d'administration
Serveur d'administration	13000	klserver	TCP	Oui	Réception des connexions des Agents d'administration
Serveur d'administration	14000	klserver	TCP	Non	Réception des connexions des Agents d'administration

Mise à jour du logiciel sur l'appareil client par un point de distribution

L'appareil client se connecte au point de distribution via le port 13000 et, si vous utilisez le point de distribution comme serveur push, également via le port 13295 ; le point de distribution effectue la multidiffusion vers les agents d'administration via le port 15000 (cf. ill. ci-dessous). Les mises à jour et les paquets d'installation sont reçus à partir d'un point de distribution via le port 15001.



Mise à jour du logiciel sur l'appareil client par un point de distribution

Pour avoir des explications sur le schéma, cf. tableau ci-après.

Mise à niveau du logiciel par un point de distribution (trafic)

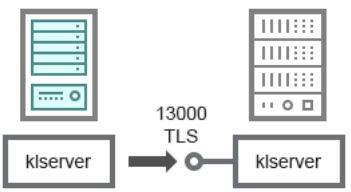
Appareil	Numéro de port	Nom du processus qui a ouvert le port	Protocole	TLS (pour TCP uniquement)	Destination du port
Agent d'administration	15000	klnagent	UDP	Aucune valeur	Diffusion multicast vers les Agents d'administration
Agent d'administration	15001	klnagent	UDP	Aucune valeur	Réception des mises à jour et des paquets d'installation à partir d'un point de distribution
Point de distribution	13000	klnagent	TCP	Oui	Réception des connexions des Agents d'administration
Point de distribution	13295	klnagent	TCP	Oui	Réception de connexions depuis les appareils clients (serveur push)

Hiérarchie des Serveurs d'administration : Serveur d'administration principal et Serveur d'administration secondaire

L'illustration (cf. ill. ci-dessous) montre comment utiliser le port 13000 pour l'interaction des Serveurs d'administration regroupés au sein de la hiérarchie.

En cas de regroupement de Serveurs dans une hiérarchie, le port 13291 des deux Serveurs doit être accessible. La connexion de la Console d'administration au Serveur d'administration s'opère via le port 13291.

Ensuite, après le regroupement des Serveurs d'administration dans une hiérarchie, vous pourrez administrer les deux Serveurs via la Console d'administration connectée au Serveur d'administration principal. Ainsi, seul le port 13291 du Serveur d'administration principal doit être accessible.



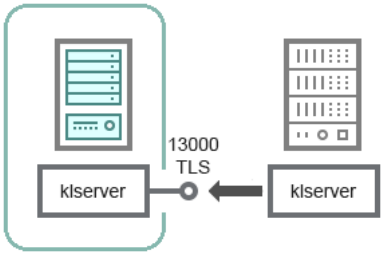
Hiérarchie des Serveurs d'administration : Serveur d'administration principal et Serveur d'administration secondaire

Pour avoir des explications sur le schéma, cf. tableau ci-après.

Hiérarchie des Serveurs d'administration (trafic)

Appareil	Numéro de port	Nom du processus qui a ouvert le port	Protocole	TLS	Destination du port
Serveur d'administration principal	13000	klserver	TCP	Oui	Réception des connexions depuis les Serveurs d'administration secondaires

Hiérarchie des Serveurs d'administration avec Serveur d'administration secondaire dans la zone démilitarisée



Hiérarchie des Serveurs d'administration avec Serveur d'administration secondaire dans la zone démilitarisée

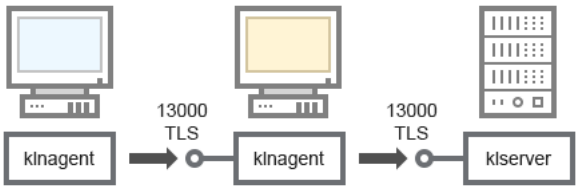
Le schéma illustre une hiérarchie de Serveurs d'administration dans laquelle le Serveur d'administration secondaire, situé dans la zone démilitarisée, reçoit une connexion d'un Serveur d'administration principal (les explications du schéma sont reprises dans le tableau ci-après). En cas de regroupement de Serveurs dans une hiérarchie, le port 13291 des deux Serveurs doit être accessible. La connexion de la Console d'administration au Serveur d'administration s'opère via le port 13291.

Ensuite, après le regroupement des Serveurs d'administration dans une hiérarchie, vous pourrez administrer les deux Serveurs via la Console d'administration connectée au Serveur d'administration principal. Ainsi, seul le port 13291 du Serveur d'administration principal doit être accessible.

Hiérarchie des Serveurs d'administration avec Serveur d'administration secondaire dans la zone démilitarisée (trafic)

Appareil	Numéro de port	Nom du processus qui a ouvert le port	Protocole	TLS	Destination du port
Serveur d'administration secondaire	13000	klserver	TCP	Oui	Réception des connexions du Serveur d'administration principal

Serveur d'administration, passerelle de connexion dans un segment du réseau et appareil client



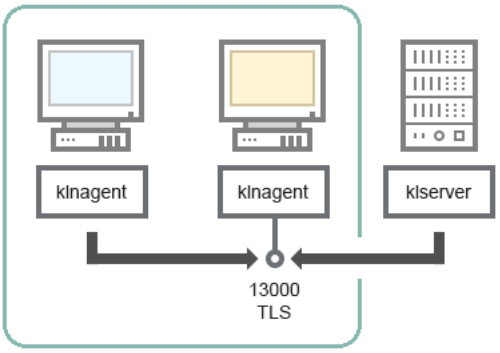
Serveur d'administration, passerelle de connexion dans un segment du réseau et appareil client

Pour avoir des explications sur le schéma, cf. tableau ci-après.

Serveur d'administration, passerelle de connexion dans un segment du réseau et appareil client (trafic)

Appareil	Numéro de port	Nom du processus qui a ouvert le port	Protocole	TLS	Destination du port
Serveur d'administration	13000	klserver	TCP	Oui	Réception des connexions des Agents d'administration
Agent d'administration	13000	klnagent	TCP	Oui	Réception des connexions des Agents d'administration

Serveur d'administration et deux appareils en DMZ : une passerelle de connexion et un appareil client



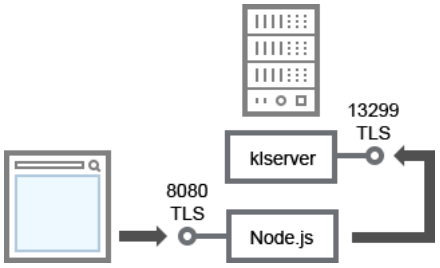
Serveur d'administration et passerelle de connexion et appareil client dans la zone démilitarisée

Pour avoir des explications sur le schéma, cf. tableau ci-après.

Serveur d'administration avec une passerelle de connexion dans un segment du réseau et appareil client (trafic)

Appareil	Numéro de port	Nom du processus qui a ouvert le port	Protocole	TLS	Destination du port
Agent d'administration	13000	klnagent	TCP	Oui	Réception des connexions des Agents d'administration

Serveur d'administration et Kaspersky Security Center Web Console



Serveur d'administration et Kaspersky Security Center Web Console

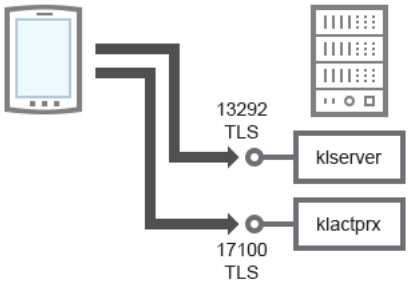
Pour avoir des explications sur le schéma, cf. tableau ci-après.

Serveur d'administration et Kaspersky Security Center Web Console (trafic)

Appareil	Numéro de port	Nom du processus qui a ouvert le port	Protocole	TLS	Destination du port
Serveur d'administration	13299	klserver	TCP	Oui	Réception des connexions de Kaspersky Security Center Web Console vers le Serveur d'administration sur OpenAPI
Kaspersky Security Center Web Console ou Serveur d'administration	8080	Node.js : JavaScript côté serveur	TCP	Oui	Réception des connexions depuis Kaspersky Security Center Web Console

Kaspersky Security Center Web Console peut être installée sur le Serveur d'administration ou sur un autre appareil.

Activation et administration de l'application de sécurité sur un appareil mobile



Activation et administration de l'application de sécurité sur un appareil mobile

Pour avoir des explications sur le schéma, cf. tableau ci-après.

Activation et administration de l'application de sécurité sur un appareil mobile (trafic)

Appareil	Numéro de port	Nom du processus qui a ouvert le port	Protocole	TLS	Destination du port
Serveur d'administration	13292	klserver	TCP	Oui	Réception des connexions de la Console d'administration au Serveur d'administration
Serveur d'administration	17100	klactprx	TCP	Oui	Réception des connexions pour l'activation de l'application depuis les appareils mobiles

Bonnes pratiques de déploiement

Kaspersky Security Center est une application distribuée. Kaspersky Security Center contient les applications suivantes :

- Le Serveur d'administration est le module central responsable de l'administration des appareils de l'entreprise et de la conservation des données dans le SGBD.
- La Console d'administration est l'outil principal de l'administrateur. La Console d'administration est livrée avec le Serveur d'administration, mais peut être également installée séparément sur un ou plusieurs appareils de l'administrateur.
- L'Agent d'administration intervient dans l'administration de l'application de sécurité installée sur l'appareil, ainsi que dans l'obtention d'informations sur l'appareil et le transfert de ces informations vers le Serveur d'administration. Les Agents d'administration s'installent sur les appareils de l'entreprise.

Le déploiement de Kaspersky Security Center dans le réseau de l'entreprise se réalise comme suit :

- Installation du Serveur d'administration
- Installation de la Console d'administration sur l'appareil de l'administrateur
- Installation de l'Agent d'administration et de l'application de sécurité sur les appareils de l'organisation

Guide de sécurisation renforcée

L'application Kaspersky Security Center a été développée pour centraliser les principales tâches d'administration et assurer le système de protection du réseau d'une entreprise. L'application permet à l'administrateur d'accéder aux informations détaillées sur le niveau de sécurité du réseau de l'entreprise. Kaspersky Security Center permet de configurer tous les modules de protection créés à l'aide des applications de Kaspersky.

Le Serveur d'administration de Kaspersky Security Center a un accès complet à l'administration de la protection des appareils clients et constitue le composant le plus important du système de sécurité de l'entreprise. Par conséquent, des méthodes de protection renforcées sont requises pour le Serveur d'administration.

Avant la configuration, créez une copie de sauvegarde du Serveur d'administration de Kaspersky Security Center à l'aide de la tâche Sauvegarde des données du Serveur d'administration ou utilitaire klbackup et enregistrez-la dans un endroit sûr.

Le Guide de sécurisation renforcée décrit les recommandations et les fonctionnalités de configuration de Kaspersky Security Center et de ses modules, dans le but de réduire les risques de compromission.

Le Guide de sécurisation renforcée contient les informations suivantes :

- Sélection de l'architecture du Serveur d'administration
- Configuration d'une connexion sécurisée au Serveur d'administration
- Configuration des comptes d'accès au Serveur d'administration
- Gestion de la protection du Serveur d'administration
- Gestion de la protection des appareils clients
- Configuration de la protection des applications administrées
- Maintenance du Serveur d'administration
- Transfert d'informations vers des applications tierces
- Recommandations de sécurité pour les systèmes d'information des tiers

Déploiement du Serveur d'administration

Architecture du Serveur d'administration

En général, le choix d'une architecture d'administration centralisée dépend de l'emplacement des appareils protégés, de l'accès depuis les réseaux adjacents, des schémas de diffusion des mises à jour des bases de données, etc.

Lors de la phase initiale du développement de l'architecture, nous vous recommandons de vous familiariser avec les Kaspersky Security Center et leur interaction, ainsi qu'avec les schémas de trafic de données et d'utilisation des ports.

Sur la base de ces informations, vous pouvez former une architecture qui spécifie :

- L'emplacement du Serveur d'administration et les connexions réseau
- Organisation des espaces de travail de l'administrateur et modes de connexion au Serveur d'administration
- Modes de déploiement de l'Agent d'administration et des logiciels de protection
- Utilisation des points de distribution
- Utilisation des Serveurs d'administration virtuels
- Utilisation de la hiérarchie de Serveurs d'administration
- Schéma de mise à jour des bases antivirus
- Autres flux d'informations

Sélection de l'appareil pour l'installation du Serveur d'administration

Nous vous recommandons d'installer le Serveur d'administration sur un serveur dédié dans l'infrastructure de l'organisation. Si aucun autre logiciel tiers n'est installé sur le serveur, vous pouvez configurer les paramètres de sécurité en fonction des exigences de Kaspersky Security Center, sans dépendre des exigences des logiciels tiers.

Vous pouvez déployer le Serveur d'administration sur un serveur physique ou sur un serveur virtuel. Veuillez vous assurer que l'appareil sélectionné répond aux exigences matérielles et logicielles.

Emplacement du Serveur d'administration

Les appareils administrés par le Serveur d'administration peuvent être localisés comme suit :

- Sur un réseau local (LAN)
- Sur Internet
- Dans la zone démilitarisée (DMZ)

Dans le même temps, le Serveur d'administration peut également se trouver dans différents segments : segments industriels, d'entreprise et DMZ.

Si vous utilisez Kaspersky Security Center pour administrer la protection d'un segment isolé du réseau, nous vous recommandons de déployer le Serveur d'administration dans un segment de la zone démilitarisée (DMZ). Cela vous permet d'organiser une segmentation correcte du réseau et de minimiser le flux de trafic vers le segment protégé, tout en conservant des capacités d'administration complètes et la livraison des mises à jour.

Restriction du déploiement du Serveur d'administration sur un contrôleur de domaine, un serveur de terminaux ou un appareil utilisateur

Il est fortement déconseillé d'installer le Serveur d'administration sur un contrôleur de domaine, un serveur de terminaux ou un appareil utilisateur.

Nous vous recommandons de prévoir une séparation fonctionnelle des nœuds de la clé de réseau. Cette approche vous permet de maintenir le fonctionnement de différents systèmes lorsqu'un nœud tombe en panne ou est compromis. En même temps, vous pouvez créer différentes stratégies de sécurité pour chaque nœud.

Par exemple, les restrictions de sécurité généralement appliquées à un contrôleur de domaine peuvent réduire considérablement les performances du Serveur d'administration et rendre impossible l'utilisation de certaines de ses fonctionnalités. Si un intrus obtient un accès privilégié au contrôleur de domaine, la base de données des services de domaine Active Directory (AD DS) peuvent être modifiés, endommagés ou détruits. De plus, tous les systèmes et comptes administrés par Active Directory peuvent être compromis.

Comptes pour l'installation et l'exécution du Serveur d'administration

Nous vous recommandons d'exécuter l'installation du Serveur d'administration sous un compte d'administrateur local pour éviter d'utiliser des comptes de domaine pour accéder à la base de données du Serveur d'administration. L'ensemble des comptes requis et leurs privilèges dépendent du type de SGBD sélectionné, de l'emplacement du SGBD et du mode de création de la base de données du Serveur d'administration.

Lors de l'installation de Kaspersky Security Center, les groupes d'utilisateurs KLAdmins et KLOperators sont automatiquement formés. Ces groupes possèdent des privilèges de connexion au Serveur d'administration et de fonctionnement avec ses objets.

Selon le compte utilisateur sous lequel l'installation de Kaspersky Security Center se passe, les groupes KLAdmins et KLOperators sont créés de la manière suivante :

- Si l'application est installée sous un compte utilisateur inclus dans un domaine, les groupes sont créés sur l'appareil du Serveur d'administration et dans le domaine qui inclut le Serveur d'administration.
- Si l'application est installée sous un compte système, les groupes sont créés uniquement sur l'appareil du Serveur d'administration.

Afin d'éviter de créer les groupes KLAdmins et KLOperators dans le domaine et, par conséquent, d'**attribuer les privilèges d'administration du Serveur d'administration à un compte extérieur à l'appareil du Serveur d'administration**, nous vous recommandons d'installer Kaspersky Security Center sous un compte local.

Lors de l'installation du Serveur d'administration, sélectionnez le compte qui sera utilisé pour démarrer le Serveur d'administration en tant que service. Par défaut, l'application crée un compte local nommé KL-AK-*, sous lequel le service du Serveur d'administration (le service klserver) sera exécuté.

Si nécessaire, le service du Serveur d'administration peut être lancé sous le compte utilisateur sélectionné. Ce compte doit disposer des privilèges nécessaires pour accéder au SGBD. Pour des raisons de sécurité, utilisez un compte utilisateur sans privilège pour exécuter le service du Serveur d'administration.

Pour éviter l'utilisation de paramètres de compte incorrects, nous vous recommandons de créer le compte automatiquement.

Exclusion du Serveur d'administration d'un domaine

Si vous utilisez le Serveur d'administration pour protéger des groupes d'appareils du système essentiel, nous vous déconseillons d'inclure l'appareil dans le domaine. Cela vous permet de différencier les droits d'administration de Kaspersky Security Center et d'interdire l'accès au Serveur d'administration si le compte de domaine est compromis.

Veuillez noter que si vous installez le Serveur d'administration sur un appareil faisant partie du groupe de travail, les scénarios d'utilisation suivants du Serveur d'administration ne seront pas disponibles :

- Utilisation du cluster de basculement Kaspersky Security Center
- Utilisation du cluster de basculement Windows Server
- Utilisation du serveur SQL pour Windows sur un appareil distinct

  Vous pouvez utiliser le Serveur SQL pour Windows sur un appareil distinct uniquement si le Serveur d'administration et le Serveur SQL se trouvent dans le même domaine ou dans des domaines approuvés. Si le Serveur d'administration, le Serveur SQL et un partage UNC pour les sauvegardes se trouvent dans un groupe de travail, vous ne pouvez pas configurer de manière sécurisée les droits d'accès et de lecture-écriture entre le Serveur SQL et le partage.
- Installation à distance à l'aide des outils du Serveur d'administration à l'aide de stratégies de groupe Active Directory

S'il faut déconnecter le Serveur d'administration du domaine Active Directory, suivez les étapes décrites dans la section : Comment modifier le nom de Kaspersky Security Center.

S'il est nécessaire d'installer le Serveur d'administration sur l'appareil qui fait partie d'un groupe de travail, vous pouvez également utiliser Kaspersky Security Center Linux au lieu de Kaspersky Security Center Windows.

Sécurité des connexions

Utilisation de TLS

Nous vous recommandons d'interdire les connexions non sécurisées au Serveur d'administration. Par exemple, vous pouvez interdire les connexions qui utilisent HTTP dans les paramètres du Serveur d'administration.

Veuillez noter que par défaut, plusieurs ports HTTP du Serveur d'administration sont fermés. Le port restant est utilisé pour le serveur Internet du Serveur d'administration (8060). Ce port peut être limité par les paramètres du pare-feu de l'appareil du Serveur d'administration.

Paramètres TLS stricts

Il est recommandé d'utiliser le protocole TLS de version 1.2 ou suivante et de restreindre ou d'interdire les algorithmes de chiffrement non sécurisés.

Vous pouvez configurer les protocoles de chiffrement (TLS) utilisés par le Serveur d'administration. Veuillez noter qu'au moment de la publication d'une version du Serveur d'administration, les paramètres du protocole de chiffrement sont configurés par défaut pour garantir la sécurité du transfert des données.

Interdiction de l'authentification à distance à l'aide de comptes Windows

Vous pouvez utiliser l'indicateur LP_RestrictRemoteOsAuth pour interdire les connexions SSPI à partir d'adresses distantes. Cet indicateur permet d'interdire l'authentification à distance sur le Serveur d'administration à l'aide de comptes Windows locaux ou de domaine.

Pour basculer l'indicateur LP_RestrictRemoteOsAuth sur le mode d'interdiction des connexions à partir des adresses distantes :

1. Exécutez l'invite de commande Windows en utilisant les droits d'administrateur, puis remplacez votre répertoire actuel par celui contenant l'utilitaire klscflag. L'utilitaire klsclag se trouve dans le dossier dans lequel le Serveur d'administration est installé. Chemin d'installation par défaut est <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

2. Exécutez la commande suivante dans la ligne de commande pour spécifier la valeur de l'indicateur LP_RestrictRemoteOsAuth :

   ```
   klscflag.exe -fset -pv .core/.independent -s KLLIM -n LP_RestrictRemoteOsAuth -t d -v 1
   ```

3. Relancez le service du Serveur d'administration.

L'indicateur LP_RestrictRemoteOsAuth ne fonctionne pas si l'authentification à distance est effectuée via Kaspersky Security Center Web Console ou la Console d'administration installée sur l'appareil du Serveur d'administration.

Restriction de l'accès à la base de données du Serveur d'administration

Nous vous recommandons de restreindre l'accès à la base de données du Serveur d'administration. Par exemple, n'accordez l'accès qu'à partir de l'appareil du Serveur d'administration. Cela réduit la probabilité que la base de données du Serveur d'administration soit compromise en raison de vulnérabilités connues.

Vous pouvez configurer les paramètres conformément au mode d'emploi de la base de données utilisée, ainsi que fournir des ports fermés sur les pare-feu.

Authentification de Microsoft SQL Server

Si Kaspersky Security Center utilise Microsoft SQL Server comme SGBD, il est nécessaire de protéger les données de Kaspersky Security Center transférées vers ou depuis la base de données et les données stockées dans la base de données contre tout accès non autorisé. Pour ce faire, vous devez sécuriser la communication entre Kaspersky Security Center et SQL Server. Le moyen le plus fiable permettant d'assurer une communication sécurisée consiste à installer Kaspersky Security Center et le serveur SQL sur le même appareil et à utiliser le mécanisme de mémoire partagée pour les deux applications. Dans tous les autres cas, nous vous recommandons d'utiliser un certificat SSL/TLS pour authentifier l'instance du serveur SQL.

En général, le Serveur d'administration peut s'adresser au serveur SQL par l'intermédiaire des fournisseurs suivant :

- SQLOLEDB utilisant le protocole TCP/IP ou des canaux nommés

  Ce fournisseur est installé dans le système d'exploitation Windows et utilisé par défaut.

- MSOLEDBSQL utilisant le protocole TCP/IP, des canaux nommés ou la mémoire partagée

  Si vous voulez utiliser ce fournisseur, vous devez l'installer sur l'appareil doté du Serveur d'administration, puis définir la valeur `1` pour la variable d'environnement globale `KLDBADO_UseMSOLEDBSQL`.

- MSOLEDBSQL19 utilisant le protocole TCP/IP, des canaux nommés ou la mémoire partagée

  Si vous voulez utiliser ce fournisseur, vous devez l'installer sur l'appareil doté du Serveur d'administration, puis définir la valeur `1` pour la variable d'environnement globale `KLDBADO_UseMSOLEDBSQL` et la valeur `MSOLEDBSQL19` pour la variable d'environnement globale `KLDBADO_ProviderName`.

De plus, avant d'utiliser le protocole TCP/IP, les canaux nommés ou la mémoire partagée, assurez-vous que le protocole requis est activé.

Interaction de la sécurité avec un SGBD externe

Si le SGBD est installé sur un appareil distinct lors de l'installation du Serveur d'administration (SGBD externe), il est recommandé de configurer les paramètres d'interaction et d'authentification sécurisées avec ce SGBD. Pour en savoir plus sur la configuration de l'authentification SSL, consultez Authentification du serveur PostgreSQL et Scénario : Authentification du serveur MySQL.

Configuration de la liste d'autorisation d'adresses IP pour se connecter au Serveur d'administration

Par défaut, l'utilisateur de Kaspersky Security Center peut se connecter à Kaspersky Security Center depuis n'importe quel appareil sur lequel la Console d'administration basée sur MMC, Kaspersky Security Center Web Console ou les applications OpenAPI sont installés. Vous pouvez configurer le Serveur d'administration afin que les utilisateurs puissent s'y connecter uniquement à partir d'appareils avec des adresses IP autorisées. Par exemple, si un intrus tente de se connecter à Kaspersky Security Center via le serveur de Kaspersky Security Center Web Console installé sur un appareil qui ne figure pas dans la liste d'autorisation, il ne pourra pas se connecter à Kaspersky Security Center.

Configuration d'une liste d'autorisation d'adresses IP pour se connecter à Kaspersky Security Center Web Console

Par défaut, les utilisateurs de Kaspersky Security Center peuvent se connecter à Kaspersky Security Center Web Console depuis n'importe quel appareil. Sur un appareil disposant de Kaspersky Security Center Web Console, vous devez configurer le pare-feu (intégré au système d'exploitation ou à un autre) afin que les opérateurs puissent se connecter à Kaspersky Security Center Web Console uniquement à partir d'adresses IP autorisées.

Sécurité de la connexion au contrôleur de domaine pendant le sondage

Le Serveur d'administration ou un point de distribution Linux se connecte au contrôleur de domaine via LDAPS pour sonder le domaine. Par défaut, la vérification du certificat n'est pas requise lors de la connexion. Pour imposer la vérification des certificats, définissez l'indicateur `KLNAG_LDAP_TLS_REQCERT` sur 1. Vous pouvez également définir un chemin d'accès personnalisé à l'autorité de certification (CA) pour accéder à la chaîne de certificat à l'aide de l'indicateur `KLNAG_LDAP_SSL_CACERT`.

Comptes et authentification

Avant d'exécuter les étapes ci-dessous, créez une copie de sauvegarde du Serveur d'administration de Kaspersky Security Center à l'aide de la tâche Sauvegarde des données du Serveur d'administration ou de l'utilitaire klbackup et enregistrez-la dans un endroit sûr.

Utilisation de la vérification en deux étapes avec le Serveur d'administration

Kaspersky Security Center propose une vérification en deux étapes pour les utilisateurs de Kaspersky Security Center Web Console et de la Console d'administration, sur la base de la norme RFC 6238 (TOTP : Time-Based One-Time Password algorithm).

Lorsque la vérification en deux étapes est activée pour votre propre compte, chaque fois que vous vous connectez à Kaspersky Security Center Web Console ou à la Console d'administration, vous entrez votre nom d'utilisateur, votre mot de passe et un code de sécurité à usage unique supplémentaire. Si vous utilisez l'authentification de domaine pour votre compte, il vous suffit de saisir un code de sécurité supplémentaire à usage unique. Pour recevoir un code de sécurité à usage unique, vous devez installer une application d'authentification sur votre ordinateur ou sur votre appareil mobile.

Il existe des authentificateurs logiciels et matériels (tokens) qui prennent en charge la norme RFC 6238. Par exemple, les authentificateurs logiciels incluent Google Authenticator, Microsoft Authenticator, FreeOTP.

Il est fortement déconseillé d'installer l'application d'authentification sur l'appareil à partir duquel la connexion au Serveur d'administration est établie. Vous pouvez installer une application d'authentification sur votre appareil mobile.

Interdiction aux nouveaux utilisateurs de configurer eux-mêmes la vérification en deux étapes

Afin d'améliorer encore la sécurité d'accès à Kaspersky Security Center Web Console, vous pouvez interdire aux nouveaux utilisateurs de configurer eux-mêmes la vérification en deux étapes.

Si cette option est activée, un utilisateur dont la vérification en deux étapes est désactivée, par exemple un nouvel administrateur de domaine, ne peut pas configurer lui-même la vérification en deux étapes. Par conséquent, cet utilisateur ne peut pas être authentifié sur le Serveur d'administration et ne peut pas se connecter à Kaspersky Security Center Web Console sans l'approbation d'un autre administrateur de Kaspersky Security Center qui a déjà activé la vérification en deux étapes.

Utilisation de l'authentification à deux facteurs pour un système d'exploitation

Nous vous recommandons d'utiliser l'authentification multifacteur (MFA) pour l'authentification sur l'appareil du Serveur d'administration à l'aide d'un token, d'une carte à puce ou d'une autre méthode (si possible).

Interdiction d'enregistrer le mot de passe administrateur

Si vous utilisez Kaspersky Security Center Web Console, il est déconseillé d'enregistrer le mot de passe administrateur dans le navigateur installé sur la machine de l'utilisateur.

Utilisation de l'authentification à deux facteurs pour un système d'exploitation

Nous vous recommandons d'utiliser l'authentification multifacteur (MFA) pour l'authentification sur l'appareil du Serveur d'administration à l'aide d'un token, d'une carte à puce ou d'une autre méthode (si possible).

Interdiction d'enregistrer le mot de passe administrateur

Si vous utilisez la Console d'administration, il est déconseillé d'enregistrer le mot de passe administrateur dans la boîte de dialogue de connexion au Serveur d'administration.

Si vous utilisez Kaspersky Security Center Web Console, il est déconseillé d'enregistrer le mot de passe administrateur dans le navigateur installé sur la machine de l'utilisateur.

Authentification d'un compte utilisateur interne

Par défaut, le mot de passe d'un compte utilisateur interne du Serveur d'administration doit respecter les règles suivantes :

- Le mot de passe doit compter entre 8 et 256 caractères.
- Le mot de passe doit compter des caractères d'au moins trois des groupes ci-dessous :
  - Lettres majuscules (A-Z)
  - Lettre minuscules (a-z)
  - Chiffres (0-9)
  - Caractères spéciaux (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
- Le mot de passe ne peut pas contenir d'espaces, de caractères Unicode ou de la combinaison " . " et " @ " lorsque " . " est placé devant " @ ".

Par défaut, le nombre maximal de tentatives autorisées est de 10. Vous pouvez modifier le nombre de tentatives autorisées de saisie du mot de passe.

L'utilisateur de Kaspersky Security Center a droit à un nombre limité d'erreur lors de la saisie du mot de passe. Une fois cette limite atteinte, le compte utilisateur est bloqué pendant une heure.

Configuration des options de modification du mot de passe des comptes utilisateurs internes

Pour modifier le mot de passe d'un compte utilisateur interne, il est recommandé de configurer les paramètres suivants :

- Période de rotation des mots de passe
- Heure de l'avertissement préliminaire sur la nécessité de modifier le mot de passe
- Valeur de l'option **L'utilisateur doit changer son mot de passe lors de la première connexion**

Protection du compte contre les modifications non autorisées

Il est recommandé d'activer une option complémentaire pour protéger le compte utilisateur interne du Serveur d'administration contre les modifications non autorisées. Cette protection doit être configurée séparément pour chaque utilisateur interne.

Groupe d'administration dédié au Serveur d'administration

Nous vous recommandons de créer un groupe d'administration dédié pour le Serveur d'administration. Accordez à ce groupe des droits d'accès spéciaux et créez une stratégie de sécurité spéciale pour lui.

Pour éviter d'abaisser intentionnellement le niveau de sécurité du Serveur d'administration, nous vous recommandons de restreindre la liste des comptes qui peuvent gérer le groupe d'administration dédié.

Les groupes KLAdmins et KLOperators

Lors de l'installation de Kaspersky Security Center, les groupes d'utilisateurs KLAdmins et KLOperators sont automatiquement formés. Le groupe KLAdmins dispose de tous les droits d'accès. Le groupe KLOperators dispose uniquement des droits de lecture et d'exécution. Les droits accordés au groupe KLAdmins sont **verrouillés**.

Vous pouvez consulter les groupes KLAdmins et KLOperators et apporter des modifications à ces groupes à l'aide des outils d'administration standard du système d'exploitation.

Lors de l'élaboration des règles d'utilisation du Serveur d'administration, il est nécessaire de déterminer si le spécialiste de la sécurité de l'information a besoin d'un accès complet (et d'une inclusion dans le groupe KLAdmins) pour exécuter les tâches standard.

La plupart des tâches d'administration de base peuvent être réparties entre les services de l'entreprise (ou différents employés d'un même service) et, par conséquent, entre différents comptes. Vous pouvez également configurer la différenciation des accès des groupes d'administration dans Kaspersky Security Center. Par conséquent, il est possible de mettre en œuvre un scénario dans lequel l'autorisation sous les comptes du groupe KLAdmins sera anormale et pourrait être considérée comme un incident.

Si Kaspersky Security Center a été installé sous un compte système, les groupes sont créés uniquement sur l'appareil du Serveur d'administration. Dans ce cas, nous vous recommandons de vous assurer que seules les entrées créées lors de l'installation de Kaspersky Security Center sont incluses dans le groupe. Il est déconseillé d'ajouter des groupes au groupe KLAdmins (local et/ou de domaine) qui est créé automatiquement lors de l'installation de Kaspersky Security Center. Vous devez également limiter les droits de modification de ce groupe. Le groupe KLAdmins doit inclure uniquement des comptes utilisateurs non privilégiés.

Si l'installation a été effectuée sous un compte utilisateur de domaine, les groupes KLAdmins et KLOperators sont créés à la fois sur le Serveur d'administration et dans le domaine qui contient le Serveur d'administration. Une approche similaire, telle que l'installation d'un compte local, est recommandée.

Restriction de l'appartenance au rôle de l'Administrateur primaire

Nous vous recommandons de restreindre l'appartenance au rôle Administrateur primaire.

Par défaut, après l'installation du Serveur d'administration, le rôle Administrateur primaire est attribué au groupe des administrateurs locaux et au groupe KLAdmins créé. Il est utile pour l'administration, mais il est essentiel du point de vue de la sécurité, car le rôle Administrateur primaire dispose d'un large éventail de privilèges, l'attribution de ce rôle aux utilisateurs doit être strictement réglementée.

Les administrateurs locaux peuvent être exclus de la liste des utilisateurs dotés des privilèges d'administrateur de Kaspersky Security Center. Le rôle Administrateur primaire ne peut pas être supprimé du groupe KLAdmins. Vous pouvez inclure dans le groupe KLAdmins les comptes qui seront utilisés pour administrer le Serveur d'administration.

Si vous utilisez l'authentification de domaine, nous vous recommandons de restreindre les privilèges des comptes d'administrateur de domaine dans Kaspersky Security Center. Par défaut, ces comptes ont le rôle d'administrateur primaire. De plus, un administrateur de domaine peut inclure son compte dans le groupe KLAdmins pour obtenir le rôle d'administrateur primaire. Pour éviter cela, dans les paramètres de sécurité de Kaspersky Security Center, vous pouvez ajouter le groupe Administrateurs du domaine, puis définir des règles d'interdiction pour celui-ci. Ces règles doivent primer sur les règles d'autorisation.

Vous pouvez également utiliser les rôles d'utilisateurs prédéfinis avec un ensemble de droits déjà configuré.

Configuration des droits d'accès aux fonctionnalités de l'application.

Nous vous recommandons d'utiliser une configuration flexible des droits d'accès aux fonctionnalités de Kaspersky Security Center pour chaque utilisateur ou groupe d'utilisateurs.

Le contrôle d'accès basé sur les rôles permet de créer des rôles d'utilisateurs standard avec un ensemble prédéfini de droits et d'attribuer ces rôles aux utilisateurs en fonction de l'étendue de leurs tâches.

Les principaux avantages du modèle de contrôle d'accès basé sur les rôles :

- Facilité d'administration
- Hiérarchie des rôles
- Approche du moindre privilège
- Séparation des tâches

Vous pouvez attribuer des rôles prédéfinis à certains employés en fonction de leur poste ou créer des rôles entièrement nouveaux.

Lors de la configuration des rôles, tenez compte des privilèges liés à la modification de l'état de protection de l'appareil doté du Serveur d'administration et à l'installation à distance de logiciels tiers :

- Administration des groupes d'administration.
- Opérations avec le Serveur d'administration.
- Installation à distance.
- Modification des paramètres de stockage des événements et d'envoi des notifications.

  Ce privilège vous permet de définir des notifications qui exécutent un script ou un module exécutable sur l'appareil du Serveur d'administration lorsqu'un événement se produit.

Compte séparé pour l'installation à distance des applications

En plus de la différenciation de base des droits d'accès, nous recommandons de restreindre l'installation à distance des applications pour tous les comptes (à l'exception de l'administrateur principal ou d'un autre compte spécialisé).

Nous vous recommandons d'utiliser un compte distinct pour l'installation à distance des applications. Vous pouvez attribuer un rôle ou des autorisations à un compte distinct.

Sécurisation des accès privilégiés Windows

Nous vous recommandons de prendre en compte les recommandations de Microsoft concernant la sécurité des accès à privilèges. Pour consulter ces recommandations, consultez la section Sécurisation des accès à privilèges article.

L'un des points clés des recommandations est la mise en œuvre des postes de travail à accès privilégié (PAW).

Utilisation d'un compte de service administré (MSA) ou d'un groupe de comptes de service administrés (gMSA) pour exécuter le service du Serveur d'administration

Active Directory dispose d'un type spécial de comptes pour l'exécution sécurisée des services, appelé compte de service administré de groupe (MSA/gMSA). Kaspersky Security Center est compatible avec les comptes de service administrés (MSA) et les comptes de service administrés de groupe (gMSA). Si ces comptes utilisateurs sont utilisés dans votre domaine, vous pouvez en choisir un comme compte pour le service du Serveur d'administration.

Audit régulier de tous les utilisateurs et de leurs actions

Nous vous recommandons d'effectuer un audit régulier de tous les utilisateurs sur l'appareil du Serveur d'administration. Cela vous permet de réagir à certains types de menaces pour la sécurité associées à une éventuelle compromission de l'appareil.

En outre, vous pouvez suivre les actions de l'utilisateur, telles que la connexion et la déconnexion du Serveur d'administration, la connexion au Serveur d'administration avec une erreur et la modification des objets (pour les objets qui prennent en charge la gestion des révisions).

Gestion de la protection du Serveur d'administration

Sélection d'un logiciel de protection du Serveur d'administration

En fonction du type de déploiement du Serveur d'administration et de la stratégie générale de protection, sélectionnez l'application pour protéger l'appareil du Serveur d'administration.

Si vous déployez le Serveur d'administration sur un appareil dédié, nous vous recommandons de sélectionner l'application Kaspersky Endpoint Security pour protéger l'appareil du Serveur d'administration. Cela permet d'appliquer toutes les technologies disponibles pour protéger l'appareil du Serveur d'administration, y compris les modules d'analyse comportementale.

Si le Serveur d'administration est installé sur un appareil qui existe dans l'infrastructure et qui a déjà été utilisé pour d'autres tâches, nous vous recommandons d'utiliser le logiciel de protection suivant :

- Kaspersky Industrial CyberSecurity for Nodes. Nous vous recommandons d'installer cette application sur les appareils qui font partie d'un réseau industriel. Kaspersky Industrial CyberSecurity for Nodes est une application qui possède des certificats de compatibilité avec divers fabricants de logiciels industriels.

- Solutions de sécurité recommandées. Si le Serveur d'administration est installé sur un appareil avec d'autres logiciels, nous vous recommandons de prendre en compte les recommandations de cet éditeur de logiciel sur la compatibilité des solutions de sécurité (il existe peut-être déjà des recommandations pour le choix d'une solution de sécurité et vous devrez peut-être configurer la zone de confiance).

Création d'une stratégie de sécurité distincte pour l'application de protection

Nous vous recommandons de créer une stratégie de sécurité distincte pour l'application qui protège l'appareil du Serveur d'administration. Cette stratégie doit être différente de la stratégie de sécurité pour les appareils clients. Cela permet de définir les paramètres de sécurité les plus appropriés pour le Serveur d'administration, sans affecter le niveau de protection des autres appareils.

Nous vous recommandons de diviser les appareils en groupes, puis de placer l'appareil du Serveur d'administration dans un groupe distinct pour lequel vous pouvez créer une stratégie de sécurité spéciale.

Modules de protection

S'il n'y a pas de recommandations particulières de l'éditeur du logiciel tiers installé sur le même appareil que le Serveur d'administration, nous vous recommandons d'activer et de configurer tous les modules de protection disponibles (après avoir vérifié le fonctionnement de ces modules de protection pendant un certain temps).

Configuration du pare-feu de l'appareil du Serveur d'administration

Sur l'appareil du Serveur d'administration, il est recommandé de configurer le pare-feu pour restreindre le nombre d'appareils à partir desquels les administrateurs peuvent se connecter au Serveur d'administration via la Console d'administration ou Kaspersky Security Center Web Console.

Par défaut, le Serveur d'administration utilise le port 13291 pour recevoir les connexions de la Console d'administration et le port 13299 pour recevoir les connexions de Kaspersky Security Center Web Console. Nous vous recommandons de restreindre le nombre d'appareils à partir desquels le Serveur d'administration peut être administré à l'aide de ces ports.

Gestion de la protection des appareils clients

Restriction de l'ajout de clés de licence aux paquets d'installation

Les paquets d'installation sont stockés dans le dossier partagé du Serveur d'administration, dans le sous-dossier Paquets. Si vous ajoutez une clé de licence à un paquet d'installation, la clé de licence peut être compromise car les droits d'accès en lecture partagés sont activés pour le stockage des paquets d'installation.

Pour éviter de compromettre la clé de licence, il est déconseillé d'ajouter des clés de licence aux paquets d'installation.

Nous vous recommandons d'utiliser la distribution automatique des clés de licence sur les appareils administrés, le déploiement via la tâche Ajouter une clé de licence pour une application administrée et l'ajout manuel d'un code d'activation ou d'un fichier clé sur les appareils.

Règles automatiques de déplacement des appareils entre les groupes d'administration

Il est conseillé de restreindre l'utilisation des règles automatiques de déplacement des appareils entre les groupes d'administration.

Si vous utilisez des règles automatiques pour le déplacement des appareils, cela peut entraîner la propagation de stratégies qui accordent plus de privilèges à l'appareil déplacé que l'appareil n'en avait avant le déplacement.

De plus, le déplacement d'un appareil client vers un autre groupe d'administration peut entraîner la propagation des paramètres de la stratégie. Ces paramètres de stratégie peuvent être indésirables pour la distribution aux appareils invités et non approuvés.

Cette recommandation ne s'applique pas à l'affectation initiale unique des appareils aux groupes d'administration.

Exigences de sécurité pour les points de distribution et les passerelles de connexion

Les appareils dotés de l'Agent d'administration peuvent faire office de point de distribution et remplir les fonctions suivantes :

- Diffusez les mises à jour et les paquets d'installation reçus du Serveur d'administration sur les appareils clients au sein du groupe.
- Effectuez l'installation à distance de logiciels tiers et d'applications Kaspersky sur les appareils clients.
- Sonder le réseau dans le but de détecter de nouveaux appareils et de mettre à jour les informations sur les appareils détectés. Le point de distribution peut utiliser les mêmes méthodes de détection des appareils que le Serveur d'administration.

Placement des points de distribution sur le réseau de l'organisation utilisés pour :

- Réduire la charge sur le Serveur d'administration
- Optimisation du trafic
- Accorder au Serveur d'administration un accès aux appareils situés dans des parties difficiles d'accès du réseau

Compte tenu des capacités disponibles, nous recommandons de protéger les appareils qui font office de points de distribution contre tout type d'accès non autorisé (y compris physiquement).

Restriction de l'attribution automatique des points de distribution

Pour simplifier l'administration et maintenir le fonctionnement du réseau, nous vous recommandons d'utiliser l'attribution automatique des points de distribution. Cependant, pour les réseaux industriels et les petits réseaux, nous vous déconseillons d'attribuer automatiquement des points de distribution, car, par exemple, les informations privées des comptes utilisés pour transmettre les tâches d'installation à distance peuvent être transférées aux points de distribution au moyen de le système d'exploitation.

Pour les réseaux industriels et les petits réseaux, vous pouvez désigner manuellement des appareils comme points de distribution.

Vous pouvez également consulter le Rapport d'activité des points de distribution.

Exigences de sécurité pour les appareils des utilisateurs de Kaspersky Security Center

Les appareils des utilisateurs de Kaspersky Security Center doivent faire l'objet d'exigences particulières en matière de sécurité. Il est conseillé de protéger ces appareils contre tout type d'accès non autorisé (y compris physique) :

Voici quelques-uns des appareils utilisés par les utilisateurs de Kaspersky Security Center :

- Appareils à partir desquels les utilisateurs se connectent à Kaspersky Security Center Web Console à l'aide d'un navigateur.
- Appareils à partir desquels l'utilisateur se connecte à Kaspersky Security Center en utilisant la Console d'administration basée sur MMC.
- Les appareils à partir desquels les applications qui interagissent avec le Serveur d'administration via OpenAPI sont connectés à Kaspersky Security Center.

Exigences de sécurité pour les appareils sur lesquels le programme d'installation de Kaspersky Security Center Web Console est installé

Les appareils sur lesquels Kaspersky Security Center Web Console est installé sont utilisés pour gérer Kaspersky Security Center. Des exigences particulières doivent donc s'appliquer à la sécurité de ces appareils. Il est conseillé de protéger ces appareils contre tout type d'accès non autorisé (y compris physique).

Configuration de la protection des applications administrées

Stratégies d'application administrées

Nous vous recommandons de créer une stratégie pour chaque type des applications utilisées et des modules de Kaspersky Security Center (Agent d'administration, Kaspersky Endpoint Security for Windows, Kaspersky Endpoint Agent et autres). Cette stratégie doit être appliquée à tous les appareils administrés (le groupe d'administration racine) ou à un groupe distinct vers lequel les nouveaux appareils administrés sont automatiquement déplacés conformément aux règles de déplacement configurées.

Définition du mot de passe pour la désactivation de la protection et la désinstallation de l'application

Pour empêcher les intrus de désactiver les applications de sécurité de Kaspersky, nous vous recommandons fortement d'activer la protection par mot de passe pour désactiver la protection et de désinstaller les applications de sécurité de Kaspersky. Vous pouvez définir le mot de passe, par exemple, pour Kaspersky Endpoint Security for Windows, Kaspersky Security for Windows Servers, l'Agent d'administration et d'autres applications de Kaspersky. Après avoir activé la protection par mot de passe, nous vous recommandons de verrouiller ces paramètres en fermant le " cadenas ".

Spécification du mot de passe pour la connexion manuelle de l'appareil client au Serveur d'administration (utilitaire klmover)

L'utilitaire klmover vous permet de connecter manuellement un appareil client au Serveur d'administration. Lors de l'installation de l'Agent d'administration sur l'appareil client, l'utilitaire est automatiquement copié dans le dossier d'installation de l'Agent d'administration.

Pour éviter que des intrus ne puissent déplacer des appareils hors du contrôle de votre Serveur d'administration, nous vous recommandons vivement d'activer la protection par mot de passe pour le lancement de l'utilitaire klmover. Pour activer la protection par mot de passe, sélectionnez l'option **Utiliser un mot de passe de désinstallation** dans les paramètres de stratégie de l'Agent d'Administration.

L'utilitaire klmover requiert des droits d'administrateur local. La protection par mot de passe pour le fonctionnement de l'utilitaire klmover peut être omise pour les appareils administrés sans les droits d'administrateur local.

L'activation de l'option **Utiliser un mot de passe de désinstallation** active également la protection par un mot de passe du nettoyage (cleaner.exe).

Utilisation de Kaspersky Security Network

Dans toutes les stratégies des applications administrées et dans les propriétés du Serveur d'administration, nous vous recommandons d'activer l'utilisation de Kaspersky Security Network (KSN) et d'accepter la Déclaration de KSN. Lorsque vous mettez à jour ou mettez à niveau le Serveur d'administration, vous pouvez accepter la Déclaration KSN mise à jour. Dans certains cas, lorsque l'utilisation des services Cloud est interdite par la loi ou d'autres réglementations, vous pouvez désactiver KSN.

Analyse régulière des appareils administrés

Pour tous les groupes d'appareils, nous vous recommandons de créer une tâche qui exécute périodiquement une analyse complète des appareils.

Découverte de nouveaux appareils

Nous vous recommandons de configurer correctement les paramètres de recherche d'appareils : configurez l'intégration à Active Directory et spécifiez les plages d'adresses IP pour la recherche de nouveaux appareils.

Pour des raisons de sécurité, vous pouvez utiliser le groupe d'administration par défaut qui inclut tous les nouveaux appareils et les stratégies par défaut affectant ce groupe.

Définition du dossier partagé

Si vous déployez le Serveur d'administration sur l'appareil fonctionnant sous Windows en sélectionnant un dossier partagé existant (utilisé, par exemple, pour le placement des paquets d'installation et le stockage des bases de données mises à jour), nous vous recommandons de vous assurer que les droits de lecture sont accordés au groupe Tout le monde, et les droits d'écriture sont accordés au groupe KLAdmins.

Maintenance du Serveur d'administration

Copie de sauvegarde des données du Serveur d'administration

La sauvegarde des données vous permet de restaurer les données du Serveur d'administration sans perte de données.

Par défaut, une tâche de sauvegarde des données est créée automatiquement après l'installation du Serveur d'administration et est exécutée périodiquement, en enregistrant les sauvegardes dans le répertoire approprié. Les paramètres de la tâche de sauvegarde des données peuvent être modifiés comme suit :

- La fréquence de sauvegarde augmente
- Un répertoire spécial pour l'enregistrement des copies est indiqué
- Les mots de passe pour les copies de sauvegarde sont modifiés

Si vous stockez les copies de sauvegarde dans un répertoire spécial, différent du répertoire par défaut, nous vous recommandons de limiter la liste de contrôle d'accès (ACL) à ce répertoire. Les comptes utilisateur du Serveur d'administration et les comptes utilisateur de la base de données du Serveur d'administration doivent disposer des droits d'accès en écriture pour ce répertoire.

Maintenance du Serveur d'administration

La maintenance du Serveur d'administration permet de réduire le volume de celle-ci, d'augmenter la productivité et la fiabilité de fonctionnement de l'application. Il est recommandé de procéder à la maintenance du Serveur d'administration au moins une fois par semaine.

La maintenance du Serveur d'administration s'effectue à l'aide de la tâche correspondante. Pendant la maintenance du Serveur d'administration, l'application exécute les opérations suivantes :

- Elle recherche les erreurs dans la base de données
- Elle réorganise les indices de la base de données
- Elle met à jour les statistiques de la base de données
- Elle comprime la base de données (si nécessaire)

Installation des mises à jour du système d'exploitation et des mises à jour logicielles tierces

Nous vous recommandons vivement d'installer régulièrement les mises à jour logicielles pour le système d'exploitation et les logiciels tiers sur l'appareil du Serveur d'administration.

Les appareils clients ne nécessitent pas une connexion continue au Serveur d'administration, vous pouvez donc redémarrer l'appareil du Serveur d'administration en toute sécurité après l'installation des mises à jour. Tous les événements enregistrés sur les appareils clients pendant l'arrêt du Serveur d'administration lui sont envoyés après le rétablissement de la connexion.

Transfert d'événements vers des systèmes tiers

Surveillance et rapports

Pour une réponse rapide aux problèmes de sécurité, nous vous recommandons de configurer les fonctionnalités de surveillance et de création de rapports.

Exportation des événements dans les systèmes SIEM

Pour une réponse rapide aux problèmes de sécurité avant que des dommages importants ne surviennent, nous vous recommandons d'utiliser l'exportation d'événements dans un système SIEM.

Notifications par e-mail des événements de l'audit

Kaspersky Security Center vous permet d'obtenir des informations sur les événements survenus pendant le fonctionnement du Serveur d'administration et des applications Kaspersky installées sur les appareils administrés. Pour une réponse rapide aux urgences, nous vous recommandons de configurer le Serveur d'administration pour envoyer des notifications sur les événements d'audit, les événements critiques, les événements d'échec et les avertissements qu'il publie.

Étant donné que ces événements sont des événements intra-système, un petit nombre d'entre eux peut être attendu, ce qui est tout à fait applicable pour le mailing.

Statistiques de la fonction Serveur d'administration

Pour réagir rapidement aux problèmes de sécurité, il est recommandé de configurer l'envoi des statistiques de la fonctionnalité du Serveur d'administration à des applications tierces, en utilisant le protocole SNMP (Simple Network Management Protocol).

Recommandations de sécurité pour les systèmes d'information des tiers

Recommandations de sécurité de CIS Benchmarks

Si vous utilisez des versions de systèmes d'exploitation, de plateformes de virtualisation ou de serveurs de base de données prises en charge par le Serveur d'administration et l'Agent d'administration, nous vous recommandons d'appliquer les pratiques exemplaires en matière de sécurité de l'information du Center for Internet Security (CIS), le cas échéant, afin de paramétrer au mieux ces systèmes d'information.

Le Centre pour la sécurité d'Internet (CIS) est une organisation à but non lucratif qui se consacre à l'amélioration de la sécurité dans le domaine des technologies de l'information. Le CIS élabore et diffuse notamment des normes de sécurité comme CIS Controls et CIS Benchmarks. Celles-ci constituent un ensemble de recommandations et de pratiques permettant d'assurer la sécurité des systèmes d'information.

Le portail CIS contient des recommandations pour les versions des systèmes d'information suivants prises en charge par le Serveur d'administration et l'Agent d'administration :

- Les systèmes d'exploitation des catégories suivantes :
  - Windows pour les ordinateurs de bureau
  - Windows pour les serveurs
  - Debian
  - Ubuntu
  - CentOS
  - Oracle Linux
  - Red Hat Enterprise Linux
  - SUSE Linux Enterprise Server
  - macOS
- Plateformes de virtualisation VMware
- Serveurs de bases de données :
  - Microsoft SQL Server
  - MySQL
  - MariaDB
  - PostgreSQL

Recommandations de sécurité pour le système d'exploitation Astra Linux

Si vous utilisez le système d'exploitation Astra Linux, il convient de suivre les recommandations de sécurité décrites dans le livre rouge pour la version correspondante d'Astra Linux.

Recommandations de sécurité pour le système d'exploitation RED OS

Si vous utilisez le système d'exploitation RED OS, il convient de suivre les recommandations de sécurité du guide de l'administrateur décrites dans la documentation officielle de RED OS.

Recommandations relatives à l'utilisation des applications de sécurité de Kaspersky

Utilisation du mot de passe KLAdmin dans Kaspersky Endpoint Security for Windows

Plusieurs utilisateurs avec différents niveaux de connaissances en informatique peuvent partager un appareil sur lequel est installé Kaspersky Endpoint Security for Windows. Si les utilisateurs ont un accès illimité à Kaspersky Endpoint Security for Windows et à ses paramètres, le niveau général de protection de l'appareil peut être réduit. La protection par mot de passe permet de restreindre l'accès des utilisateurs à Kaspersky Endpoint Security for Windows, en fonction des autorisations qui leur ont été accordées (par exemple, l'autorisation de quitter l'application).

L'un des moyens de limiter l'accès à Kaspersky Endpoint Security for Windows et à ses paramètres consiste à utiliser un compte KLAdmin. Le compte KLAdmin est un compte administrateur avec un accès libre à Kaspersky Endpoint Security for Windows. Le compte KLAdmin a le droit d'effectuer toute action protégée par mot de passe dans Kaspersky Endpoint Security for Windows. Les autorisations du compte KLAdmin ne peuvent pas être révoquées. Vous pouvez définir le mot de passe du compte KLAdmin dans les propriétés de la stratégie de Kaspersky Endpoint Security for Windows. L'administrateur de Kaspersky Endpoint Security for Windows est entièrement responsable de la protection du mot de passe du compte KLAdmin. Si votre organisation a sa propre stratégie de mot de passe, suivez les instructions de cette stratégie.

Voici nos recommandations pour protéger l'organisation contre le vol du mot de passe KLAdmin :

- **Exigences générales**

  N'utilisez pas le nom du compte ou une partie de son nom comme mot de passe.

- **Longueur minimale du mot de passe requise**

  Créez un mot de passe d'au moins 10 caractères.

- **Conditions d'utilisation de plusieurs types de caractères**

  Définissez un mot de passe complexe qui contient des caractères de différentes catégories : lettres minuscules et majuscules, chiffres et caractères spéciaux.

- **Conditions d'expiration du mot de passe**

  Définissez une date d'expiration minimum du mot de passe de 90 jours. Le nouveau mot de passe ne doit correspondre à aucun des 24 derniers mots de passe.

Préparatifs du déploiement

Cette section décrit les étapes à suivre absolument avant de pouvoir déployer Kaspersky Security Center.

Planification du déploiement de Kaspersky Security Center

Cette section contient des informations sur les options optimales de déploiement des modules de Kaspersky Security Center sur le réseau de l'entreprise en fonction de différents facteurs :

- Nombre total d'appareils
- Existence de divisions organisationnelles ou territoriales (bureaux, filiales)
- Présence de réseaux isolés reliés par les canaux étroits
- Possibilité d'accès au Serveur d'administration via Internet

Schémas typiques de déploiement du système de protection

Cette section décrit les schémas typiques de déploiement du système de protection dans le réseau de l'entreprise à l'aide de Kaspersky Security Center.

Il est indispensable de protéger le système contre tout type d'accès non autorisé. Nous vous recommandons d'installer toutes les mises à jour de la protection disponibles pour votre système d'exploitation avant d'installer l'application sur votre appareil et de protéger physiquement le(s) Serveur(s) d'administration et de mettre à jour le ou les point(s) de distribution.

Vous pouvez déployer le système de protection dans le réseau de l'entreprise à l'aide de Kaspersky Security Center, en utilisant les schémas suivants de déploiement :

- Le déploiement du système de protection via les outils de Kaspersky Security Center à l'aide d'un des moyens suivants :
  - Par la Console d'administration
  - Par Kaspersky Security Center Web Console

  L'installation des applications de Kaspersky sur les appareils client et la connexion des appareils clients au Serveur d'administration ont lieu automatiquement à l'aide de Kaspersky Security Center.

  Le schéma principal de déploiement est le déploiement du système de protection via la Console d'administration. L'utilisation de Kaspersky Security Center Web Console permet de lancer l'installation des applications de Kaspersky via le navigateur.
- Le déploiement manuel du système de protection à l'aide des paquets d'installation autonomes, formés dans Kaspersky Security Center.

  L'installation des applications de Kaspersky sur les appareils client et le poste de travail de l'administrateur s'opère manuellement. Les paramètres de connexion des appareils client au Serveur d'administration sont définis lors de l'installation de l'Agent d'administration.

  Cette option de déploiement est recommandée dans les cas, quand l'installation à distance n'est pas possible.

Kaspersky Security Center permet aussi de déployer votre système de protection à l'aide des stratégies de groupe Active Directory®.

À propos de la planification du déploiement de Kaspersky Security Center dans le réseau de l'entreprise

Un Serveur d'administration peut servir un maximum de 100 000 appareils. Si le total des appareils sur le réseau de l'entreprise est supérieur à 100 000, il faut installer sur le réseau de l'entreprise plusieurs Serveurs d'administration regroupés dans une hiérarchie pour simplifier l'administration centralisée.

Si l'entreprise compte de gros bureaux dans différentes régions (filiales) dotés de leurs propres administrateurs, il convient de placer des Serveurs d'administration dans ces bureaux. Dans le cas contraire, ces bureaux doivent être considérés comme des réseaux isolés reliés par des canaux étroits, cf. section " Configuration typique : quelques bureaux importants répartis géographiquement avec leurs propres administrateurs ".

En présence de réseaux isolés reliés par des canaux étroits, il faut désigner un ou plusieurs Agents d'administration en tant que points de distribution (cf. le tableau pour le calcul de la quantité des points de distribution), dans le but d'économiser le trafic dans ces réseaux. Dans ce cas, tous les appareils du réseau isolé recevront les mises à jour de ces centres de mises à jour locaux. Les points de distribution eux-mêmes peuvent télécharger les mises à jour depuis le Serveur d'administration (comportement par défaut) ou depuis des serveurs de Kaspersky sur Internet, cf. la section « Configuration typique : plusieurs petits bureaux répartis géographiquement ».

La section « Configurations typiques de Kaspersky Security Center » reprend des descriptions détaillées des configurations typiques de Kaspersky Security Center. Lors de la planification du déploiement, il faut, en fonction de la structure de l'entreprise, choisir la configuration typique qui convient le mieux.

Lors de la planification du déploiement, il faut examiner la nécessité d'attribuer au Serveur d'administration un certificat spécial X.509. L'attribution d'un certificat X.509 au Serveur d'administration peut se justifier dans les cas suivants (liste non-exhaustive) :

- Pour inspecter le trafic SSL à l'aide d'un proxy de terminaison SSL ou pour utiliser un proxy inverse
- Pour l'intégration avec l'infrastructure à clés publiques (PKI) de l'entreprise
- Pour attribuer les valeurs souhaitées des champs du certificat
- Pour garantir la robustesse souhaitée du chiffrement du certificat

Sélection de la structure de protection de la société

La sélection de la structure de protection de l'entreprise est définie par les facteurs suivants :

- La topologie du réseau de l'entreprise.
- La structure d'organisation.
- Le nombre d'employés qui sont responsables de la protection du réseau et de la diffusion des obligations entre eux.
- Les ressources matérielles qui peuvent être indiquées pour installer les modules d'administration de la protection.

- La capacité de transmission des voies de communication qui peuvent être indiquées pour le fonctionnement des modules de protection dans le réseau d'une entreprise.

- Le temps d'exécution disponible des opérations administratives indispensables dans le réseau de l'entreprise. Les opérations d'administration indispensables reprennent, par exemple, la diffusion des mises à jour des bases antivirus et la modification des stratégies pour les appareils clients.

Lors de la sélection de la structure de la protection, il est recommandé de définir tout d'abord les ressources matérielles et réseau existantes qui peuvent être utilisées pour le fonctionnement du système centralisé de protection.

Afin d'analyser l'infrastructure de réseau et matérielle, la succession suivante d'actions est prévue :

1. Définir les paramètres suivants du réseau à déployer la protection :

   - Nombre de segments du réseau.

   - Vitesse des liaisons entre les segments du réseau particuliers.

   - Nombre d'appareils administrés dans chacun des segments du réseau.

   - capacité de transmission de chaque liaison qui peut être indiquée pour le fonctionnement de la protection.

2. Définir la durée admise pour l'exécution des opérations d'administration clés sur tous les appareils administrés.

3. Analyser les informations des points 1 et 2, ainsi que les données du test de charge du système d'administration. Répondre aux questions sur la base de l'analyse réalisée :

   - Est-il possible de maintenir tous les clients par un seul Serveur d'administration ou faut-il avoir une hiérarchie des Serveurs d'administration ?

   - Quelle configuration matérielle des Serveurs d'administration est requise pour maintenir tous les clients pendant le temps défini dans le point 2 ?

   - Faut-il utiliser les points de distribution pour diminuer la charge sur les canaux de liaison ?

Après avoir répondu aux questions citées à l'étape 3 ci-dessus, vous pouvez composer l'ensemble des structures accessibles de la protection de l'entreprise.

Le réseau de l'entreprise permet d'utiliser une des structures types de la protection :

- Un Serveur d'administration. Tous les appareils clients connectés à un Serveur d'administration. Le Serveur d'administration joue rôle de point de distribution.

- Un Serveur d'administration avec des points de distribution. Tous les appareils clients connectés à un Serveur d'administration. Les appareils clients qui remplissent la fonction de points de distribution sont mis en évidence dans le réseau.

- Hiérarchie des Serveurs d'administration. Pour chaque segment du réseau, un Serveur d'administration séparé inclus dans la hiérarchie partagée des Serveurs d'administration est indiqué. Le Serveur d'administration principal joue rôle de point de distribution.

- Hiérarchie des serveurs d'administration avec des points de distribution. Pour chaque segment du réseau, un Serveur d'administration séparé inclus dans la hiérarchie partagée des Serveurs d'administration est indiqué. Les appareils clients qui remplissent la fonction de points de distribution sont mis en évidence dans le réseau.

Configurations typiques de Kaspersky Security Center

Cette section présente les configurations typiques suivantes pour le déploiement des modules de Kaspersky Security Center dans le réseau d'une entreprise :

- Un bureau
- Quelques bureaux importants répartis géographiquement avec leurs propres administrateurs
- Plusieurs petits bureaux répartis géographiquement

Configuration typique : un bureau

Le réseau de l'entreprise peut compter un ou plusieurs Serveurs d'administration. La quantité de Serveurs peut être choisie en fonction du matériel disponible, ainsi qu'en fonction du total d'appareils administrés.

Un Serveur d'administration peut servir jusqu'à 100 000 appareils. Il faut prendre en considération la possibilité d'augmenter la quantité d'appareils administrés dans un proche avenir : il peut être souhaitable de connecter un peu moins d'appareils à un Serveur d'administration.

Les Serveurs d'administration peuvent être installés dans le réseau interne ou dans la zone démilitarisée, en fonction de la nécessité de pouvoir accéder aux Serveurs d'administration depuis Internet.

S'il existe plusieurs Serveurs, il est conseillé de les regrouper dans une hiérarchie. L'existence d'une hiérarchie de Serveurs d'administration permet d'éviter le dédoublement de stratégies et de tâches, de travailler avec tous les appareils administrés comme s'ils étaient administrés par un seul Serveur d'administration : exécuter la recherche d'appareils, créer des sélections d'appareils, créer des rapports.

Configuration typique : quelques bureaux importants répartis géographiquement avec leurs propres administrateurs

Si une organisation dispose de quelques bureaux à grande échelle et géographiquement séparés, vous devez envisager la possibilité de déployer des Serveurs d'administration dans chacun de ces bureaux. Un ou plusieurs Serveurs d'administration peuvent être déployés par bureau, selon le nombre d'appareils client et de matériel disponibles. Dans ce cas, chacun des bureaux peut être abordé comme un cas de " Configuration typique : un bureau ". Pour faciliter l'administration, il est recommandé de combiner tous les Serveurs d'administration en une hiérarchie (éventuellement à plusieurs niveaux).

Si certains employés se déplacent avec leurs appareils (ordinateurs portables) d'un bureau à l'autre, créez des profils de connexion de l'Agent d'administration dans la stratégie de l'Agent d'administration. Les profils de connexion de l'Agent d'administration ne sont pris en charge que pour les appareils Windows et macOS.

Configuration typique : plusieurs petits bureaux isolés

Cette configuration standard prévoit un siège social et une multitude de petits bureaux distants, probablement reliés au siège principal via Internet. Il se peut que chacun des bureaux distants se trouve au-delà du Network Address Translation (NAT), c'est-à-dire que la connexion d'un bureau distant à un autre est impossible car les bureaux sont isolés.

Un Serveur d'administration doit être déployé au siège et un ou plusieurs points de distribution dans les autres bureaux doivent être désignés. Si la communication entre les bureaux s'opère via Internet, il peut être utile de créer pour les points de distribution une tâche *Télécharger les mises à jour sur les stockages des points de distribution* afin que les agents de mises à jour téléchargent la mise à jour non pas depuis le Serveur d'administration, mais directement depuis les serveurs de Kaspersky, ou d'un dossier local ou réseau.

Si une partie des appareils dans un bureau distant n'a pas d'accès direct au Serveur d'administration (par exemple, l'accès au Serveur d'administration s'opère via Internet, mais certains appareils n'ont pas d'accès Internet), il faut basculer les points de distribution en mode de passerelle (Connection Gateway). Dans ce cas, les Agents d'administration sur les appareils dans un bureau distant se connectent (pour la synchronisation) au Serveur d'administration non pas directement mais via la passerelle.

Dans la mesure où le Serveur d'administration ne peut probablement pas sonder le réseau dans le bureau distant, il est préférable de confier cette fonction à un des points de distribution.

Le Serveur d'administration ne peut pas envoyer les notifications sur le port 15000 UDP aux appareils administrés situés au-delà du NAT dans le bureau distant. Pour résoudre ce problème, vous pouvez activer le mode de maintien de la connexion au Serveur d'administration dans les propriétés des appareils qui sont des points de distribution (case **Maintenir la connexion au Serveur &d'administration**). Ce mode est accessible si le total des points de distribution n'est pas supérieur à 300. Utilisez des serveurs push pour garantir la continuité de la connexion entre l'appareil administré et le Serveur d'administration. Pour plus de détails, reportez-vous à la rubrique suivante : Utilisation d'un point de distribution en tant que serveur push.

Sélection d'un SGBD pour le Serveur d'administration

Au moment de choisir un SGBD qui va être utilisé par le Serveur d'administration, il faut tenir compte du nombre d'appareils desservis par le Serveur d'administration.

Le tableau suivant répertorie les options de SGBD valides, ainsi que les recommandations et restrictions relatives à leur utilisation.

Recommandations et restrictions sur le SGBD

SGBD	Recommandations et restrictions
SQL Server Express Edition 2016 et suivante	Utilisez ce SGBD si vous prévoyez d'utiliser un seul Serveur d'administration pour moins de 10 000 appareils. Il est recommandé de désactiver la tâche Inventaire des logiciels et de désactiver (dans les paramètres de stratégie Kaspersky Endpoint Security) les notifications du Serveur d'administration sur les applications lancées. Vous pouvez limiter le nombre d'événements dans le stockage d'événements pour éviter un débordement de base de données. Pour plus de détails, reportez-vous à la section suivante : Calcul de l'espace disponible dans la base de données. L'utilisation conjointe du SGBD Server Express Edition par le Serveur d'administration et une autre application est strictement interdite. La base de données Microsoft SQL Express n'est pas prise en charge pour la tâche **Synchronisation des mises à jour Windows Update**.
SQL Server Edition local, différent d'Express. 2016 et suivante	Pas de restrictions.
SQL Server Edition distant, différent d'Express, 2016 et suivante	Valide uniquement si les deux appareils se trouvent dans le même domaine Windows® ; si les domaines diffèrent, il faut établir une relation de confiance bilatérale entre eux.
MySQL 5.5, 5.6 ou 5.7 local ou distant (les versions MySQL 5.5.1, 5.5.2, 5.5.3, 5.5.4 et 5.5.5 ne sont plus prises en charge)	Utilisez ce SGBD si vous prévoyez d'utiliser un seul Serveur d'administration pour moins de 10 000 appareils. Il est recommandé de désactiver la tâche Inventaire des logiciels et de désactiver (dans les paramètres de stratégie Kaspersky Endpoint Security) les notifications du Serveur d'administration sur les applications lancées. Pour plus de détails, reportez-vous à la section suivante : Calcul de l'espace disponible dans la base de données.
MySQL local ou distant 8.0.20 ou version ultérieure	Utilisez ce SGBD si vous prévoyez d'utiliser un seul Serveur d'administration pour moins de 50 000 appareils. Il est recommandé de désactiver la tâche Inventaire des logiciels et de désactiver (dans les paramètres de stratégie Kaspersky Endpoint Security) les notifications du Serveur d'administration sur les applications lancées. Pour plus de détails, reportez-vous à la section suivante : Calcul de l'espace disponible dans la base de données.

SGBD	Recommandations et restrictions
MariaDB locale ou distante (voir les versions prises en charge)	Utilisez ce SGBD si vous prévoyez d'utiliser un seul Serveur d'administration pour moins de 20 000 appareils. Il est recommandé de désactiver la tâche Inventaire des logiciels et de désactiver (dans les paramètres de stratégie Kaspersky Endpoint Security) les notifications du Serveur d'administration sur les applications lancées. Pour plus de détails, reportez-vous à la section suivante : Calcul de l'espace disponible dans la base de données.
PostgreSQL, Postgres Pro (cf. les versions compatibles)	Utilisez l'un de ces SGBD si vous prévoyez d'utiliser un seul Serveur d'administration pour moins de 50 000 appareils. Il est recommandé de désactiver la tâche Inventaire des logiciels et de désactiver (dans les paramètres de stratégie Kaspersky Endpoint Security) les notifications du Serveur d'administration sur les applications lancées. Pour plus de détails, reportez-vous à la section suivante : Calcul de l'espace disponible dans la base de données.

Si vous utilisez SQL Server 2019 en tant que SGBD et vous n'avez pas de correctif cumulatif CU12 ou ultérieur, vous devez effectuer les opérations suivantes après d'installer Kaspersky Security Center :

1. Connectez-vous à SQL Server à l'aide de SQL Management Studio.
2. Exécutez les commandes suivantes (si vous avez choisi un nom différent pour la base de données, utilisez ce nom au lieu de KAV) :

   ```
   USE KAV
   GO
   ALTER DATABASE SCOPED CONFIGURATION SET TSQL_SCALAR_UDF_INLINING = OFF
   GO
   ```

3. Redémarrez le service SQL Server 2019.

Sinon, l'utilisation de SQL Server 2019 peut entraîner des erreurs, telles que « la mémoire système est insuffisante dans le pool de ressources 'interne' pour exécuter cette requête ».

Configuration du serveur MariaDB x64 pour fonctionner avec Kaspersky Security Center 15.1

Pour configurer correctement le serveur MariaDB x64 afin qu'il fonctionne avec Kaspersky Security Center, vous devez utiliser les paramètres par défaut du serveur, à l'exception des paramètres indiqués dans cet article.

Kaspersky Security Center 15.1 prend en charge les SGBD MariaDB. Pour plus d'informations sur les versions prises en charge de MariaDB, consultez la section Configuration matérielle et logicielle requise.

Si vous utilisez le SGBD MariaDB pour Kaspersky Security Center, activez la prise en charge du stockage InnoDB et MEMORY, ainsi que des encodages UTF-8 et UCS-2.

Paramètres recommandés pour le fichier my.ini

Pour configurer le fichier my.ini :

1. Ouvrez le fichier my.ini avec un éditeur de texte.

2. Ajoutez les lignes suivantes dans la section `[mysqld]` du fichier my.ini :

```
sort_buffer_size=10M
join_buffer_size=100M
join_buffer_space_limit=300M
join_cache_level=8
tmp_table_size=512M
max_heap_table_size=512M
key_buffer_size=200M
innodb_buffer_pool_size=< la valeur réelle ne doit pas être inférieure à 80 % de la
taille prévue de la base de données KAV >
innodb_thread_concurrency=20
innodb_flush_log_at_trx_commit=0
innodb_lock_wait_timeout=300
max_allowed_packet=32M
max_connections=151
max_prepared_stmt_count=12800
table_open_cache=60000
table_open_cache_instances=4
table_definition_cache=60000
sql_mode="STRICT_TRANS_TABLES,NO_AUTO_CREATE_USER,NO_ENGINE_SUBSTITUTION"
```

La valeur de `innodb_buffer_pool_size` ne doit pas être inférieure à 80 % de la taille de base de données KAV attendue. Notez que la mémoire indiquée est allouée au démarrage du serveur. Si la taille de la base de données est inférieure à la taille de la mémoire tampon indiquée, seule la mémoire requise est allouée. Si vous utilisez MariaDB 10.4.3 ou une version antérieure, la taille réelle de la mémoire allouée est supérieure d'environ 10 % à la taille de la mémoire tampon indiquée.

Il est recommandé d'utiliser la valeur de paramètre `innodb_flush_log_at_trx_commit=0`, car les valeurs "1" ou "2" affectent négativement la vitesse de fonctionnement de MariaDB. Assurez-vous que le paramètre `innodb_file_per_table` présente la valeur `1`.

Pour MariaDB 10.1, saisissez également les lignes suivantes dans la section [mysqld] :

```
innodb_file_format='Barracuda'
innodb_default_row_format=dynamic
innodb_large_prefix=1
```

Pour MariaDB 10.6, saisissez également les lignes suivantes dans la section [mysqld] :

```
optimizer_prune_level=0
optimizer_search_depth=8
```

Par défaut, les modules complémentaires d'optimisation [[join_cache_incremental]], [[join_cache_hashed]] et [[join_cache_bka]] sont activés. Si ces modules complémentaires ne sont pas activés, vous devez les activer.

Pour vérifier si les modules complémentaires d'optimisation sont activés :

1. Dans la console client MariaDB, exécutez la commande :

   ```
   SELECT @@optimizer_switch;
   ```

2. Vérifiez que sa sortie contient les lignes suivantes :

   ```
   join_cache_incremental=on
   join_cache_hashed=on
   join_cache_bka=on
   ```

   Si ces lignes sont présentes et ont la valeur `on`, alors les modules complémentaires d'optimisation sont activés.

   Si ces lignes manquent ou ont la valeur `off`, effectuez les opérations suivantes :

   1. Ouvrez le fichier my.ini avec un éditeur de texte.

   2. Ajoutez les lignes suivantes dans la section `[mysqld]` du fichier my.ini :

      ```
      optimizer_switch='join_cache_incremental=on'
      optimizer_switch='join_cache_hashed=on'
      optimizer_switch='join_cache_bka=on'
      ```

Les modules complémentaires `join_cache_incremental`, `join_cache_hash` et `join_cache_bka` sont activés.

Configuration du serveur MySQL x64 pour fonctionner avec Kaspersky Security Center 15.1

Pour configurer correctement le serveur MySQL x64 afin qu'il fonctionne avec Kaspersky Security Center, vous devez utiliser les paramètres par défaut du serveur, à l'exception des paramètres indiqués dans cet article.

Si vous utilisez le SGBD MySQL pour Kaspersky Security Center, activez la prise en charge du stockage InnoDB et MEMORY, ainsi que des encodages UTF-8 et UCS-2.

Paramètres recommandés pour le fichier my.ini

Pour configurer le fichier my.ini :

1. Ouvrez le fichier my.ini avec un éditeur de texte.

2. Ajoutez les lignes suivantes dans la section `[mysqld]` du fichier my.ini :

```
sort_buffer_size=10M
join_buffer_size=20M
tmp_table_size=600M
max_heap_table_size=600M
key_buffer_size=200M
innodb_buffer_pool_size=< la valeur réelle ne doit pas être inférieure à 80 % de la taille prévue de la base de données KAV >
innodb_thread_concurrency=20
innodb_flush_log_at_trx_commit=0 (dans la plupart des cas, le serveur utilise de petites transactions)
innodb_lock_wait_timeout=300
max_allowed_packet=32M
max_connections=151
max_prepared_stmt_count=12800
table_open_cache=60000
table_open_cache_instances=4
table_definition_cache=60000
```

Notez que la mémoire indiquée dans la valeur `innodb_buffer_pool_size` est allouée au démarrage du serveur. Si la taille de la base de données est inférieure à la taille de la mémoire tampon indiquée, seule la mémoire requise est allouée. La taille réelle de la mémoire allouée est supérieure d'environ 10 % à la taille de la mémoire tampon indiquée. Pour plus d'informations, voir la documentation MySQL.

Il est recommandé d'utiliser la valeur de paramètre `innodb_flush_log_at_trx_commit = 0`, car les valeurs "1" ou "2" affectent négativement la vitesse de fonctionnement de MySQL. Assurez-vous que le paramètre `innodb_file_per_table` présente la valeur `1`.

Configuration du serveur PostgreSQL ou Postgres Pro pour fonctionner avec Kaspersky Security Center 15.1

Pour configurer correctement le serveur PostgreSQL ou Postgres Pro afin qu'il fonctionne avec Kaspersky Security Center, vous devez utiliser les paramètres par défaut du serveur, à l'exception des paramètres indiqués dans cet article.

Kaspersky Security Center 15.1 est compatible avec les SGBD PostgreSQL et Postgres Pro. Si vous utilisez l'un de ces SGBD, pensez à configurer les paramètres du serveur de SGBD pour optimiser le fonctionnement du SGBD avec Kaspersky Security Center.

Le chemin d'accès par défaut au fichier de configuration est : `C:\Program Files\PostgreSQL\<VERSION>\data\postgresql.conf`

Paramètres recommandés pour PostgreSQL et Postgres Pro :

- `shared_buffers` = 25 % de la valeur de la mémoire vive de l'appareil sur lequel les SGBD sont installés

  Si la RAM est inférieure à 1 Go, laissez la valeur par défaut.

- `max_stack_depth = 2MB`

- `temp_buffers = 24MB`
- `work_mem = 16MB`
- `max_connections = 151`
- `max_parallel_workers_per_gather = 0`
- `maintenance_work_mem = 128MB`

Assurez-vous que le paramètre `standard_conforming_strings` présente la valeur par défaut `on`. Actualisez la configuration ou redémarrez le serveur après la mise à jour du fichier postgresql.conf. Pour plus d'informations, voir la documentation PostgreSQL.

Si vous utilisez Postgres Pro 15.7 ou Postgres Pro 15.7.1, désactivez le paramètre `enable_compound_index_stats` :

```
enable_compound_index_stats = off
```

Pour obtenir des informations détaillées sur les paramètres des serveurs PostgreSQL et Postgres Pro et sur la façon de spécifier ces paramètres, reportez-vous à la documentation du SGBD correspondant.

Reportez-vous à la rubrique suivante pour en savoir plus sur la création et la configuration des comptes utilisateur pour PostgreSQL et Postgres Pro : Configuration des comptes utilisateur pour une utilisation avec PostgreSQL et Postgres Pro.

Administration des appareils mobiles dotés de Kaspersky Endpoint Security for Android

L'administration des appareils mobiles dotés de Kaspersky Endpoint Security for Android™ (ci-après les appareils KES) s'opère via le Serveur d'administration. Kaspersky Security Center est compatible avec les fonctions suivantes d'administration des appareils KES :

- utilisation des appareils mobiles comme des appareil clients :
  - appartenance aux groupes d'administration
  - Surveillance, par exemple concernant l'affichage des statuts, des événements et des rapports
  - modification des paramètres locaux et désignation de stratégies pour l'application Kaspersky Endpoint Security for Android
- envoi centralisé de commandes
- installation à distance de paquets des applications mobiles.

Le Serveur d'administration gère les appareils KES via TLS, port TCP 13292.

Octroi de l'accès au Serveur d'administration via Internet

Dans certains cas, il faut octroyer un accès au Serveur d'administration depuis Internet :

- Mise à jour régulière des bases de données, des modules logiciels et des applications Kaspersky
- mise à jour du logiciel tiers

  Par défaut, une connexion Internet n'est pas requise pour que le Serveur d'administration installe les mises à jour logicielles Microsoft sur les appareils administrés. Les appareils administrés peuvent ainsi télécharger les mises à jour logicielles Microsoft directement à partir des serveurs Microsoft Update ou à partir de Windows Server lorsque Microsoft Windows Server Update Services (WSUS) est déployé sur le réseau de votre organisation. Le Serveur d'administration doit être connecté à Internet dans les cas suivants :

  - Lorsque vous utilisez le Serveur d'administration comme serveur WSUS
  - Pour installer des mises à jour de logiciels tiers autres que les logiciels Microsoft
- Correction des vulnérabilités dans les applications tierces

  Une connexion Internet est requise pour que le Serveur d'administration puisse effectuer les tâches suivantes :

  - Pour dresser une liste des correctifs recommandés pour les vulnérabilités des logiciels Microsoft. La liste est créée et régulièrement mise à jour par des spécialistes de Kaspersky.
  - Pour corriger les vulnérabilités de logiciels tiers autres que les logiciels Microsoft.
- Pour l'administration des appareils (ordinateurs portables) des utilisateurs itinérants
- Pour l'administration des appareils dans les bureaux distants
- Coopération entre les Serveurs d'administration secondaire et principal dans des bureaux distants
- Pour administrer les appareils mobiles.

Cette section aborde les moyens typiques d'octroi de l'accès au Serveur d'administration depuis Internet. Dans tous les cas d'octroi de l'accès au Serveur d'administration depuis Internet, il peut être nécessaire d'attribuer un certificat spécial au Serveur d'administration.

Accès depuis Internet : Serveur d'administration dans le réseau local

Si le Serveur d'administration se trouve dans le réseau interne de l'entreprise, envisagez de rendre accessible le port 13000 TCP du Serveur d'administration depuis l'extérieur au moyen du mécanisme de redirection des ports. Si l'administration des appareils mobiles est requise, envisagez de rendre le port 13292 TCP accessible.

Accès depuis Internet : Serveur d'administration dans la zone démilitarisée

Si le Serveur d'administration se trouve dans la zone démilitarisée du réseau de l'entreprise, il n'a pas accès au réseau interne de l'entreprise. Les restrictions suivantes se manifestent par conséquent :

- Le Serveur d'administration ne peut pas détecter seul les nouveaux appareils.
- Le Serveur d'administration ne peut pas exécuter le déploiement initial de l'Agent d'administration au moyen d'une installation forcée sur les appareils du réseau interne de l'entreprise.

Il s'agit uniquement de l'installation initiale de l'Agent d'administration. Les mises à jour suivantes de la version de l'Agent d'administration ou l'installation de l'application de sécurité peuvent être exécutées via le Serveur d'administration. Cependant le déploiement initial des Agents d'administration peut être exécuté par d'autres moyens, par exemple, à l'aide des stratégies de groupe de Microsoft® Active Directory®.

- Le Serveur d'administration ne peut pas envoyer aux appareils administrés des notifications sur le port 15000 UDP, ce qui ne constitue pas un problème pour le fonctionnement de Kaspersky Security Center.

- Le Serveur d'administration ne peut pas sonder Active Directory. Toutefois, les résultats du sondage d'Active Directory ne sont pas requis dans la majorité des cas.

Si les restrictions décrites ci-dessus sont critiques, il est possible de les lever à l'aide des points de distribution situés dans le réseau de l'entreprise :

- Pour exécuter le déploiement initial sur des appareils sans Agent d'administration, il faut préalablement installer l'Agent d'administration sur un des appareils et désigner celui-ci comme point de distribution. Après l'installation finalement initiale de l'Agent d'administration, le Serveur d'administration est installé sur les autres appareils via ce point de distribution.

- Pour détecter de nouveaux appareils sur le réseau interne de l'entreprise et pour sonder Active Directory, il faut activer les méthodes de recherche d'appareils pertinentes sur l'un des points de distribution.

Pour garantir l'envoi de notifications aux appareils administrés au sein du réseau interne de l'entreprise sur le port 15000 UDP, il faut couvrir tout le réseau de l'entreprise de points de distribution. Dans les propriétés des points de distribution qui ont été attribués, cochez la case **Maintenir la connexion au Serveur &d'administration**. Ainsi, le Serveur d'administration peut maintenir la communication avec les points de distribution tandis qu'ils peuvent envoyer des notifications au port 15000 UDP aux appareils situés dans le réseau interne de l'entreprise (il peut s'agir d'un réseau IPv4 ou IPv6).

Accès depuis Internet : Agent d'administration en tant que passerelle de connexion dans la zone démilitarisée

Le Serveur d'administration peut se trouver sur le réseau interne de l'entreprise tandis que dans la zone démilitarisée du réseau, on retrouve l'appareil doté de l'Agent d'administration qui fonctionne en tant que passerelle de connexion avec connexion inverse (le Serveur d'administration établit la connexion avec l'Agent d'administration). Dans ce cas, pour organiser l'accès depuis Internet, il faut remplir les conditions suivantes :

- Il faut installer l'Agent d'administration sur l'appareil qui se trouve dans la zone démilitarisée. Lors de l'installation de l'Agent d'administration, dans la fenêtre de l'Assistant d'installation **Passerelle de connexion**, sélectionnez **Utiliser l'Agent d'administration en tant que passerelle de connexion en DMZ**.

- L'appareil avec la passerelle de connexion installée doit être ajouté en tant que point de distribution. Lorsque vous ajoutez la passerelle de connexion, dans la fenêtre **Ajouter un point de distribution**, sélectionnez l'option **Sélectionner → Ajouter la passerelle de connexion, située en DMZ, en fonction de l'adresse**.

- Pour utiliser une connexion Internet pour connecter des appareils de bureau externes au Serveur d'administration, le paquet d'installation de l'Agent d'administration doit être corrigé. Dans les propriétés du paquet d'installation créé, sélectionnez l'option **Avancé →Se connecter au Serveur d'administration au moyen d'une passerelle de connexion**, puis indiquez la passerelle de connexion nouvellement créée.

Si la passerelle de connexion se trouve dans la zone démilitarisée, le Serveur d'administration crée un certificat signé par le certificat du Serveur d'administration. Si l'administrateur a décidé d'attribuer un certificat personnalisé au Serveur d'administration, il faut réaliser l'opération avant la création de la passerelle des connexions dans la zone démilitarisée.

S'il existe des employés avec des ordinateurs portables qui peuvent se connecter au Serveur d'administration depuis le réseau local ou depuis Internet, il convient peut-être de créer une règle de permutation de l'Agent d'administration dans la stratégie de l'Agent d'administration.

À propos des points de distribution

Un appareil avec l'Agent d'administration installé peut servir de point de distribution. Dans ce mode, l'Agent d'administration peut exercer les fonctions suivantes :

- Diffuser les mises à jour ces mises à jour peuvent être obtenues à partir du Serveur d'administration comme à partir des serveurs de mise à jour de Kaspersky. Dans ce cas, il faut créer la tâche *Télécharger les mises à jour sur les stockages des points de distribution* pour l'appareil qui fait office de point de distribution :
    - Installer le logiciel sur d'autres appareils, y compris exécuter le déploiement initial des Agents d'administration sur les appareils.
    - Sonder le réseau dans le but de détecter de nouveaux appareils et de mettre à jour les informations sur les appareils détectés. Un point de distribution peut exécuter les mêmes méthodes de recherche d'appareils que le Serveur d'administration.

Le déploiement de points de distribution sur le réseau de l'entreprise poursuit les buts suivants :

- Réduire la charge sur le Serveur d'administration.
- Optimiser le trafic.
- Accorder au Serveur d'administration un accès aux appareils dans les parties du réseau de l'entreprise difficilement accessibles. La présence d'un point de distribution qui se trouve au-delà du NAT (par rapport au Serveur d'administration) du réseau permet au Serveur d'administration d'exécuter les actions suivantes :
    - Envoyer des notifications aux appareils via UDP sur le réseau IPv4 ou IPv6
    - Sonder le réseau IPv4 ou IPv6
    - Exécuter le déploiement initial
    - Fonctionnement en tant que serveur push

Un point de distribution est assigné au groupe d'administration. Dans ce cas, la zone d'action du point de distribution reprend les appareils situés dans ce groupe d'administration et l'ensemble de ses sous-groupes. L'appareil qui fait office de point de distribution ne doit pas se trouver obligatoirement dans le groupe d'administration auquel il est attribué.

Vous pouvez faire fonctionner un point de distribution comme une passerelle de connexion. Dans ce cas, les appareils qui se trouvent dans la zone d'action de ce point de distribution se connectent au Serveur d'administration non pas directement, mais via la passerelle. Ce mode est utile dans les cas où il est impossible d'établir une connexion directe entre le Serveur d'administration et les appareils administrés.

Si vous utilisez un appareil basé sur Linux en tant que point de distribution, nous vous recommandons fortement d'augmenter la limite de descripteurs de fichiers pour le service klnagent, car si la portée du point de distribution inclut de nombreux appareils, le nombre maximal par défaut de fichiers pouvant être ouverts peut s'avérer insuffisant.

Augmentation du nombre de descripteurs de fichiers pour le service klnagent

Si la zone d'action d'un point de distribution Linux inclut de nombreux appareils, la limite par défaut de fichiers pouvant être ouverts (descripteurs de fichier) peut ne pas être suffisante. Pour éviter cela, vous pouvez augmenter le nombre de descripteurs de fichiers pour le service klnagent.

Pour augmenter le nombre de descripteurs de fichiers pour le service klnagent, procédez comme suit :

1. Sur l'appareil Linux qui joue le rôle de point de distribution, ouvrez le fichier `/lib/systemd/system/klnagent64.service` puis indiquez les limites matérielles et logicielles des descripteurs de fichier dans le paramètre `LimitNOFILE` de la section `[Service]` :

   `LimitNOFILE=<limite de ressource souple>:<limite de ressources rigide>`

   Par exemple, `LimitNOFILE=32768:131072`. Notez que la limite logicielle des descripteurs de fichier doit être inférieure ou égale à la limite stricte.

2. Exécutez la commande suivante pour vous assurer que les paramètres sont indiqués correctement :

   `systemd-analyze verify klnagent64.service`

   En cas d'erreur de définition des paramètres, cette commande peut produire une des erreurs suivantes :

   - `/lib/systemd/system/klnagent64.service:11: Failed to parse resource value, ignoring: 32768:13107`

     Si cette erreur se produit, les symboles dans la ligne `LimitNOFILE` ont été indiqués incorrectement. Vous devez vérifier et corriger la ligne saisie.

   - `/lib/systemd/system/klnagent64.service:11: Soft resource limit chosen higher than hard limit, ignoring: 32768:13107`

     Si cette erreur se produit, la limite souple des descripteurs de fichier que vous avez entrés est supérieure à la limite stricte. Vous devez vérifier la ligne saisie et vous assurer que la limite logicielle des descripteurs de fichier est inférieure ou égale à la limite stricte.

3. Exécutez la commande suivante pour recharger le processus systemd :

   `systemctl daemon-reload`

4. Exécutez la commande suivante pour redémarrer le service de l'Agent d'administration :

   `systemctl restart klnagent`

5. Exécutez la commande suivante pour vous assurer que les paramètres indiqués sont appliqués correctement :

   `less /proc/<nagent process id>/limits`

   où le paramètre `<nagent process id>` est l'identifiant du processus de l'Agent d'administration. Vous pouvez exécuter la commande suivante pour obtenir l'identifiant :

   `ps -ax | grep klnagent`

Pour le point de distribution Linux, la limite d'ouvertures de fichiers est augmentée.

Calcul de la quantité et de la configuration des points de distribution

Plus un réseau compte d'appareils clients, plus le nombre de points de distribution requis augmente. Il est recommandé de ne pas désactiver la définition automatique des points de distribution. Lorsque la définition automatique des points de distribution est activée, le Serveur d'administration désigne les points de distribution si le nombre des appareils clients est assez élevé, et définit leur configuration.

Utilisation de points de distribution assignés exclusivement

Si vous envisagez d'utiliser des ensembles d'appareils (à savoir, des serveurs affectés de manière exclusive) en tant que points de distribution, vous pouvez ne pas utiliser la définition automatique des points de distribution. Dans ce cas, assurez-vous que les appareils dont vous souhaitez faire des points de distribution disposent de suffisamment d'espace libre sur le disque, qu'ils ne sont pas régulièrement éteints et que le " mode veille " est désactivé.

Nombre de points de distribution exclusivement attribués sur un réseau qui contient un segment unique, sur la base du nombre d'appareils en réseau

Nombre d'appareils clients administrés dans le segment du réseau	Nombre des points de distribution
Moins de 300	0 (ne pas assigner de points de distribution)
Plus de 300	Acceptable : (N/10 000 + 1), recommandé : (N/5 000 + 2), où N représente le nombre d'appareils sur le réseau

Nombre de points de distribution exclusivement attribués sur un réseau qui contient plusieurs segments, sur la base du nombre d'appareils en réseau

Nombre d'appareils clients par segment de réseau	Nombre des points de distribution
Moins de 10	0 (ne pas assigner de points de distribution)
10–100	1
Plus de 100	Acceptable : (N/10 000 + 1), recommandé : (N/5 000 + 2), où N représente le nombre d'appareils sur le réseau

Utilisation d'appareils clients standard (postes de travail) en tant que points de distribution

Si vous avez l'intention d'utiliser des appareils clients standard (à savoir, des postes de travail) en tant que points de distribution, nous vous conseillons de les désigner comme dans les tableaux ci-dessous afin d'éviter une charge excessive des canaux de communication et du Serveur d'administration :

Nombre de postes de travail servant de points de distribution sur un réseau qui contient un segment unique, sur la base du nombre d'appareils en réseau

Nombre d'appareils clients administrés dans le segment du réseau	Nombre des points de distribution
Moins de 300	0 (ne pas assigner de points de distribution)
Plus de 300	(N/300 +1), où N est le nombre des appareils sur le réseau ; il doit y avoir au moins 3 points de distribution

Nombre de postes de travail servant de points de distribution sur un réseau qui contient plusieurs segments, sur la base du nombre d'appareils en réseau

Nombre d'appareils clients par segment de réseau	Nombre des points de distribution
Moins de 10	0 (ne pas assigner de points de distribution)
10–30	1

Nombre d'appareils clients par segment de réseau	Nombre des points de distribution
31–300	2
Plus de 300	(N/300 +1), où N est le nombre des appareils sur le réseau ; il doit y avoir au moins 3 points de distribution

Si un point de distribution est éteint (ou indisponible pour toute autre raison), les appareils administrés situés dans sa zone d'action peuvent accéder au Serveur d'administration pour les mises à jour.

Hiérarchie des Serveurs d'administration

Il peut y avoir plus d'un Serveur d'administration par MSP. L'administration de plusieurs serveurs hétérogènes n'est pas pratique et pour cette raison, il est utile de les regrouper dans une hiérarchie. La configuration " primaire/secondaire " entre deux Serveurs d'administration offre les possibilités suivantes :

- Le Serveur d'administration secondaire hérite des stratégies et des tâches du Serveur d'administration principal, les paramètres en double sont supprimés.
- Les sélections d'appareils sur le Serveur d'administration principal peuvent reprendre des appareils de Serveurs d'administration secondaires.
- Les rapports relatifs au Serveur d'administration principal peuvent comprendre des données (y compris des données détaillées) des Serveurs d'administration secondaires.

Le Serveur d'administration principal reçoit uniquement les données des Serveurs d'administration secondaires non virtuels qui respectent les options répertoriées ci-dessus. Cette restriction ne s'applique pas aux Serveurs d'administration virtuels qui partagent la base de données avec leur Serveur d'administration principal.

Serveurs d'administration virtuels

Il est possible de créer dans un Serveur d'administration physique plusieurs Serveurs d'administration virtuels dans une multitude de Serveurs secondaires semblables. Par rapport au modèle de partage de l'accès qui repose sur des listes de contrôle de l'accès (ACL), le modèle des Serveurs d'administration virtuels est plus pratique et permet une isolation plus poussée. Outre la structure propre des groupes d'administration pour les appareils administrés avec les stratégies et les tâches, chaque Serveur d'administration virtuel possède également son propre groupe d'appareils non définis, ses propres sélections de rapports, ses sélections d'appareils et d'événements, ses paquets d'installation, ses règles de déplacement des appareils, etc. La fonction des Serveurs d'administration virtuels peut être utilisée par les fournisseurs de services (xSP) afin d'isoler le plus possible différents commanditaires ou par de grandes sociétés dotées d'une structure complexe et d'un nombre élevé d'administrateurs.

Les Serveurs d'administration virtuels ressemblent en de nombreux points aux Serveurs d'administration secondaires, mais ils possèdent les différences suivantes :

- Le Serveur d'administration virtuel ne possède pas la plupart des paramètres globaux, ni ses propres ports TCP.
- Le Serveur d'administration virtuel ne peut pas avoir de serveurs secondaires.
- Le Serveur d'administration virtuel ne peut pas avoir ses propres serveurs virtuels.

- le Serveur d'administration physique présente les appareils, les groupes, les événements et les objets des appareils administrés (éléments de la quarantaine, registre des applications, etc.) de l'ensemble de ses Serveurs virtuels.
- Le Serveur d'administration virtuel peut analyser le réseau uniquement à l'aide des points de distribution qui y sont connectés.

Informations sur les restrictions de Kaspersky Security Center

Le tableau ci-après reprend les restrictions de la version actuelle de Kaspersky Security Center.

Restrictions de Kaspersky Security Center

Type de restriction	Valeur
Nombre maximal d'appareils administrés par un Serveur d'administration	100 000
Nombre maximum d'appareils pour lesquels l'option **Maintenir la connexion au Serveur d'administration** est sélectionnée	300
Nombre maximum des groupes d'administration	10 000
Nombre maximum d'événements enregistrés	45 000 000
Nombre maximum de stratégies	2000
Nombre maximum de tâches	2000
Nombre total maximum d'objets Active Directory (unités organisationnelles (OUs) et comptes utilisateurs, appareils et groupes de sécurité)	1 000 000
Nombre maximum de profils dans une stratégie	100
Nombre maximum de Serveurs d'administration secondaires pour un Serveur d'administration principal	500
Nombre maximum de Serveurs d'administration virtuels	500
Nombre maximum d'appareils qu'un point de distribution peut couvrir (les points de distribution ne peuvent couvrir que des appareils non mobiles)	10 000
Nombre maximum d'appareils qui peuvent utiliser une passerelle de connexion unique	10 000, y compris des appareils mobiles
Nombre maximal d'appareils mobiles sur un Serveur d'administration	100 000, moins le nombre d'appareils administrés fixes

Charge sur le réseau

Cette section fournit des informations sur le volume de trafic réseau échangé entre les appareils clients et le Serveur d'administration dans le cadre de l'exécution des scénarios d'administration clés.

La charge principale sur le réseau est liée avec l'exécution des scénarios d'administration suivants :

- Déploiement initial de la protection antivirus
- Mise à jour initiale des bases antivirus
- Synchronisation de l'appareil client avec le Serveur d'administration
- Mise à jour régulière des bases antivirus
- Traitement des événements des appareils clients par le Serveur d'administration

Déploiement initial de la protection antivirus

Cette section fournit la consommation de trafic en cas d'installation d'un Agent d'administration et de Kaspersky Endpoint Security for Windows sur un appareil client (cf. tableau ci-après).

L'Agent d'administration est installé via une installation forcée quand les fichiers indispensables à l'installation sont copiés par le Serveur d'administration dans le dossier partagé sur l'appareil client. Après l'installation, l'Agent d'administration reçoit le paquet de distribution de Kaspersky Endpoint Security for Windows, en utilisant la connexion avec le Serveur d'administration.

Débit du trafic

Scénario	Installation de l'Agent d'administration pour un appareil client	Installation de Kaspersky Endpoint Security for Windows pour un appareil client (avec des bases mises à jour)	Installation collective de l'Agent d'administration et de Kaspersky Endpoint Security for Windows
Trafic depuis l'appareil client vers le Serveur d'administration, Ko	1638,4	7843,84	9707,52
Trafic depuis le Serveur d'administration vers l'appareil client, Ko	69,990.4	259 317,76	329 318,4
Trafic général (pour un appareil client), Ko	71,628.8	267 161,6	339 025,92

Une fois les Agents d'administration installés sur les appareils du client, l'un des appareils du groupe d'administration peut être assigné pour agir comme point de distribution. Il sera utilisé pour la propagation des paquets d'installation. En ce cas, le volume du trafic transmis lors du déploiement initial de la protection antivirus diffère essentiellement en fonction de l'utilisation de la diffusion IP multiadresse.

En cas d'utilisation de la multidiffusion, les paquets d'installation sont envoyés simultanément à tous les appareils repris dans le groupe d'administration. Ainsi, le trafic général est divisé par N, où N représente le nombre d'appareils repris dans le groupe d'administration. Si la diffusion IP multiadresse n'est pas utilisée, le trafic général coïncide avec le fait d'obtention des paquets de distribution du Serveur d'administration, et ce n'est pas le Serveur d'administration qui est la source des paquets d'installation, mais c'est l'agent de mises à jour. Cependant, c'est la source du paquet qui est le point de distribution, non pas le Serveur d'administration.

Mise à jour initiale des bases antivirus

Les taux de trafic lors de la mise à jour initiale des bases antivirus (lors du premier démarrage de la tâche de mise à jour de la base sur un poste client) sont les suivants :

- Trafic depuis l'appareil client vers le Serveur d'administration : 1.8 Mo.
- Trafic depuis le Serveur d'administration vers l'appareil client : 113 Mo.
- Trafic général (pour un appareil client) : 114 Mo.

Les données peuvent différer un peu en fonction de la version actuelle des bases antivirus.

Synchronisation du client avec le Serveur d'administration

Ce scénario détermine l'état du système d'administration lors de la synchronisation active des données entre l'appareil client et le Serveur d'administration. Les appareils clients se connectent au Serveur d'administration selon une période définie par l'administrateur. Le Serveur d'administration compare l'état des données sur l'appareil client à celui des données sur le Serveur, enregistre les données relatives à la dernière connexion de l'appareil client dans la base de données et synchronise les données.

Cette section reprend les informations sur le débit du trafic pour les scénarios d'administration généraux lors de la connexion du poste client au Serveur d'administration avec synchronisation (cf. tableau ci-après). Les données, présentées dans le tableau, peuvent différer un peu en fonction de la version actuelle des bases antivirus.

Scénario	Trafic depuis les appareils clients vers le Serveur d'administration, Ko	Trafic depuis le Serveur d'administration vers les appareils clients, Ko	Trafic général (pour un appareil client), Ko
Synchronisation initiale avant la mise à jour des bases de données sur l'appareil client	699,44	568,42	1267,86
Synchronisation initiale après la mise à jour des bases de données sur l'appareil client	735,8	4474,88	5210,68
Synchronisation en l'absence de modifications sur l'appareil client et le Serveur d'administration	11,99	6,73	18,72
Synchronisation lors de la modification d'un paramètre dans la stratégie du groupe	9,79	11,39	21,18
Synchronisation lors de la modification d'un paramètre dans la tâche de groupe	11,27	11,72	22,99
Synchronisation forcée en l'absence de modifications sur l'appareil client	77,59	99,45	177,04

Le volume du trafic général varie essentiellement en fonction de l'utilisation de la diffusion IP multi-adresses au sein des groupes d'administration. En cas d'utilisation de la multidiffusion, le trafic pour le groupe est divisé environ par N, où N représente le nombre d'appareils repris dans le groupe d'administration.

Lors de la synchronisation initiale précédant et suivant la mise à jour des bases de données, le volume du trafic est indiqué dans les cas suivants :

- Installation sur l'appareil client d'un Agent d'administration et d'une application de sécurité
- Transfert d'un appareil client dans un groupe d'administration
- Application à l'appareil client des stratégies et des tâches crées pour le groupe par défaut

Le tableau indique le volume du trafic lors de la modification de l'un des paramètres de protection inclus dans les paramètres de la stratégie de Kaspersky Endpoint Security. Les données pour d'autres paramètres de la stratégie peuvent être différents des données présentées dans le tableau.

Mise à jour complémentaire des bases antivirus

Le débit du trafic lors de la mise à jour d'incrémentation des bases antivirus dans 20 heures après la mise à jour précédente sont les suivants :

- Trafic depuis l'appareil client vers le Serveur d'administration : 169 Ko.
- Trafic depuis le Serveur d'administration vers l'appareil client : 16 Mo.
- Trafic général (pour un appareil client) : 16.3 Mo.

Les données, présentées dans le tableau, peuvent différer un peu en fonction de la version actuelle des bases antivirus.

Le volume du trafic varie essentiellement en fonction de l'utilisation de la diffusion IP multiadresse à l'intérieur des groupes d'administration. En cas d'utilisation de la multidiffusion, le trafic pour le groupe est divisé environ par N, où N représente le nombre d'appareils repris dans le groupe d'administration.

Traitement des événements des clients par le Serveur d'administration

Cette section indique le débit du trafic lorsque l'événement " Virus détecté " survient sur l'appareil client et dont les informations sont transmises au Serveur d'administration et consignées dans la base de données (cf. tableau ci-après).

Scénario	Transfert des données vers le Serveur d'administration quand un événement " Virus découvert " survient	Transfert des données vers le Serveur d'administration quand neufs événements " Virus découvert " surviennent
Trafic depuis l'appareil client vers le Serveur d'administration, Ko	49,66	64,05
Trafic depuis le Serveur d'administration vers l'appareil client, Ko	28,64	31,97
Trafic général (pour un appareil client), Ko	78,3	96,02

Les données présentées dans le tableau peuvent différer légèrement en fonction de la version de l'application antivirus et en fonction des événements spécifiés dans la stratégie comme nécessitant un enregistrement dans la base de données du Serveur d'administration.

Débit du trafic pendant 24 heures

Cette section fournit des informations sur le débit de trafic pendant 24 heures de fonctionnement du système d'administration en mode "veille" quand aucune donnée n'est modifiée ni du côté des appareils clients, ni du côté du Serveur d'administration (cf. tableau ci-dessous).

Les données, affichées dans le tableau, caractérisent l'état du réseau après l'installation standard de Kaspersky Security Center et après la fin du fonctionnement de l'Assistant de configuration initiale de l'application. La période de synchronisation de l'appareil client avec le Serveur d'administration était de 20 minutes, le téléchargement des mises à jour dans le stockage du Serveur d'administration a eu lieu toutes les heures.

Taux de trafic toutes les 24 heures en mode inactif

Flux de trafic	Valeur
Trafic depuis l'appareil client vers le Serveur d'administration, Ko	3235,84
Trafic depuis le Serveur d'administration vers l'appareil client, Ko	64,378.88
Trafic général (pour un appareil client), Ko	67,614.72

Préparation de l'administration des appareils mobiles

Cette section contient des informations sur :

- Le serveur MDM iOS pour l'administration des appareils iOS par l'installation sur ceux-ci de profils MDM iOS spéciaux.
- L'administration des appareils mobiles dotés de l'application Kaspersky Endpoint Security for Android.

Serveur MDM iOS

Le serveur MDM iOS permet d'administrer les appareils iOS en installant sur ceux-ci des profils MDM iOS spéciaux. Les fonctions suivantes sont prises en charge :

- Verrouillage d'appareil
- Récupération du mot de passe
- Suppression des données de l'appareil

- Installation ou suppression des applications
- Utilisation du profil MDM iOS avec les paramètres avancés (tels que les paramètres VPN, le courrier, Wi-Fi, la caméra, les certificats, etc.)

Le serveur MDM iOS est un serveur Web qui reçoit les connexions entrantes des appareils mobiles sur son port TLS (le port 443 par défaut) et qui est administré par Kaspersky Security Center à l'aide de l'Agent d'administration. L'Agent d'administration s'installe localement sur l'appareil doté d'un serveur MDM iOS déployé.

Lors du déploiement du Serveur MDM iOS, l'administrateur doit absolument exécuter les actions suivantes :

- Octroyer à l'Agent d'administration un accès au Serveur d'administration
- Garantir aux appareils mobiles un accès au port TCP du serveur MDM iOS

Cette section présente deux configurations typiques d'un serveur MDM iOS.

Configuration typique : Kaspersky Device Management for iOS en zone démilitarisée

Le serveur MDM iOS est installé dans la zone démilitarisée du réseau de l'entreprise avec accès Internet. La particularité de cette approche est l'absence de problèmes d'accès du service Internet MDM iOS depuis Internet pour les appareils.

Puisque l'administration du Serveur MDM iOS requiert un Agent d'administration local, il faut garantir l'interaction de cet Agent d'administration avec le Serveur d'administration. Plusieurs moyens s'offrent à vous :

- Placer le Serveur d'administration dans la zone démilitarisée.
- Utiliser la passerelle des connexions :

  a. Sur l'appareil doté d'un serveur MDM iOS, connecter l'Agent d'administration au Serveur d'administration via la passerelle de connexion.

  b. Sur l'appareil doté d'un serveur MDM iOS, désigner un Agent d'administration comme passerelle de connexions.

Configuration typique : serveur MDM iOS sur le réseau local de l'entreprise

Le serveur MDM iOS se trouve sur le réseau interne de l'entreprise. Le port 443 (port par défaut) doit être activé pour l'accès externe, par exemple, en publiant le service Web MDM iOS sur le proxy inversé qui prend en charge la délégation contrainte Kerberos.

Quel que soit le type de configuration typique, il faut garantir l'accès pour le Serveur MDM iOS aux services Internet d'Apple (plage d'adresses 17.0.0.0/8) via le port TCP 2197. Ce port est utilisé pour signaler les nouvelles commandes aux appareils via le service spécial APNs.

Administration des appareils mobiles dotés de Kaspersky Endpoint Security for Android

L'administration des appareils mobiles dotés de Kaspersky Endpoint Security for Android™ (ci-après les appareils KES) s'opère via le Serveur d'administration. Kaspersky Security Center est compatible avec les fonctions suivantes d'administration des appareils KES :

- utilisation des appareils mobiles comme des appareil clients :
  - appartenance aux groupes d'administration
  - Surveillance, par exemple concernant l'affichage des statuts, des événements et des rapports
  - modification des paramètres locaux et désignation de stratégies pour l'application Kaspersky Endpoint Security for Android
- envoi centralisé de commandes
- installation à distance de paquets des applications mobiles.

Le Serveur d'administration gère les appareils KES via TLS, port TCP 13292.

Informations sur la productivité du Serveur d'administration

La section présente les résultats des essais de performances du Serveur d'administration pour différentes configurations matérielles ainsi que les restrictions de connexion des appareils administrés au Serveur d'administration.

Restrictions de connexion au Serveur d'administration

Le Serveur d'administration peut administrer jusqu'à 100 000 appareils sans perte de performances.

Restrictions sur les connexions au Serveur d'administration sans perte de performances :

- Un Serveur d'administration peut prendre en charge jusqu'à 500 Serveurs d'administration virtuels.
- Le Serveur d'administration principal prend en charge simultanément un maximum de 1 000 sessions.
- Les Serveurs d'administration virtuels prennent en charge simultanément un maximum de 1 000 sessions.

Résultats des essais de performances du Serveur d'administration

Les résultats des essais de performances du Serveur d'administration ont permis de définir le nombre maximum d'appareils clients avec lesquels le Serveur d'administration peut réaliser une synchronisation au cours de la période indiquée. Vous pouvez utiliser ces informations pour sélectionner les schémas optimaux de déploiement de la protection antivirus dans les réseaux informatiques.

Pour le test, des appareils avec les configurations matérielles suivantes ont été utilisées (cf. tableaux ci-après) :

Configuration matérielle du Serveur d'administration

Paramètre	Valeur
Processeur	Intel Xeon CPU E5630, fréquence de base 2,53 GHz, 2 connecteur, 8 cœurs, 16 processeurs logiques
Mémoire vive	26 Go
Disque dur	IBM ServeRAID M5014 SCSI Disk Device, 487 Go
Système d'exploitation	Microsoft Windows Server 2019 Standard, version 10.0.17763, build 17763
Réseau	QLogic BCM5709C Gigabit Ethernet (client NDIS VBD)

Configuration matérielle de l'appareil avec SQL Server

Paramètre	Valeur
Processeur	Intel Xeon CPU X5570, fréquence de base 2,93 GHz, 2 connecteurs, 8 cœurs, 16 processeurs logiques
Mémoire vive	32 Go
Disque dur	Appareil de disque SCSI Adaptec Array, 2047 Go
Système d'exploitation	Microsoft Windows Server 2019 Standard, version 10.0.17763, build 17763
Réseau	Intel 82576 Gigabit

Le Serveur d'administration avait pris en charge la création de 500 Serveurs d'administration virtuels.

La période de synchronisation était de 15 minutes tous les 10 000 appareils administrés (cf. tableau ci-après).

Résultats généralisés du test de charge du Serveur d'administration

Période de synchronisation, min.	Nombre des appareils administrés
15	10 000
30	20 000
45	30 000
60	40 000
75	50 000
90	60 000
105	70 000
120	80 000
135	90 000
150	100 000

Lors de la connexion du Serveur d'administration au serveur de la base de données MySQL et SQL Express, il est déconseillé d'utiliser l'application pour administrer plus de 5 000 appareils. Pour le système de gestion de base de données MariaDB, le nombre maximal recommandé d'appareils administrés est de 20 000.

Résultats des tests de performance du Serveur proxy KSN

Si le réseau de votre entreprise comprend un grand nombre d'appareils clients et qu'ils utilisent le Serveur d'administration comme serveur proxy KSN, le matériel du Serveur d'administration doit répondre à des exigences spécifiques pour pouvoir traiter les demandes des appareils clients. Vous pouvez utiliser les résultats des essais ci-dessous pour évaluer la charge du Serveur d'administration de votre réseau et planifier les ressources matérielles afin de garantir un fonctionnement normal du service KSN proxy.

Les tableaux ci-dessous présentent la configuration matérielle du Serveur d'administration et de SQL Server. Cette configuration a été utilisée dans le cadre de tests.

Configuration matérielle du Serveur d'administration

Paramètre	Valeur
Processeur	Intel Xeon (R) UC E5450, fréquence de base 3,00 GHz, 2 connecteurs, 8 cœurs, 16 processeurs logiques
Mémoire vive	32 Go
Système d'exploitation	Microsoft Windows Server 2016 Standard

Configuration matérielle de SQL Serveur

Paramètre	Valeur
Processeur	Intel Xeon (R) UC E5450, fréquence de base 3,00 GHz, 2 connecteurs, 8 cœurs, 16 processeurs logiques
Mémoire vive	32 Go
Système d'exploitation	Microsoft Windows Server 2019 Standard

Le tableau ci-dessous montre les résultats du test.

Résumé des résultats des tests de performance du serveur proxy KSN

Paramètre	Valeur
Nombre maximal de demandes traitées par seconde	4914
Utilisation maximale du processeur	36%

Paramètres réseau pour l'interaction avec des services externes

Kaspersky Security Center utilise les paramètres réseau suivants pour interagir avec les services externes.

Paramètres réseau	Adresse	Description
Port : 443 Protocole : HTTPS	activation-v2.kaspersky.com	Activation des applications.
Port : 443 Protocole : HTTPS	https://s00.upd.kaspersky.com https://s01.upd.kaspersky.com https://s02.upd.kaspersky.com https://s03.upd.kaspersky.com https://s04.upd.kaspersky.com https://s05.upd.kaspersky.com https://s06.upd.kaspersky.com https://s07.upd.kaspersky.com https://s08.upd.kaspersky.com https://s09.upd.kaspersky.com https://s10.upd.kaspersky.com https://s11.upd.kaspersky.com https://s12.upd.kaspersky.com https://s13.upd.kaspersky.com https://s14.upd.kaspersky.com https://s15.upd.kaspersky.com https://s16.upd.kaspersky.com https://s17.upd.kaspersky.com https://s18.upd.kaspersky.com https://s19.upd.kaspersky.com https://cm.k.kaspersky-labs.com	Mise à jour des bases de données, des modules logiciels et des applications de Kaspersky.
Port : 443 Protocole : HTTPS	https://downloads.upd.kaspersky.com	• Mise à jour des bases de données, des modules logiciels et des applications de Kaspersky. • Vérification de l'accessibilité des serveurs de Kaspersky. Avant de télécharger les bases de données et les modules logiciels de Kaspersky, Kaspersky Security Center vérifie si les serveurs de Kaspersky sont accessibles. Si l'accès aux serveurs via le DNS système n'est pas possible, l'application utilise les serveurs DNS publics.

Paramètres réseau	Adresse	Description
Port : 80 Protocole : HTTP	http://p00.upd.kaspersky.com http://p01.upd.kaspersky.com http://p02.upd.kaspersky.com http://p03.upd.kaspersky.com http://p04.upd.kaspersky.com http://p05.upd.kaspersky.com http://p06.upd.kaspersky.com http://p07.upd.kaspersky.com http://p08.upd.kaspersky.com http://p09.upd.kaspersky.com http://p10.upd.kaspersky.com http://p11.upd.kaspersky.com http://p12.upd.kaspersky.com http://p13.upd.kaspersky.com http://p14.upd.kaspersky.com http://p15.upd.kaspersky.com http://p16.upd.kaspersky.com http://p17.upd.kaspersky.com http://p18.upd.kaspersky.com http://p19.upd.kaspersky.com http://downloads0.kaspersky-labs.com http://downloads1.kaspersky-labs.com http://downloads2.kaspersky-labs.com http://downloads3.kaspersky-labs.com http://downloads4.kaspersky-labs.com http://downloads5.kaspersky-labs.com http://downloads6.kaspersky-labs.com http://downloads7.kaspersky-labs.com http://downloads8.kaspersky-labs.com http://downloads9.kaspersky-labs.com http://downloads.kaspersky-labs.com http://cm.k.kaspersky-labs.com	Mise à jour des bases de données, des modules logiciels et des applications de Kaspersky.
Port : 443 Protocole : HTTPS	ds.kaspersky.com dc1.ksn.kaspersky-labs.com dc1-file.ksn.kaspersky-labs.com dc1-pp.ksn.kaspersky-labs.com dc1-st.ksn.kaspersky-labs.com	Utilisation de Kaspersky Security Network.
Port : 443, 1443 Protocole : HTTPS	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-info-geo.kaspersky-labs.com ksn-cinfo-geo.kaspersky-labs.com	Utilisation de Kaspersky Security Network.

Paramètres réseau	Adresse	Description
Protocole : HTTPS	click.kaspersky.com redirect.kaspersky.com	En suivant les liens depuis l'interface.
Port : 80 Protocole : HTTP	http://crl.kaspersky.com http://ocsp.kaspersky.com	Ces serveurs font partie de l'infrastructure à clés publiques (PKI) et sont nécessaires pour vérifier l'état de validité des certificats de signature numérique de Kaspersky. La CRL est une liste de certificats révoqués. L'OCSP vous permet de demander l'état d'un certificat particulier en temps réel. Ces serveurs contribuent à garantir la sécurité des interactions avec les certificats numériques et à se protéger contre d'éventuelles attaques.
Port : 443 Protocole : HTTPS	https://ipm-klca.kaspersky.com	Annonces marketing.

Pour une interaction correcte de Kaspersky Security Center avec les services externes, tenez compte des recommandations suivantes :
- Le trafic réseau non chiffré doit être autorisé sur les ports 443 et 1443 sur l'équipement réseau et le serveur proxy de votre organisation.
- Lorsque le Serveur d'administration interagit avec les serveurs de mise à jour de Kaspersky et les serveurs de Kaspersky Security Network, il est nécessaire d'éviter de détourner le trafic réseau avec substitution de certificats (attaques MITM).

Pour télécharger les mises à jour via le protocole HTTP ou HTTPS à l'aide de l'utilitaire klscflag :

1. Exécutez l'invite de commande Windows en utilisant les droits d'administrateur, puis remplacez votre répertoire actuel par celui contenant l'utilitaire klscflag. L'utilitaire klsclag se trouve dans le dossier dans lequel le Serveur d'administration est installé. Chemin d'installation par défaut est <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

2. Si vous souhaitez télécharger les mises à jour via le protocole HTTP, exécutez une des commandes suivantes :

   - Sur l'appareil sur lequel le Serveur d'administration est installé :

     ```
     klscflag.exe -fset -pv klserver -s Updater -n DisableKLHttps -t d -v 1
     ```

   - Sur un point de distribution :

     ```
     klscflag.exe -fset -pv klnagent -s Updater -n DisableKLHttps -t d -v 1
     ```

   Si vous souhaitez télécharger les mises à jour via le protocole HTTPS, exécutez une des commandes suivantes :

   - Sur l'appareil sur lequel le Serveur d'administration est installé :

     ```
     klscflag.exe -fset -pv klserver -s Updater -n DisableKLHttps -t d -v 0
     ```

   - Sur un point de distribution :

     ```
     klscflag.exe -fset -pv klnagent -s Updater -n DisableKLHttps -t d -v 0
     ```

Déploiement de l'Agent d'administration et de l'application de sécurité

Pour administrer les appareils de l'entreprise, il faut installer l'Agent d'administration sur les appareils. Le déploiement de l'application distribuée Kaspersky Security Center sur les appareils de l'entreprise commence d'habitude par l'installation de l'Agent d'administration sur ceux-ci.

Sous Microsoft Windows XP, un Agent d'administration peut ne pas effectuer correctement les opérations suivantes : télécharger les mises à jour directement à partir des serveurs de Kaspersky (comme point de distribution) ; fonctionner comme proxy KSN (comme point de distribution) et détecter les vulnérabilités tierces (si la gestion des vulnérabilités et des correctifs est utilisée).

Déploiement initial

Pour administrer les appareils de l'entreprise, il faut installer l'Agent d'administration sur chaque appareil.

L'installation de l'Agent d'administration sur l'appareil administré fonctionnant sous Windows peut se faire de plusieurs manières :

- A l'aide d'outils tiers d'installation à distance d'applications.
- Via le clonage de l'image du disque dur de l'administrateur avec le système d'exploitation et l'Agent d'administration installé, à l'aide des ressources offertes par Kaspersky Security Center pour manipuler des images de disque ou à l'aide d'outils tiers.
- Via le mécanisme des stratégies de groupe Microsoft Windows, à l'aide des outils standard d'administration des stratégies de groupe Microsoft Windows ou de manière automatisée ou à l'aide de l'option correspondante dans la tâche d'installation à distance des applications de Kaspersky Security Center.
- En mode forcé, en utilisant les ressources du système d'exploitation via la tâche d'installation à distance de Kaspersky Security Center.
- Via l'envoi aux utilisateurs des appareils de liens vers les paquets autonomes créés par Kaspersky Security Center. Les paquets autonomes sont des modules exécutables qui contiennent la distribution des applications sélectionnés avec les paramètres configurés.
- Manuellement, en lançant les programmes d'installation sur les appareils.

L'installation initiale de l'Agent d'administration sur l'appareil administré fonctionnant sous Linux peut se faire de plusieurs manières :

- En vous connectant à l'Appareil administré via SSH et en exécutant la tâche d'installation à distance.
- En exécutant le programme d'installation du paquet sur l'appareil administré.

L'installation initiale de l'Agent d'administration sur l'appareil administré fonctionnant sous macOS peut se faire de plusieurs manières :

- En exécutant la tâche d'installation à distance sur le point de distribution macOS.
- Via l'envoi aux utilisateurs des appareils de liens vers les paquets autonomes créés par Kaspersky Security Center. Les paquets autonomes sont des modules exécutables qui contiennent la distribution des applications sélectionnés avec des paramètres prédéfinis.

Après le programme d'installation de l'Agent d'administration sur l'appareil, vous pouvez procéder à l'installation à distance des applications de Kaspersky sur cet appareil au moyen de cet Agent d'administration. Dans ce cas, le paquet de distribution de l'application à installer avec les paramètres d'installation définis par l'administrateur se réalise via les canaux de communication entre les Agents d'administration et le Serveur d'administration. Pour transférer le paquet de distribution, vous pouvez utiliser des centres intermédiaires de diffusion sous la forme de points de distribution, d'une diffusion multicast, etc.

Lors de la sélection des méthodes et des stratégies de déploiement des applications sur le réseau administré, il faut prendre en considération une série de facteurs (liste non exhaustive) :

- Configuration du réseau de l'organisation.
- Nombre total d'appareils.
- Présence sur le réseau de l'entreprise d'appareils qui n'appartiennent à aucun domaine Active Directory et présence de comptes utilisateurs unifiés avec les privilèges d'administrateur sur ces appareils.
- Capacité du canal entre le Serveur d'administration et les appareils.
- Caractère de la communication entre le Serveur d'administration et les sous-réseaux distants et la capacité des canaux réseau à l'intérieur de ces sous-réseaux.
- Paramètres de sécurité appliqués sur les appareils distants au début du déploiement. Ces paramètres permettent d'établir une connexion à distance à l'appareil administré et de lancer le programme d'installation.

Configuration des paramètres des programmes d'installation

Avant de procéder au déploiement des applications de Kaspersky dans le réseau, il faut définir les paramètres de l'installation, à savoir ces paramètres qui sont définis au cours de l'installation de l'application. Lors de l'installation de l'Agent d'administration, il faut définir au moins l'adresse pour la connexion au Serveur d'administration et, si possible, certains paramètres avancés. En fonction du mode d'installation choisi, les paramètres peuvent être définis de différentes façons. Dans le cas le plus simple (installation manuelle interactive sur l'appareil sélectionné), les paramètres indispensables peuvent être définis via l'interface utilisateur du programme d'installation.

Ce mode de configuration des paramètres est inappropriée pour une installation silencieuse des applications sur des groupes d'appareils. Dans un cas typique, l'administrateur doit définir centralement les valeurs des paramètres qui peuvent être utilisés par la suite pour l'installation silencieuse sur les appareils choisis dans le réseau.

Paquets d'installation

La méthode principale de configuration des paramètres d'installation des applications est universelle et convient à tous les moyens d'installation des applications : aussi bien via les outils de Kaspersky Security Center qu'à l'aide de la majorité des outils tiers. Ce moyen prévoit la création dans Kaspersky Security Center des paquets d'installation des applications.

Les paquets d'installation sont créés selon un des moyens suivants :

- Automatiquement au départ des distributions indiquées sur la base des *descripteurs* repris dans leur composition (fichiers portant l'extension kud contenant les règles de l'installation, l'analyse du résultat et d'autres informations).

- Depuis les fichiers exécutables des installateurs ou depuis les installateurs au format natif (.msi, .deb, .rpm), pour les applications standard ou prises en charge.

Les paquets d'installation créés sont organisés hiérarchiquement sous forme de dossiers avec des sous-dossiers et des fichiers. Outre le paquet de distribution original, le paquet d'installation contient également des paramètres modifiés (y compris les paramètres du programme d'installation et la règle du traitement de situations, comme la nécessité du redémarrage du système d'exploitation pour terminer l'installation), ainsi que de petits modules auxiliaires.

Les valeurs des paramètres d'installation propres à une application concrète prise en charge peuvent être définies dans l'interface utilisateur de la Console d'administration lors de la création du paquet d'installation. En cas d'installation à distance des applications via les outils de Kaspersky Security Center, les paquets d'installation sont remis aux appareils de telle sorte que le programme d'installation de l'application offre l'accès à tous les paramètres définis par l'administrateur disponibles pour cette application. En cas d'utilisation d'outils tiers pour installer des applications de Kaspersky, il suffit de garantir l'accès sur l'appareil à l'ensemble du paquet d'installation, à savoir la disponibilité du paquet de distribution et ses paramètres. Les paquets d'installation sont créés et enregistrés par Kaspersky Security Center dans un sous-dossier dédié du dossier partagé.

N'indiquez pas dans les paramètres des paquets d'installation les données des comptes utilisateur privilégiés.

Pour obtenir des instructions sur l'utilisation de cette méthode de configuration pour les applications de Kaspersky avant le déploiement via des outils tiers, consultez la section « Déploiement à l'aide du mécanisme des stratégies de groupe Microsoft Windows ».

Directement après l'installation de Kaspersky Security Center, plusieurs paquets d'installation, prêts à l'emploi, sont créés automatiquement. Il s'agit entre autres de paquets de l'Agent d'administration et de l'application de sécurité pour la plateforme Microsoft Windows.

Malgré le fait que la clé de licence pour la licence de l'application peut être définie dans les propriétés du paquet d'installation, il vaut mieux ne pas utiliser ce mode de diffusion des licences en raison de l'accessibilité des paquets d'installation en lecture. Il faut utiliser des clés de licence diffusées automatiquement ou les tâches pour l'installation des clés de licence.

Propriétés MSI et fichiers de transformation

Une autre manière configurer les paramètres de l'installation sur la plateforme Windows consiste à désigner les propriétés MSI et les fichiers de transformation. Cette méthode peut être utilisée dans les cas suivants :

- Lors de l'installation via des stratégies de groupe Windows à l'aide d'outils Microsoft standard ou d'autres outils tiers de manipulation des stratégies de groupe Windows.

- Lors de l'installation à l'aide d'outils tiers orientés sur une utilisation avec des programmes d'installation au format Microsoft Installer.

Déploiement à l'aide d'outils tiers d'installation à distance d'applications

Si l'entreprise possède d'autres moyens quelconque d'installation à distance des applications (par exemple, Microsoft System Center), il est conseillé de réaliser le déploiement initial à l'aide de ces outils.

Procédez comme suit :

- Sélectionner la méthode de configuration des paramètres d'installation la mieux adaptée à l'outil de déploiement utilisé.
- Définir le mécanisme de synchronisation entre la modification des paramètres des paquets d'installation dans l'interface de la Console d'administration et l'utilisation des outils tiers de déploiement des applications choisis depuis les données des paquets d'installation.
- En cas d'installation depuis le dossier partagé, il faut s'assurer que les performances de cette ressource fichiers sont suffisantes.

À propos des tâches d'installation à distance des applications de Kaspersky Security Center

Kaspersky Security Center propose les méthodes d'installation à distance d'applications les plus diverses, présentées sous la forme de tâches d'installation à distance des applications (installation forcée, installation à l'aide de la copie de l'image du disque dur, installation à l'aide de stratégies de groupe Microsoft Windows). Il est possible de créer une tâche d'installation à distance aussi bien pour un groupe d'administration indiqué que pour un ensemble d'appareils et des appareils spécifiques que pour une sélection d'appareils (ces tâches apparaissent dans la Console d'administration, dans le dossier **Tâches**). Lors de la création de la tâche, vous pouvez choisir les paquets d'installation (de l'Agent d'administration et/ou d'une autre application) qui peuvent être installés à l'aide de cette tâche ainsi que définir plusieurs paramètres qui définissent le mode d'installation à distance. De plus, il est possible d'utiliser l'Assistant de l'installation à distance des applications à la base duquel on retrouve également la création d'une tâche d'installation à distance d'applications et la surveillance des résultats.

Les tâches pour les groupes d'administration agissent non seulement sur les appareils affectés à un groupe spécifique, mais également sur tous les appareils de l'ensemble des sous-groupes de ce groupe d'administration. Si le paramètre correspondant est activé dans les paramètres de la tâche, la tâche s'applique aux appareils des Serveurs d'administration secondaires situés dans ce groupe ou dans ses sous-groupes.

Les tâches pour 'ensemble d'appareils mettent à jour la liste des appareils clients à chaque lancement, conformément à la composition de la sélection d'appareils au lancement de la tâche. Si la sélection d'appareils contient des appareils connectés à des Serveurs d'administration secondaires, la tâche est également lancée sur ces appareils. Pour en savoir plus sur ces paramètres et les modes d'installation, reportez-vous au reste de cette section.

Pour garantir le fonctionnement de la tâche d'installation à distance sur les appareils connectés à des Serveurs d'administration secondaires, il faut d'abord transmettre les paquets d'installation utilisés par la tâche aux Serveurs d'administration secondaires correspondant à l'aide d'une tâche de transmission.

Déploiement par prise d'image et copie d'image d'un appareil

S'il faut installer l'Agent d'administration sur des appareils sur lesquels il faut aussi installer (ou réinstaller) un système d'exploitation et d'autres logiciels, vous pouvez utiliser le mécanisme de capture et de copie de l'image de cet appareil.

Pour effectuer un déploiement en capturant et en copiant un disque dur, procédez comme suit :

1. Créer l'appareil de référence avec le système d'exploitation et l'ensemble de logiciels requis, y compris l'Agent d'administration et l'application de sécurité.

2. Prendre l'image de l'appareil « étalon », puis la diffuser sur les nouveaux appareils à l'aide d'une tâche de Kaspersky Security Center.

   Pour prendre l'image du disque et l'installer, vous pouvez utiliser les outils dont dispose l'entreprise ou la fonction offerte par Kaspersky Security Center (avec la licence de Gestion des vulnérabilités et des correctifs).

Si vous utilisez des outils tiers pour manipuler les images de disque, il faut veiller lors du déploiement sur l'appareil au départ de l'image étalon à supprimer les informations qui permettent à Kaspersky Security Center d'identifier l'appareil administré. Dans le cas contraire, le Serveur d'administration ne sera pas en mesure d'établir la distinction entre les appareils créés à l'aide de la copie de la même image.

Ce problème est résolu automatiquement lors de la prise de l'image à l'aide des outils de Kaspersky Security Center.

Copie de l'image du disque dur à l'aide d'outils tiers

En cas d'utilisation d'outils tiers pour prendre l'image de l'appareil doté d'un Agent d'administration, il faut utiliser une des méthodes suivantes :

- Méthode recommandée. Lors de l'installation de l'Agent d'administration sur un appareil étalon, capturez l'image de l'appareil avant le premier démarrage du service de l'Agent d'administration (vu que les informations uniques qui identifient l'appareil sont créées à la première connexion de l'Agent d'administration au Serveur d'administration). Par la suite, il est conseillé de ne pas accepter le lancement du service de l'Agent d'administration jusqu'à l'exécution de l'opération de prise de l'image.

- Sur l'appareil étalon, arrêter le service de l'Agent d'administration et lancer l'utilitaire klmover avec la clé -dupfix. L'utilitaire klmover fait partie du paquet d'installation de l'Agent d'administration. Par la suite, refuser le lancement du service de l'Agent d'administration jusqu'à l'exécution de l'opération de prise de l'image.

- Garantir le lancement de l'utilitaire klmover avec la clé -dupfix avant (point important) le premier lancement du service de l'Agent d'administration sur les appareils au premier démarrage du système d'exploitation après le déploiement de l'image. L'utilitaire klmover fait partie du paquet d'installation de l'Agent d'administration.

- Utilisez le mode de clonage de disque de l'Agent d'administration.

Si l'image du disque dur n'a pas été copiée correctement, vous pouvez résoudre ce problème.

Vous pouvez également capturer l'image d'un appareil sur lequel l'Agent d'administration n'est pas installé. Pour ce faire, exécutez le déploiement de l'image sur les appareils cibles, puis déployez l'Agent d'administration. Si vous utilisez cette méthode, autorisez l'accès au dossier réseau avec les paquets d'installation autonomes d'un appareil.

Erreur d'exécution de la copie de l'image du disque dur

Si la copie de l'image du disque dur avec l'Agent d'administration installé a été réalisée sans tenir compte des règles de déploiement, une partie des appareils dans la Console d'administration peut s'afficher comme une icône d'appareil dont le nom change en permanence.

Adoptez une des méthodes suivantes pour résoudre ce problème :

- Suppression de l'Agent d'administration

  Cette méthode est la plus sûre. Sur les appareils incorrectement copiés depuis l'image, il faut supprimer l'Agent d'administration à l'aide d'outils tiers, puis l'installer à nouveau. La suppression de l'Agent d'administration ne peut pas être exécutée à l'aide des outils de Kaspersky Security Center car pour le Serveur d'administration, il est impossible de discerner les appareils problématiques (ils correspondent tous à la même icône dans la Console d'administration).

- Lancement de l'utilitaire klmover avec la clé « -dupfix »

  Sur les appareils problématiques (tous ceux qui ont été copiés incorrectement depuis l'image), il faut lancer simultanément l'utilitaire klmover avec la clé « -dupfix » (klmover dupfix) situé dans le dossier d'installation de l'Agent d'administration à l'aide d'outils tiers. L'utilitaire ne peut être lancé à l'aide des outils de Kaspersky Security Center car pour le Serveur d'administration, il est impossible de discerner les appareils problématiques (ils correspondent tous à la même icône dans la Console d'administration).

  Ensuite, il faut supprimer l'icône sur laquelle les appareils problématiques s'affichaient avant le lancement de l'utilitaire.

- Durcissement de la règle de détection des appareils incorrectement copiés.

  > Cette méthode peut être utilisée uniquement si le Serveur d'administration et les Agents d'administration installés correspondent à la version 10 Service Pack 1 ou ultérieure.

  Il faut durcir la règle de détection des Agents d'administration incorrectement copiés de telle sorte que la modification du nom NetBIOS de l'appareil entraîne la « réparation » automatique de ces agents d'administration (on suppose que les appareils copiés possèdent des noms NetBIOS différents).

  Il faut importer le fichier reg ci-dessous dans le Registre de l'appareil doté du Serveur d'administration, puis relancer le Serveur d'administration.

  - Si l'appareil doté du Serveur d'administration tourne sous un système d'exploitation 32 bits :

```
REGEDIT4
[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags]
"KLSRV_CheckClones"=dword:00000003
```

  - Si l'appareil doté du Serveur d'administration tourne sous un système d'exploitation 64 bits :

```
REGEDIT4
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags]
"KLSRV_CheckClones"=dword:00000003
```

Déploiement à l'aide du mécanisme des stratégies de groupe Microsoft Windows

Il est conseillé de réaliser le déploiement initial des Agents d'administration à l'aide des stratégies de groupe Microsoft Windows quand les conditions suivantes sont remplies :

- Les appareils sont les membres du domaine Active Directory.
- Le plan de déploiement permet d'attendre le redémarrage standard des appareils avant le début du déploiement sur ceux ci des Agent d'administration ou la stratégie de groupe Windows peut être imposée aux appareils.

L'essence de ce mode de déploiement est la suivante :

- Le paquet de distribution de l'application au format Microsoft Installer (paquet MSI) se place dans le dossier partagé (le dossier accessible en lecture aux comptes utilisateurs LocalSystem des appareils).
- Dans la stratégie de groupe Active Directory, l'objet d'installation est créé pour le paquet de distribution.
- La zone d'action de l'installation est définie en indiquant l'organisation unitaire et/ou le groupe de sécurité qui contient le ou les appareil(s) cible(s).
- Lorsque l'appareil entre à nouveau dans le domaine (avant l'entrée des utilisateurs de l'appareil dans le système), la recherche de la présence de l'application requise parmi les applications installées a lieu. Si l'application est absente, le paquet de distribution est téléchargé depuis la ressource définie dans la stratégie, puis l'installation a lieu.

Un des avantages de ce mode de déploiement est le fait que les applications désignées sont installées sur les appareils lors du chargement du système d'exploitation avant l'entrée de l'utilisateur dans le système. Même si l'utilisateur doté des privilèges requis supprime l'application, celle-ci est à nouveau installée au prochain chargement du système d'exploitation. Ce mode de déploiement présente toutefois un inconvénient : les modifications introduites par l'administrateur dans la stratégie de groupe entrent en vigueur uniquement après le redémarrage des appareils (sans l'application des moyens complémentaires).

Les stratégies de groupe permettent d'installer l'Agent d'administration ainsi que d'autres applications dont les programmes d'installation possèdent le format Windows Installer.

Si vous choisissez ce mode de déploiement, il faut, entre autres, évaluer la charge sur la ressource fichier d'où les fichiers seront copiés vers les appareils au moment de l'application des stratégies de groupe Windows.

Utilisation des stratégies Microsoft Windows avec l'aide de la tâche d'installation à distance des applications de Kaspersky Security Center

La méthode la plus simple pour installer des applications à l'aide de stratégies de groupe Microsoft Windows consiste à sélectionner l'option **Réparer l'installation du paquet d'installation dans les stratégies de groupe d'Active Directory** dans les propriétés de la tâche d'installation à distance de Kaspersky Security Center. Dans ce cas, le Serveur d'administration exécute lui-même les actions suivantes au lancement de la tâche :

- Création des objets nécessaires dans la stratégie de groupe Microsoft Windows.
- Création des groupes spéciaux de sécurité qui reprennent les appareils et désignation de l'installation des applications sélectionnées pour ces groupes de sécurité. La composition du groupe de sécurité est actualisée à chaque lancement de la tâche conformément à l'ensemble d'appareils au moment du lancement.

Pour que cette fonction soit opérationnelle, il faut renseigner dans les paramètres de la tâche un compte utilisateur autorisé à modifier les stratégies de groupe Active Directory.

S'il est prévu d'installer l'Agent d'administration et une autre application au cours de la même tâche, la sélection de l'option **Réparer l'installation du paquet d'installation dans les stratégies de groupe d'Active Directory** entraîne la création dans la stratégie Active Directory d'un objet d'installation uniquement pour l'Agent d'administration. La deuxième application choisie dans la tâche s'installe quant à elle via les outils de l'Agent d'administration dès que celui-ci a été installé sur l'appareil. Si pour une raison quelconque il faut installer une application autre que l'Agent d'administration à l'aide de stratégies de groupe Windows, il faut créer une tâche d'installation uniquement pour ce paquet d'installation (sans le paquet de l'Agent d'administration). Toutes les applications ne peuvent pas être installées à l'aide des stratégies de groupe Microsoft Windows. Vous pouvez en savoir plus sur cette fonction en consultant les informations sur les modes d'installation de l'application.

Quand les objets nécessaires sont créés dans la stratégie de groupe via les outils de Kaspersky Security Center, la source du paquet d'installation est le dossier partagé de Kaspersky Security Center. Lors de la planification du déploiement, il faut comparer la vitesse de la lecture depuis ce dossier à la quantité d'appareils et à la taille du paquet de distribution à installer. Il sera probablement logique de placer le dossier partagé de Kaspersky Security Center dans un stockage spécialisé de fichiers puissant.

Outre sa simplicité, la création automatique de stratégies de groupe Windows à l'aide des outils de Kaspersky Security Center offre un autre avantage : lors de la planification de l'installation de l'Agent d'administration, il est facile de désigner le groupe d'administration de Kaspersky Security Center vers lequel les appareils vont être déplacés automatiquement à l'issue de l'installation. Le groupe peut être désigné dans l'Assistant de création d'une tâche ou dans la fenêtre des paramètres de la tâche d'installation à distance.

Dans le cadre de l'utilisation de stratégies de groupe Windows par les outils de Kaspersky Security Center, la désignation des appareils pour l'objet de la stratégie de groupe s'opère via la création d'un groupes de sécurité. Kaspersky Security Center synchronise la composition du groupe de sécurité avec l'ensemble actuel d'appareils de la tâche. En cas d'utilisation d'autres outils pour travailler avec les stratégies de groupe, il est possible d'associer des objets des stratégies de groupe directement aux sous-section Active Directory choisies.

Installation indépendante d'applications à l'aide de stratégies Microsoft Windows

L'administrateur peut créer lui-même dans la stratégie de groupe Windows les objets nécessaires à l'installation. Dans ce cas, il est possible de faire référence aux paquets qui se trouvent dans le dossier partagé de Kaspersky Security Center ou de placer les paquets sur un serveur de fichiers distinct et de les référencer.

Les scénarios d'installation suivants sont possible :

- L'administrateur crée le paquet d'installation et configure ses propriétés dans la Console d'administration. L'objet de la stratégie de groupe fait référence au fichier MSI de ce paquet d'installation qui se trouve dans le dossier partagé de Kaspersky Security Center.

- L'administrateur crée le paquet d'installation et configure ses propriétés dans la Console d'administration. Ensuite, l'administrateur copie l'ensemble du sous-dossier EXEC de ce paquet dans le dossier partagé de Kaspersky Security Center et le colle dans le dossier sur une ressource fichiers spéciale de l'entreprise. L'objet de la stratégie de groupe fait référence au fichier MSI de ce paquet configuré qui se trouve dans le sous-dossier sur une ressource fichier spéciale de l'entreprise.

- L'administrateur charge le paquet de distribution de l'application (y compris la distribution de l'Agent d'administration) depuis Internet et la place sur la ressource fichier spéciale de l'entreprise. L'objet de la stratégie de groupe fait référence au fichier MSI de ce paquet configuré qui se trouve dans le sous-dossier sur une ressource fichier spéciale de l'entreprise. La configuration des paramètres de l'installation s'opère via la configuration des propriétés MSI ou via la configuration des fichiers de transformation MST.

Déploiement forcé à l'aide d'une tâche d'installation à distance des applications de Kaspersky Security Center

Pour réaliser le déploiement initial de l'Agent d'administration ou d'autres applications, vous pouvez forcer l'installation des paquets d'installation sélectionnés à l'aide de la tâche d'installation à distance de Kaspersky Security Center, à condition que chaque appareil dispose d'un ou plusieurs comptes utilisateurs avec des droits d'administrateur local.

L'installation forcée peut être utilisée notamment dans le cas où le Serveur d'administration n'a pas d'accès direct aux appareils : par exemple, les appareils se trouvent sur des réseaux isolés ou bien ils se trouvent sur un réseau local, mais le Serveur d'administration se trouve dans la zone démilitarisée.

Lors du déploiement initial, l'Agent d'administration n'est pas installé. Par conséquent, dans les paramètres de la tâche d'installation à distance, il n'est pas possible de sélectionner la distribution des fichiers nécessaires à l'installation de l'application à l'aide de l'Agent d'administration. Vous pouvez uniquement choisir de distribuer des fichiers en utilisant les ressources du système d'exploitation par l'intermédiaire du Serveur d'administration ou des points de distribution.

Le service du Serveur d'administration doit être exécuté sous un compte disposant de privilèges d'administrateur sur les appareils cibles. Vous pouvez également désigner un compte ayant accès au partage admin$ dans les paramètres de la tâche d'installation à distance.

> Par défaut, la tâche d'installation à distance est appliquée aux appareils à l'aide des identifiants du compte sous lequel le Serveur d'administration est exécuté. Il est important de préciser qu'il s'agit du compte utilisé pour accéder au partage admin$, et non du compte sous lequel s'exécute la tâche d'installation à distance. L'installation s'effectue sous le compte LocalSystem.

Les appareils peuvent être désignés explicitement (via une liste) soit via la sélection du groupe d'administration de Kaspersky Security Center auquel ils appartiennent, soit via la création d'une sélection d'appareils selon une condition définie. Le début de l'installation est défini par la programmation de la tâche. Si le paramètre **Lancer les tâches non exécutées** est activé dans les propriétés de la tâche, la tâche peut être exécutée directement après l'activation des appareils ou lors de leur transfert dans le groupe d'administration cible.

L'installation forcée implique la remise des paquets d'installation aux appareils cibles, suivie de la copie des fichiers sur la ressource d'administration admin$ de chacun des appareils et l'enregistrement à distance sur ceux-ci des services auxiliaires. La remise des paquets d'installation sur les appareils cibles s'opère à l'aide de la fonction de Kaspersky Security Center chargée de l'interaction sur le réseau. Les conditions suivantes doivent être remplies :

- Les appareils cibles sont accessibles du côté du Serveur d'administration ou du point de distribution.
- La résolution des noms pour les appareils fonctionne correctement sur le réseau.
- Les ressources d'administration partagées admin$ ne sont pas désactivées sur les appareils administrés.
- Les services système suivants sont exécutés sur les appareils cibles :
  - Server (LanmanServer)

    Par défaut, ce service est exécuté.
  - DCOM Server Process Launcher (DcomLaunch)
  - RPC Endpoint Mapper (RpcEptMapper)
  - Remote Procedure Call (RpcSs)
- Le port TCP 445 est ouvert sur les appareils cibles pour permettre l'accès à distance via l'instrumentation de gestion Windows.

  Les protocoles TCP 139, UDP 137 et UDP 138 sont utilisés par des protocoles plus anciens et ne sont plus nécessaires pour les applications actuelles.

  Les ports d'accès dynamiques sortants doivent être autorisés sur le pare-feu pour les connexions du Serveur d'administration et des points de distribution vers les appareils cibles.
- Les paramètres de sécurité de la stratégie de domaine Active Directory sont autorisés à assurer le fonctionnement du protocole NTLM lors du déploiement de l'Agent d'administration.
- Sur les appareils cibles exécutant Microsoft Windows XP, le mode Simple File Sharing est désactivé.
- Sur les appareils cibles, le modèle d'accès partagé et de sécurité est défini sur *Habituel – les utilisateurs locaux s'authentifient comme eux-mêmes*. Il ne peut en aucun cas être défini sur *Invité – les utilisateurs locaux s'authentifient en tant qu'invité*.
- Les appareils appartiennent au domaine ou des comptes utilisateurs unifiés avec privilèges d'administration sont créés au préalable sur les appareils.

Pour réussir le déploiement de l'Agent d'administration ou d'autres applications sur un appareil qui n'est pas joint à un domaine Active Directory Windows Server 2003 ou une version ultérieure, vous devez désactiver le contrôle de compte d'utilisateur à distance sur cet appareil. Le contrôle de compte d'utilisateur à distance est l'une des raisons qui empêche les comptes d'administration locaux d'accéder à admin$, ce qui est nécessaire pour le déploiement forcé de l'Agent d'administration ou d'autres applications. La désactivation du contrôle de compte d'utilisateur à distance n'affecte pas le contrôle de compte d'utilisateur local.

Lors de l'installation sur de nouveaux appareils qui ne figurent pas encore dans les groupe d'administration de Kaspersky Security Center, il est possible de définir dans les propriétés de la tâche d'installation à distance le groupe d'administration dans lequel les appareils vont être placés à l'issue de l'installation de l'Agent d'administration sur ces appareils.

Lors de la création de la tâche de groupe, il ne faut pas oublier que la tâche de groupe agit sur les appareils de tous les sous-groupes du groupe sélectionné. C'est la raison pour laquelle il n'est pas nécessaire de duplique les tâches d'installation dans les sous-groupes.

L'installation automatique est un moyen simplifié de créer des tâches pour l'installation forcée d'applications. Pour cela, il faut sélectionner dans la liste des paquets d'installation des propriétés du groupe d'administration les paquets à installer sur les appareils de ce groupe. Au final, les paquets d'installation sélectionnés sont installés automatiquement sur tous les appareils de ce groupe et de ses sous-groupes. La période pendant laquelle les paquets sont installés dépend de la bande passe du réseau et du total d'appareils dans le réseau.

Pour réduire la charge sur le Serveur d'administration lors de la propagation des paquets d'installation sur les appareils, vous pouvez sélectionner l'installation via les points de distribution dans la tâche d'installation. Il ne faut pas oublier que ce mode d'installation génère une charge sensible sur les appareils désignés comme points de distribution. C'est la raison pour laquelle il est recommandé de sélectionner des appareils conformes aux exigences des points de distribution. Si vous utilisez des points de distribution, vous devez vous assurer qu'ils sont présents dans chacun des sous-réseaux isolés hébergeant des appareils cibles.

L'utilisation de points de distribution en guise de centres locaux d'installation peut être pratique notamment pour les installations sur des appareils dans des sous-réseaux connectés au Serveur d'administration via un canal de communication étroit alors qu'il existe un canal large entre les appareils au sein du sous-réseau.

Il faut que l'espace disponible dans la section contenant le dossier %ALLUSERSPROFILE %\Application Data\KasperskyLab\adminkit soit plusieurs fois supérieur au volume total des paquets de distribution des applications à installer.

Lancement de paquets autonomes créés par Kaspersky Security Center

Les méthodes décrites ci-dessus pour le déploiement initial de l'Agent d'administration et des applications ne sont pas toujours applicables en raison de l'impossibilité de remplir toutes les conditions requises. Dans ce cas, il est possible de créer un seul fichier exécutable au départ des paquets d'installations préparés par l'administrateur et dotés des paramètres requis pour l'installation à l'aide des outils de Kaspersky Security Center. Ce paquet est un *paquet d'installation autonome*. Le paquet d'installation autonome se place dans le dossier partagé de Kaspersky Security Center.

Kaspersky Security Center permet d'envoyer un lien aux utilisateurs sélectionnés par email. Ce lien mène au fichier dans le dossier partagé et le message invite le destinataire à lancer le fichier (en mode interactif ou en mode silencieux avec la clé « -s »). Le paquet d'installation autonome peut être joint au message électronique pour les utilisateurs des appareils qui n'ont pas accès au dossier partagé de Kaspersky Security Center. L'administrateur peut copier le paquet autonome sur un disque amovible et livrer le paquet à l'appareil requis en vue de son prochain démarrage.

Le paquet autonome peut être créé au départ du paquet de l'Agent d'administration, du paquet d'une autre application (par exemple, l'application de sécurité) ou directement au départ des deux paquets. Si le paquet autonome est créé au départ de l'Agent d'administration et d'une autre application, l'installation commence par l'Agent d'administration.

Lors de la création d'un paquet autonome avec l'Agent d'administration, il est possible d'indiquer le groupe d'administration dans lequel les nouveaux appareils (qui ne figuraient pas encore dans des groupes d'administration) vont être automatiquement placés à l'issue de l'installation de l'Agent d'administration.

Les paquets autonomes peuvent être installés interactivement (par défaut), avec l'affichage du résultat de l'installation des applications qu'ils contiennent ou en mode silencieux (lancement avec la clé " -s "). Le mode " silencieux " peut être utilisé pour une installation au départ de certains scripts (par exemple, des scripts configurés pour être lancés à la fin du déploiement de l'image du système d'exploitation, etc.). Le résultat de l'installation en mode " silencieux " est défini par le code de retour du processus.

L'Agent d'administration autonome pour Linux dépend, en option, de l'utilitaire nmap. Si l'utilitaire nmap n'existe pas ou est antérieur à la version 6.0, la fonctionnalité Broadcast DHCP Discover n'est pas prise en charge.

Possibilités d'installation manuelle des applications

Les administrateurs ou les utilisateurs expérimentés peuvent installer les applications manuellement en mode interactif. Ils peuvent utiliser dans ce cas de figure des distributions originales ou des paquets d'installation créés au départ de celles-ci et stockés dans le dossier partagé de Kaspersky Security Center. Les programmes d'installation fonctionnent par défaut en mode interactif et demande à l'utilisateur de confirmer toutes les valeurs des paramètres. Mais en cas de lancement du processus setup.exe depuis la racine du paquet d'installation avec la clé « -s », le programme d'installation fonctionne en mode « silencieux » selon les paramètres définis lors de la configuration du paquet d'installation.

Lors du lancement de setup.exe depuis la racine du paquet d'installation placé dans le dossier partagé de Kaspersky Security Center, le paquet est d'abord copié dans un dossier local temporaire, puis le programme d'installation de l'application est lancé depuis le dossier local.

Création d'un fichier MST

Pour transformer le contenu d'un paquet MSI et appliquer les paramètres de personnalisation à un fichier MSI existant, vous devez créer un fichier de transformation au format MST. Pour ce faire, utilisez l'éditeur Orca.exe, inclus dans le SDK Windows.

Pour créer un fichier MST, procédez comme suit :

1. Exécutez l'éditeur Orca.exe.
2. Accédez à l'onglet **Fichier**, puis dans le menu, cliquez sur **Ouvrir**.
3. Sélectionnez le fichier Kaspersky Network Agent.msi.
4. Accédez à l'onglet **Transformation** et, dans le menu, sélectionnez **Nouvelle transformation**.
5. Dans la colonne **Tableaux**, sélectionnez **Propriété** et écrivez les valeurs suivantes :
   - *EULA=1*
   - *SERVERADDRESS=<Adresse du Serveur d'administration>*

   Cliquez sur le bouton **Enregistrer**.
6. Accédez à l'onglet **Transformation** et, dans le menu, sélectionnez **Générer la transformation**.
7. Dans la fenêtre qui s'ouvre, indiquez un nom pour le fichier de transformation que vous créez, puis cliquez sur le bouton **Enregistrer**.

Le fichier MST est enregistré.

Installation à distance des applications sur les appareils dotés de l'Agent d'administration

Si un Agent d'administration opérationnel et connecté au Serveur d'administration principal (ou à un de ses Serveurs secondaires) est installé sur l'appareil, il est possible de mettre à niveau la version de l'Agent d'administration sur cet appareil ainsi que d'installer, mettre à niveau ou supprimer n'importe quelle application prise en charge à l'aide de l'Agent d'administration.

Vous pouvez activer l'option **En utilisant l'Agent d'administration** dans les propriétés de la tâche d'installation à distance.

Si cette option est sélectionnée, la transmission des paquets d'installation avec les paramètres d'installation définis par l'administrateur se réalise via les canaux de communication entre l'Agent d'administration et le Serveur d'administration.

Pour optimiser la charge sur le Serveur d'administration et limiter le trafic entre le Serveur d'administration et les appareils, il conseillé de désigner des points de distribution sur chaque réseau distant ou dans chaque domaine de diffusion (cf. les sections " Rôle des points de distribution " et " Élaboration de la structure de groupes d'administration et désignation des points de distribution "). Dans ce cas, la diffusion des paquets d'installation et des paramètres du programme d'installation se réalise depuis le Serveur d'administration sur les appareils via les points de distribution.

De même, l'utilisation des points de distribution permet de réaliser une multidiffusion des paquets d'installation. Ceci contribue à une réduction sensible du trafic réseau lors du déploiement des applications.

Lors de la transmission des paquets d'installation aux appareils via les canaux de communication entre les Agents d'administration et le Serveur d'administration, les paquets d'installation préparés pour la transmission sont également mis en cache dans le dossier %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\.working\FTServer. En cas d'utilisation d'un grand nombre de paquets d'installation divers de grande taille et en présence d'un nombre élevé de points de distribution, la taille de ce dossier peut sensiblement augmenter.

Il est impossible de supprimer manuellement des fichiers du dossier FTServer. Lors de la suppression des paquets d'installation d'origine, les données correspondantes sont également supprimées automatiquement du dossier FTServer.

Les données acceptées par les points de distribution sont conservées dans le dossier %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1103\$FTCITmp.

Il est impossible de supprimer manuellement des fichiers du dossier $FTCITmp. Le contenu de ce dossier est supprimé automatiquement au fur et à mesure que les tâches qui utilisent les données de ce dossier se terminent.

Puisque les paquets d'installation sont diffusés via les canaux de communication entre le Serveur d'administration et les Agents d'administration depuis un stockage intermédiaire et dans un format optimisé pour le transfert via le réseau, il ne faut pas modifier les paquets d'installation dans le dossier source du paquet d'installation. Ces modifications ne seraient pas automatiquement prises en compte par le Serveur d'administration. S'il est nécessaire de modifier manuellement les fichiers des paquets d'installation (bien que cela soit déconseillé), il faut absolument introduire la moindre modification des paramètres du paquet d'installation dans la Console d'administration. La modification des paramètres du paquet d'installation dans la Console d'administration oblige le Serveur d'administration à mettre à jour l'image du paquet dans le cache préparé pour le transfert sur les appareils.

Administration du redémarrage des appareils dans la tâche d'installation à distance

Souvent, pour terminer l'installation à distance des applications (surtout sur la plateforme Windows), il faut redémarrer l'appareil.

En cas d'utilisation de la tâche d'installation à distance des applications de Kaspersky Security Center, l'Assistant de création d'une tâche ou la fenêtre des propriétés de la tâche créée (section **Redémarrage du système d'exploitation**) vous permet de sélectionner l'action à effectuer lorsque l'appareil Windows nécessite un redémarrage :

- **Ne pas redémarrer l'appareil**. Dans ce cas, le redémarrage automatique n'a pas lieu. Pour terminer l'installation, il faut redémarrer l'appareil (par exemple, manuellement ou à l'aide d'une tâche d'administration des appareils). Les informations sur la nécessité du redémarrage seront enregistrées dans les résultats de la tâche et dans l'état de l'appareil. Cette option convient aux tâches d'installation sur les serveurs et autres appareils pour lesquels la continuité des opérations est critique.

- **Redémarrer l'appareil**. Dans ce cas, le redémarrage est toujours exécuté automatiquement, si celui-ci est requis pour terminer l'installation. Cette option convient aux tâches d'installation sur des appareils pour lesquels des interruptions périodiques sont admises (débranchement, redémarrage).

- **Demander à l'utilisateur**. Dans ce cas, le message sur le fait que l'appareil client doit être redémarré à la main s'affiche sur l'écran de l'appareil. Pour cette option, il est possible de configurer des paramètres avancés : le texte du message pour l'utilisateur, la fréquence du message, ainsi que le délai à l'issue duquel le redémarrage sera forcé (sans confirmation de l'utilisateur). L'option **Demander à l'utilisateur** convient le mieux aux postes de travail dont les utilisateurs doivent pouvoir choisir le moment qu'ils préfèrent pour le redémarrage.

Utilité de la mise à jour des bases de données dans le paquet d'installation de l'application de sécurité

Avant de déployer la protection, il faut tenir compte de la possibilité de mettre à jour les bases antivirus (y compris les modules des correctifs automatiques), diffusés en même temps que le paquet de distribution de l'application de sécurité. Il est conseillé de forcer la mise à jour dans le paquet d'installation de l'application avant le début du déploiement (par exemple, à l'aide de la commande correspondante dans le menu contextuel du paquet d'installation sélectionné). Cela réduit le nombre de redémarrages requis pour terminer le déploiement de la protection sur les appareils.

Utilisation des outils d'installation à distance des applications de Kaspersky Security Center pour lancer des fichiers exécutables arbitraires sur les appareils administrés

L'Assistant de création du paquet d'installation permet de choisir un fichier exécutable arbitraire et de définir pour celui-ci les paramètres de la ligne de commande. De plus, vous pouvez placer dans ce paquet d'installation le fichier sélectionné lui-même ou l'ensemble du dossier dans lequel ce fichier se trouve. Puis il faut créer la tâche d'installation à distance et choisir le paquet d'installation créé.

Lors de l'exécution de la tâche sur les appareils, le fichier exécutable indiqué à la création est lancé via la ligne de commande avec les paramètres définis.

En cas d'utilisation de programmes d'installation au format Microsoft Windows Installer (MSI), Kaspersky Security Center utilise les possibilités standard d'analyse du résultat de l'installation.

En présence d'une licence de Gestion des vulnérabilités et des correctifs, Kaspersky Security Center peut également utiliser les règles d'installation et d'analyse des résultats de l'installation, présents dans sa base mise à jour, lors de la création d'un paquet d'installation pour une des applications prises en charge et diffusées dans l'environnement de l'entreprise.

Dans d'autres cas, la tâche attend par défaut la fin du processus lancé et de tous ses processus enfants pour les fichiers exécutables. A la fin des processus lancés, la tâche réussit, quel que soit le code de retour du processus d'origine. Pour modifier ce comportement de tâche, avant la création de la tâche, vous devez modifier manuellement le fichier .kpd généré par Kaspersky Security Center dans le dossier et les sous-dosiers du paquet d'installation qui vient d'être créé.

Les fichiers .kpd utilisent le codage ASCII. Les fichiers .kud utilisent le codage Unicode.

Pour que la tâche n'attende pas la fin du processus lancé, il faut attribuer la valeur 0 au paramètre Wait dans la section [SetupProcessResult] :

```
[SetupProcessResult]
Wait=0
```

Sous Windows, pour que la tâche attende uniquement la fin du processus original et pas celle des processus enfant, il faut attribuer la valeur 0 au paramètres WaitJob dans la section [SetupProcessResult] :

```
[SetupProcessResult]
WaitJob=0
```

Pour que la tâche se termine correctement ou renvoie une erreur en fonction du code de retour du processus en cours d'exécution, créez un fichier .bat exécutable qui enregistre le code d'erreur dans un fichier, par exemple :

```
echo [ResponseResult] > setup.log
echo ResultCode=2 >> setup.log
exit 0
```

Modifiez ensuite les fichiers .kud générés par Kaspersky Security Center dans le dossier du paquet d'installation nouvellement créé :

```
[SetupMainResult]
File=setup.log
Section=ResponseResult
Value=ResultCode
[SetupMainResult_SuccessCodes]
0=Installation completed successfully.
[SetupMainResult_ErrorCodes]
1=Installation script error
2=Custom error
```

Dans ce cas, n'importe quel code différent des codes cités indique une erreur.

Pour que les résultats de la tâche reprennent une ligne avec un commentaire sur la réussite de la tâche ou un message d'erreur, il faut définir des descriptions brèves des erreurs correspondant aux codes de retour du processus dans les sections [SetupProcessResult_SuccessCodes] et [SetupProcessResult_ErrorCodes], par exemple :

```
[SetupProcessResult_SuccessCodes]
0= Installation completed successfully
3010=A reboot is required to complete the installation
[SetupProcessResult_ErrorCodes]
1602=Installation cancelled by the user
1603=Fatal error during installation
```

Pour que les outils de Kaspersky Security Center interviennent dans l'administration du redémarrage de l'appareil (si le redémarrage est nécessaire pour terminer l'opération), il faut énumérer en plus les codes de retour du processus qui indiquent la nécessité du redémarrage dans la section [SetupProcessResult_NeedReboot] :

```
[SetupProcessResult_NeedReboot]
3010=
```

Surveillance du déploiement

Pour contrôler le déploiement de Kaspersky Security Center et pour s'assurer de la présence sur les appareils administrés d'une application de sécurité et de l'Agent d'administration, vous devez vérifier l'indicateur de couleur dans la section **Déploiement**. L'indicateur se trouve dans l'espace de travail de l'entrée Serveur d'administration dans la fenêtre principale de la Console d'administration. L'indicateur affiche l'état actuel du déploiement. À côté de l'indicateur, on retrouve le nombre d'appareils dotés d'un Agent d'administration et d'applications de sécurité. En présence de tâches d'installation actives, l'état d'avancement de la tâche s'affiche. En cas d'erreur d'installation, le nombre d'erreurs apparaît ici. Pour voir les détails d'une erreur, cliquez sur le lien.

Vous pouvez également utiliser le diagramme de déploiement dans l'espace de travail du dossier **Appareils administrés** sous l'onglet **Groupes**. Le diagramme illustre le processus de déploiement : la quantité d'appareils sans Agent d'administration, avec Agent d'administration, avec Agent d'administration et application de sécurité.

Une description plus détaillée du déroulement du déploiement (ou de l'exécution d'une tâche d'installation en particulier) apparaît dans la fenêtre des résultats de l'exécution de la tâche correspondante d'installation à distance. La fenêtre des résultats est accessible via un clic droit et la sélection de **Résultats** dans le menu contextuel. La fenêtre propose deux listes : la liste du haut contient la liste des états de la tâche sur les appareils et la liste du bas reprend les événements de la tâche sur l'appareil sélectionné dans la liste du haut.

Les informations sur les erreurs de déploiement sont enregistrées dans le journal des événements Kaspersky sur le Serveur d'administration. Les informations relatives aux erreurs sont également accessibles dans la sélection d'événements correspondante dans l'entrée du Serveur d'administration, sous l'onglet **Événements**.

Configuration des paramètres des programmes d'installation

La section contient des informations sur les fichiers des programmes d'installation de Kaspersky Security Center et sur les paramètres d'installation, ainsi que des recommandations sur l'installation du Serveur d'administration et l'Agent d'administration en mode « silencieux ».

Informations générales

Les programmes d'installation des composants de Kaspersky Security Center 15.1 (le Serveur d'administration, l'Agent d'administration et la Console d'administration) ont été élaborés selon les technologies Windows Installer. Le noyau du programme d'installation est un paquet MSI. Ce format d'empaquetage de la distribution permet d'utiliser tous les avantages de la technologie Windows Installer : montée en puissance, possibilité d'utiliser le système d'application de correctifs et le système de transformation, possibilité d'installer des solutions tierces de manière centralisée, transparence de l'enregistrement dans le système d'exploitation.

Installation en mode silencieux (avec fichier des réponses)

Les programmes d'installation du Serveur d'administration et de l'Agent d'administration permettent d'utiliser un fichier de réponses (ss_install.xml) qui contient les paramètres de l'installation en mode silencieux sans intervention de l'utilisateur. Le fichier ss_install.xml se trouve dans le même dossier que le paquet MSI et il est utilisé automatiquement lors de l'installation en mode silencieux. Vous pouvez activer le mode silencieux d'installation à l'aide de la touche de ligne de commande "/s".

Exemple de lancement :

```
setup.exe /s
```

Avant de lancer le programme d'installation en mode silencieux, lisez le Contrat de licence utilisateur final (CLUF). Si le kit de distribution Kaspersky Security Center ne contient pas de fichier TXT avec le texte du CLUF, vous pouvez télécharger le fichier depuis le site de Kaspersky.

Le fichier ss_install.xml représente le format interne des paramètres du programme d'installation de Kaspersky Security Center. Les paquets de la distribution reprennent le fichier ss_install.xml avec les paramètres par défaut.

Veuillez ne pas modifier le fichier ss_install.xml manuellement. Ce fichier est modifié à l'aide des outils de Kaspersky Security Center lors de la modification des paramètres des paquets d'installation dans la Console d'administration.

Pour modifier le fichier de réponses pour l'installation du Serveur d'administration :

1. Ouvrez le paquet de distribution de Kaspersky Security Center. Si vous utilisez un fichier EXE de paquet complet, décompressez-le.

2. Créez le dossier Server, ouvrez la ligne de commande, puis exécutez la commande suivante :

   ```
   setup.exe /r ss_install.xml
   ```

   Le programme d'installation de Kaspersky Security Center démarre.

3. Suivez les étapes de l'Assistant pour configurer l'installation de Kaspersky Security Center.

   Lorsque vous avez terminé l'Assistant, le fichier de réponses est automatiquement modifié en fonction des nouveaux paramètres que vous avez définis.

Installation de l'Agent d'administration en mode silencieux (sans fichier des réponses)

L'Agent d'administration peut être installé à l'aide d'un seul paquet .msi, avec la définition des valeurs des propriétés MSI selon la méthode standard. Ce scénario permet d'installer l'Agent d'administration à l'aide de stratégies de groupe.

Ne renommez pas le paquet d'installation Kaspersky Network Agent.msi. Le fait de renommer ce paquet peut entraîner des erreurs d'installation lors de futures mises à jour de l'Agent d'administration.

Pour éviter tout conflit entre les paramètres définis à l'aide des propriétés MSI et les paramètres définis dans le fichier des réponses, il est possible de désactiver le fichier des réponses en définissant la propriété `DONT_USE_ANSWER_FILE=1`. Le fichier MSI se trouve dans le paquet de distribution de Kaspersky Security Center, dans le dossier Packages\NetAgent\exec. Vous trouverez ci-après un exemple de lancement du programme d'installation de l'Agent d'administration à l'aide du paquet .msi.

L'installation de l'Agent d'administration en mode silencieux requiert l'acceptation des dispositions du Contrat de licence utilisateur final (CLUF). Utilisez le paramètre `EULA=1` uniquement si vous avez entièrement lu, compris et accepté les conditions du Contrat de licence utilisateur final.

Exemple :
```
msiexec /i "Kaspersky Network Agent.msi" /qn DONT_USE_ANSWER_FILE=1 SERVERADDRESS=kscserver.mycompany.com EULA=1
```

Il est également possible de définir les paramètres d'installation du paquet msi en préparant au préalable un fichier de réponse (fichier avec l'extension mst). La commande ressemble à ceci :

Exemple :
```
msiexec /i "Kaspersky Network Agent.msi" /qn TRANSFORMS=test.mst;test2.mst
```

Plusieurs fichiers de transformation peuvent être indiqués dans une seule commande.

Si vous souhaitez mettre à niveau l'Agent d'administration à l'aide du programme d'installation de Windows, exécutez la commande suivante :

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
REINSTALL=ALL REINSTALLMODE=vomus /norestart
```

Configuration partielle des paramètres d'installation via setup.exe

Le lancement de 'installation des applications via setup.exe permet de transmettre au paquet MSI les valeurs de n'importe quelle propriété MSI.

La commande ressemble à ceci :

Exemple :
```
/v"PROPERTY_NAME1=PROPERTY_VALUE1 PROPERTYNAME2=PROPERTYVALUE2"
```

Paramètres d'installation du Serveur d'administration

Le tableau ci-après décrit les propriétés MSI que l'on peut configurer lors de l'installation du Serveur d'administration. Tous les paramètres sont facultatifs, à l'exception du Contrat de licence utilisateur final (EULA) et de la politique de confidentialité (PRIVACYPOLICY).

Paramètres d'installation du Serveur d'administration en mode silencieux

Propriété MSI	Description	Valeurs possibles
CLUF	Acceptation des conditions du Contrat de licence utilisateur final (paramètre obligatoire).	• 1 : j'ai entièrement lu, compris et accepté les conditions du Contrat de licence utilisateur final. • Une autre valeur ou non définie - Je refuse les conditions du Contrat de licence (l'installation n'aura pas lieu).
PRIVACYPOLICY	Acceptation des conditions de la Politique de confidentialité (paramètre obligatoire)	• 1—Je sais et j'accepte que mes données soient traitées et transmises (y compris à des pays tiers) comme décrit dans la Politique de confidentialité. Je confirme que j'ai entièrement lu et que je comprends la Politique de confidentialité. • Une autre valeur ou non définie - Je refuse les conditions de la Politique de confidentialité (l'installation n'aura pas lieu).
INSTALLATIONMODETYPE	Type d'installation du Serveur d'administration	• Standard. • Personnalisée.
INSTALLDIR	Dossier d'installation de l'application	Valeur de chaîne.
ADDLOCAL	Liste des modules à installer (séparés par une virgule).	CSAdminKitServer, NAgent, CSAdminKitConsole, NSAC, MobileSupport, KSNProxy, SNMPAgent, GdiPlusRedist, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86. Minimum suffisant pour l'installation correcte du Serveur d'administration dans la liste des modules : `ADDLOCAL=CSAdminKitServer, CSAdminKitConsole, KSNProxy, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86`
NETRANGETYPE	Taille du réseau.	• NRT_1_100 — de 1 à 100 appareils. • NRT_100_1000 : de 101 à 1000 appareils. • NRT_GREATER_1000 : plus de 1000 appareils.
SRV_ACCOUNT_TYPE	Mode de désignation de l'utilisateur pour le fonctionnement du service du Serveur d'administration.	• SrvAccountDefault : le compte utilisateur va être créé automatiquement. • SrvAccountUser : le compte utilisateur est créé manuellement.
SERVERACCOUNTNAME	Nom d'utilisateur pour le service.	Valeur de chaîne.
SERVERACCOUNTPWD	Mot de passe de l'utilisateur pour le service.	Valeur de chaîne.

Propriété MSI	Description	Valeurs possibles
DBTYPE	Type de la base de données.	• MySQL : une base de données MySQL ou MariaDB sera utilisée. • MSSQL : une base de données Microsoft SQL Server (SQL Express) sera utilisée.
MYSQLSERVERNAME	Nom complet du serveur MySQL ou MariaDB server	Valeur de chaîne.
MYSQLSERVERPORT	Le numéro de port pour se connecter au serveur MySQL ou MariaDB	Valeur numérique.
MYSQLDBNAME	Nom de la base de données du serveur MySQL ou MariaDB	Valeur de chaîne.
MYSQLACCOUNTNAME	Nom d'utilisateur pour la connexion à la base de données du serveur MySQL ou MariaDB	Valeur de chaîne.
MYSQLACCOUNTPWD	Mot de passe pour la connexion à la base de données du serveur MySQL ou MariaDB	Valeur de chaîne.
MSSQLCONNECTIONTYPE	Type d'utilisation de la base de données MSSQL.	• InstallMSSEE : installer à partir du paquet. • ChooseExisting : utiliser le serveur installé.
MSSQLSERVERNAME	Nom complet de l'instance de SQL Server.	Valeur de chaîne.
MSSQLDBNAME	Nom de la base de données de SQL Server.	Valeur de chaîne.
MSSQLAUTHTYPE	Mode d'authentification lors de la connexion à SQL Server.	• Windows. • SQLServer.
MSSQLACCOUNTNAME	Nom d'utilisateur pour la connexion à SQL Server en mode SQLServer.	Valeur de chaîne.
MSSQLACCOUNTPWD	Mot de passe de l'utilisateur pour la connexion à SQL Server en mode SQLServer.	Valeur de chaîne.

CREATE_SHARE_TYPE	Mode de définition du dossier partagé	• Create : créer un dossier partagé. Dans ce cas, il faut définir les propriétés :
		  • SHARELOCALPATH : le chemin d'accès au dossier local.
		  • SHAREFOLDERNAME : le nom de réseau du dossier.
		• Vide : il faut définir la propriété EXISTSHAREFOLDERNAME.

EXISTSHAREFOLDERNAME	Le chemin d'accès complet au dossier partagé existant.	Valeur de chaîne.
SERVERPORT	Le numéro de port pour se connecter au Serveur d'administration	Valeur numérique.
SERVERSSLPORT	Numéro de port pour l'établissement de la connexion SSL avec le Serveur d'administration.	Valeur numérique.
SERVERADDRESS	Adresse du Serveur d'administration	Valeur de chaîne.

Propriété MSI	Description	Valeurs possibles
SERVERCERT2048BITS	Longueur de la clé pour le certificat de Serveur d'administration (en bits)	• 1 : la longueur de la clé pour le certificat du Serveur d'administration est de 2048 bits. • 0 : la longueur de la clé pour le certificat du Serveur d'Administration est de 1024 bits. • Si la valeur n'est pas définie, la longueur de la clé pour le certificat du Serveur d'administration est de 2 048 bits.
MOBILESERVERADDRESS	Adresse du Serveur d'administration pour la connexion des appareils mobiles est ignoré si le module MobileSupport n'a pas été sélectionné.	Valeur de chaîne.

Paramètres d'installation de l'Agent d'administration

Le tableau ci-après décrit les propriétés MSI que l'on peut configurer lors de l'installation de l'Agent d'administration. Tous les paramètres sont facultatifs, à l'exception du Contrat de licence de l'utilisateur final (CLUF) et SERVERADDRESS.

Paramètres d'installation d e l'Agent d'administration en mode silencieux

Propriété MSI	Description	Valeurs possibles
CLUF	Accord avec les conditions du Contrat de licence	• 1 : je confirme que j'ai entièrement lu le présent Contrat de licence utilisateur final, que je le comprends et que j'accepte toutes ses conditions. • 0 : je refuse les conditions du Contrat de licence (l'installation n'aura pas lieu). • Aucune valeur : je refuse les conditions du Contrat de licence (l'installation n'aura pas lieu).
DONT_USE_ANSWER_FILE	Lire les paramètres d'installation dans le fichier des réponses	• 1—Ne pas utiliser. • Une autre valeur ou non définie—Lire.
INSTALLDIR	Chemin d'accès au dossier de l'Agent d'administration	Valeur de chaîne.
SERVERADDRESS	Adresse du Serveur d'administration (paramètre obligatoire)	Valeur de chaîne.
SERVERPORT	Numéro de port pour se connecter au Serveur d'administration	Valeur numérique.
SERVERSSLPORT	Le numéro du port pour établir une connexion sécurisée avec le Serveur d'administration via le protocole SSL	Valeur numérique.
USESSL	S'il faut utiliser la connexion SSL	• 1 : utiliser. • Une autre valeur ou non définie : ne pas utiliser.
OPENUDPPORT	S'il faut ouvrir le port UDP	• 1 : ouvrir. • Une autre valeur ou non définie : ne pas ouvrir.
UDPPORT	Numéro Port UDP	Valeur numérique.
USEPROXY	S'il faut utiliser le serveur proxy. Pour des raisons de compatibilité, il est déconseillé d'indiquer les paramètres de connexion par proxy dans les paramètres du paquet d'installation de l'Agent d'administration.	• 1 : utiliser. • Une autre valeur ou non définie : ne pas utiliser.

Propriété MSI	Description	Valeurs possibles
PROXYLOCATION (PROXYADDRESS:PROXYPORT)	Adresse du serveur proxy et numéro de port pour se connecter au serveur proxy	Valeur de chaîne.
PROXYLOGIN	Compte utilisateur pour se connecter au serveur proxy	Valeur de chaîne.
PROXYPASSWORD	Mot de passe du compte pour la connexion au serveur proxy (N'indiquez pas dans les paramètres des paquets d'installation les données des comptes utilisateur privilégiés.)	Valeur de chaîne.
GATEWAYMODE	Mode d'utilisation de la passerelle des connexions	• 0 : ne pas utiliser la passerelle de connexion. • 1 : utiliser l'Agent d'administration donné en tant que passerelle de connexion. • 2 : se connecter au Serveur d'administration via la passerelle de connexion.
GATEWAYADDRESS	Adresse de la passerelle de connexion	Valeur de chaîne.
CERTSELECTION	Mode d'obtention du certificat	• GetOnFirstConnection : obtenir un certificat du Serveur d'administration. • GetExistent : sélectionnez un certificat existant. Si vous choisissez cette option, il faut définir la propriété CERTFILE.
CERTFILE	Chemin d'accès au certificat	Valeur de chaîne.
VMVDI	Activer le mode dynamique pour Virtual Desktop Infrastructure (VDI)	• 1 : activer. • 0 : ne pas activer. • Aucune valeur : ne pas activer.
VMOPTIMIZE	Définit si les paramètres de l'Agent d'administration sont optimaux pour l'hyperviseur	• 1 : activer. • 0 : ne pas activer. • Aucune valeur : ne pas activer.
LAUNCHPROGRAM	S'il faut lancer le service de l'Agent d'administration après l'installation. Le paramètre est ignoré si VMVDI=1	• 1 : démarrer. • Une autre valeur ou non définie : ne pas lancer.
NAGENTTAGS	Tag pour l'Agent d'administration (a la priorité par rapport au tag fourni dans le fichier de réponse)	Valeur de chaîne.

Infrastructure virtuelle

Kaspersky Security Center prend en charge les machines virtuelles. Vous pouvez installer l'Agent d'administration et l'application de sécurité sur chaque machine virtuelle, et vous pouvez protéger les machines virtuelles au niveau de l'hyperviseur. Dans le premier cas, la protection des machines virtuelles peut être confiée à une application de sécurité standard ou à Kaspersky Security for Virtualization Light Agent. Dans le second cas, vous pouvez utiliser Kaspersky Security for Virtualization Agentless.

Kaspersky Security Center prend en charge le retour à l'état antérieur des machines virtuelles.

Recommandations sur la réduction de la charge sur les machines virtuelles

En cas d'installation de l'Agent d'administration sur une machine virtuelle, il faut envisager la possibilité de désactiver la partie des fonctions de Kaspersky Security Center qui ne sont pas très utiles aux machines virtuelles.

Lors de l'installation de l'Agent d'administration sur une machine virtuelle ou sur un modèle qui servira plus tard à créer des machines virtuelles, nous recommandons de réaliser les opérations suivantes :

- En cas d'installation à distance, sélectionnez l'option **Optimiser les paramètres pour VDI** dans la fenêtre des propriétés du paquet d'installation de l'Agent d'administration, dans la section **Avancé**.
- En cas d'installation interactive à l'aide de l'assistant, sélectionnez l'option **Optimiser les paramètres de l'Agent d'administration pour l'infrastructure virtuelle** dans la fenêtre de l'assistant.

En sélectionnant ces options, vous modifiez les paramètres de l'Agent d'administration afin que les fonctions suivantes soient désactivées par défaut (avant l'application d'une stratégie) :

- Réception d'informations sur les logiciels installés
- Réception d'informations sur la configuration matérielle
- Réception d'informations sur la présence de vulnérabilités
- Réception d'informations sur les mises à jour nécessaires

En général, les fonctions énumérées ne sont pas nécessaires sur les machines virtuelles dans la mesure où le logiciel et la configuration matérielle virtuelle sont homogènes.

Les fonctions peuvent être réactivées. Si n'importe laquelle des fonctions désactivées est malgré tout requise, elle peut être activée à l'aide d'une stratégie de l'Agent d'administration ou dans les paramètres locaux de l'Agent d'administration. Les paramètres locaux de l'Agent d'administration sont accessibles via le menu contextuel de l'appareil concerné dans la Console d'administration.

Prise en charge des machines virtuelles dynamiques

Kaspersky Security Center prend en charge les machines virtuelles dynamiques. Si une infrastructure virtuelle a été déployée sur le réseau de l'entreprise, il est possible d'utiliser dans certains cas des machines virtuelles dynamiques (temporaires). Ces machines sont créées avec des noms uniques au départ d'un modèle préparé par l'administrateur. L'utilisateur travaille un certain temps sur la machine créée et une fois désactivée, cette machine virtuelle disparaît de l'infrastructure virtuelle. Si Kaspersky Security Center a été déployé sur le réseau de l'entreprise, la machine virtuelle dotée de l'Agent d'administration est ajoutée à la base de données du Serveur d'administration. Une fois que machine virtuelle a été désactivée, son enregistrement doit également être supprimé de la base de données du Serveur d'administration.

Pour garantir le fonctionnement de la suppression automatique des enregistrements relatifs aux machines virtuelles, sélectionnez l'option **Activer le mode dynamique pour VDI** lors de l'installation de l'Agent d'administration sur le modèle qui va servir à la création des machines virtuelles dynamiques :

- En cas d'installation à distance : dans la fenêtre des propriétés du paquet d'installation de l'Agent d'administration (section **Avancé**)
- En cas d'installation interactive – dans l'assistant d'installation de l'Agent d'administration

Évitez de sélectionner l'option **Activer le mode dynamique pour VDI** lors de l'installation de l'Agent d'administration sur des appareils physiques.

Si les événements sur les machines virtuelles dynamiques doivent être conservés un certain temps sur le Serveur d'administration après la suppression des machines virtuelles, vous devez sélectionner l'option **Conserver les événements après la suppression des appareils** dans la section **Stockage d'événements** de la fenêtre des propriétés du Serveur d'administration, puis indiquer la durée de conservation maximale des événements en jours.

Nous vous déconseillons d'activer le chiffrement des disques sur les machines virtuelles dynamiques.

Prise en charge de la copie des machines virtuelles

Copier une machine virtuelle dotée de l'Agent d'administration ou la créer au départ d'un modèle doté de l'Agent d'administration est similaire au déploiement par prise d'une image du disque dur et copie de celui-ci. Pour cette raison, en général, lors de la copie de machines virtuelles, il faut réaliser les mêmes actions que lors du déploiement de l'Agent d'administration par copie d'une image du disque.

Cependant, dans les deux cas décrits ci-après, l'Agent d'administration détecte la copie automatiquement. Il n'est dès lors pas nécessaire d'exécuter les actions complexes décrites dans la section " Déploiement par prise d'image et copie d'image du disque dur de l'appareil " :

- Lors de l'installation de l'Agent d'administration, l'option **Activer le mode dynamique pour VDI** a été sélectionnée : après chaque redémarrage du système d'exploitation, cette machine virtuelle est considérée comme un nouvel appareil, qu'elle ait été copiée ou non.
- Utilisation d'un des hyperviseurs suivants : VMware™, HyperV® ou Xen® : l'Agent d'administration détermine l'opération de copie de la machine virtuelle à l'aide de la modification des indicateurs de la configuration matérielle virtuelle.

L'analyse des modifications de la configuration matérielle virtuelle n'est pas absolument sûre. Avant d'utiliser largement cette méthode, il faut d'abord confirmer son fonctionnement sur un nombre restreint de machines virtuelles pour la version de l'hyperviseur utilisée par l'entreprise.

Prise en charge de la restauration du système de fichiers pour les appareils dotés de l'Agent d'administration

Kaspersky Security Center est une application distribuée. La restauration du système de fichiers à un état antérieur sur un des appareils dotés de l'Agent d'administration entraîne une perte de la synchronisation des données et le fonctionnement incorrect de Kaspersky Security Center.

La restauration du système de fichiers (ou d'une de ses parties) à un état antérieur peut se produire dans les cas suivants :

- Lors de la copie de l'image du disque dur.
- Lors de la restauration de l'état de la machine virtuelle à l'aide des outils de l'infrastructure virtuelle.
- Lors de la restauration des données depuis la copie de sauvegarde ou du point de restauration.

S'agissant de Kaspersky Security Center, les seuls scénarios critiques sont ceux où un logiciel tiers sur les appareils dotés de l'Agent d'administration touche le dossier %ALLUSERSPROFILE %\Application Data\KasperskyLab\adminkit\. Pour cette raison, il faut veiller, dans la mesure du possible, à toujours exclure ce dossier de la procédure de restauration.

Vu que dans plusieurs entreprises, le règlement de travail prévoit la restauration de l'état du système de fichiers des appareils, Kaspersky Security Center, depuis la version 10 Maintenance Release 1 (le Serveur d'administration et les Agents d'administration doivent correspondre à la version 10 Maintenance Release 1 ou suivante), prend en charge la détection de la restauration du système de fichiers sur les appareils dotés de l'Agent d'administration. En cas de détection, ces appareils sont automatiquement reconnectés au Serveur d'administration avec un nettoyage et une synchronisation des données complets.

Dans Kaspersky Security Center 15.1, la prise en charge de la détection de la restauration du système de fichiers est activée par défaut.

Dans la mesure du possible, il faut éviter de restaurer le dossier %ALLUSERSPROFILE %\Application Data\KasperskyLab\adminkit\ sur les appareils dotés de l'Agent d'administration car la nouvelle synchronisation complète des données requiert un volume important de ressources.

La restauration de l'état du système n'est pas disponible sur les appareils dotés du Serveur d'administration. La restauration à l'état antérieur de la base de données utilisée par le Serveur d'administration est également impossible.

La restauration de l'état du Serveur d'administration au départ de la copie de sauvegarde est possible uniquement à l'aide de l'utilitaire standard klbackup.

Installation locale des applications

Cette section décrit la procédure d'installation des applications qui peuvent être uniquement installées localement sur les appareils.

Pour pouvoir installer localement des applications sur l'appareil client sélectionné, vous devez posséder les autorisations d'administrateur sur cet appareil.

Pour installer l'application localement sur l'appareil client sélectionné, procédez comme suit :

1. Installez sur l'appareil client l'Agent d'administration, puis configurez la connexion entre l'appareil client et le Serveur d'administration.

2. Installez sur l'appareil toutes les applications requises en fonction des descriptions présentées dans les manuels de ces dernières.

3. Installez sur le poste de travail de l'administrateur le plug-in d'administration pour chaque application installée.

Kaspersky Security Center prend aussi en charge la possibilité d'installation locale des applications à l'aide du paquet d'installation autonome. Kaspersky Security Center ne prend pas en charge l'installation de toutes les applications de Kaspersky.

Installation locale de l'Agent d'administration

Pour installer l'Agent d'administration sur l'appareil localement, procédez comme suit :

1. Sur l'appareil, lancez le fichier setup.exe du paquet de distribution reçu via Internet. Pour en savoir plus, reportez-vous à la rubrique suivante : Obtention du paquet d'installation de l'Agent d'administration à partir du kit de distribution de Kaspersky Security Center.

   La fenêtre de sélection des applications Kaspersky s'ouvre pour l'installation.

2. Dans la fenêtre de sélection des applications, cliquez sur le lien **Installer uniquement l'Agent d'administration de Kaspersky Security Center** pour démarrer l'Assistant d'installation de l'Agent d'administration. Suivez les instructions de l'assistant.

   a. **Serveur d'administration**

   Port

   Définit le port non-SSL utilisé par le Serveur d'administration pour recevoir les connexions des Agents d'administration.

   La valeur par défaut de cette option est 14000.

   Port SSL

   Définit le port SSL utilisé par le Serveur d'administration pour recevoir les connexions des Agents d'administration.

   Par défaut, cette option a la valeur 13000.

   Utiliser SSL pour se connecter au Serveur d'administration

   Si l'option est activée, la connexion au Serveur d'administration est établie via le port sécurisé à l'aide du protocole SSL.

   Cette option est activée par défaut.

   Autoriser l'Agent d'administration à ouvrir le port UDP

   Si cette option est activée, le programme d'installation ouvre automatiquement le port utilisé par le Serveur d'administration pour administrer l'appareil client et recevoir les informations à ce sujet.

   Cette option est activée par défaut.

   Port UDP

   Permet de configurer le port utilisé par le Serveur d'administration pour administrer l'appareil client et recevoir les informations à son sujet.

   La valeur 15000 est définie par défaut pour cette option.

   b. **Configuration du serveur proxy**

Utiliser un serveur proxy

Si cette option est activée, vous pouvez indiquer les identifiants pour l'authentification sur le serveur proxy.

Nous vous recommandons de spécifier les informations d'identification d'un compte disposant des privilèges minimaux requis uniquement pour l'authentification sur le serveur proxy.

Cette option est Inactif par défaut.

Adresse

Port

Compte utilisateur

Le nom d'utilisateur du compte à partir duquel la connexion au serveur proxy est effectuée.

Nous vous recommandons de spécifier les informations d'identification d'un compte disposant des privilèges minimaux requis uniquement pour l'authentification sur le serveur proxy.

Mot de passe

Le mot de passe du compte à partir duquel la connexion au serveur proxy est effectuée.

Nous vous recommandons de spécifier les informations d'identification d'un compte disposant des privilèges minimaux requis uniquement pour l'authentification sur le serveur proxy.

c. Passerelle de connexion

Ne pas utiliser la passerelle de connexion

Utiliser l'Agent d'administration en tant que passerelle de connexion en DMZ

Sélectionnez cette option pour utiliser l'Agent d'administration comme passerelle de connexion dans la zone démilitarisée (DMZ) pour vous connecter au Serveur d'administration, communiquer avec lui et conserver les données sur l'Agent d'administration en toute sécurité pendant la transmission des données.

Se connecter au Serveur d'administration au moyen d'une passerelle de connexion

Sélectionnez cette option, puis indiquez l'appareil qui agira comme passerelle de connexion.

d. **Certificat du Serveur d'administration**

e. **Tags de l'agent**

f. Paramètres avancés

Installer automatiquement les mises à jour et les correctifs nécessaires pour les modules dont l'état est Non défini

Nous vous recommandons de laisser cette option activée. Vous pouvez décocher cette option pour désactiver la mise à jour automatique et les correctifs des modules de Kaspersky Security Center. L'administrateur peut réactiver l'installation automatique plus tard à l'aide d'une stratégie.

Cette option est Inactif par défaut.

Activer la protection du service de l'Agent d'administration

Lorsque cette option est activée, après l'installation de l'Agent d'administration sur un appareil administré, le module ne peut pas être supprimé ou reconfiguré sans les privilèges requis. Il est impossible d'arrêter le service de l'Agent d'administration. Cette option n'a aucun effet sur les contrôleurs de domaine.

Activez cette option pour protéger l'Agent d'administration sur les postes de travail exploités avec des privilèges d'administrateur local.

Cette option est Inactif par défaut.

Activer le mode dynamique pour VDI

Si cette option est activée, pour l'Agent d'administration installé sur la machine virtuelle, le mode dynamique pour Virtual Desktop Infrastructure (VDI) sera activé.

Cette option est Inactif par défaut.

Optimisez les paramètres de l'Agent d'administration de Kaspersky Security Center pour VDI. Désactiver l'analyse des vulnérabilités et l'inventaire des applications et du matériel. Vous pouvez modifier les paramètres actuels via les stratégies de l'Agent d'administration.

Si cette option est activée, les fonctionnalités suivantes sont désactivées dans les paramètres de l'Agent d'administration :

- Réception d'informations sur les logiciels installés
- Réception d'informations sur la configuration matérielle
- Réception d'informations sur la présence de vulnérabilités
- Réception d'informations sur les mises à jour nécessaires

Cette option est Inactif par défaut.

g. **Lancer l'application**

A la fin du travail de l'Assistant d'installation, l'Agent d'administration est installé sur l'appareil.

Vous pouvez consulter les propriétés du service de l'Agent d'administration de Kaspersky Security Center. Vous pouvez également lancer, arrêter et suivre le fonctionnement de l'Agent d'administration à l'aide des outils standard d'administration Microsoft Windows : Administration de l'ordinateur\Services.

Installation de l'Agent d'administration en mode silencieux

L'Agent d'administration peut être installé en mode silencieux, c'est-à-dire sans saisie interactive des paramètres d'installation. L'installation silencieuse utilise un paquet Windows Installer (MSI) pour l'Agent d'administration. Le fichier MSI se trouve dans le paquet de distribution de Kaspersky Security Center, dans le dossier Packages\NetAgent\exec.

Ne renommez pas le paquet d'installation Kaspersky Network Agent.msi. Le fait de renommer ce paquet peut entraîner des erreurs d'installation lors de futures mises à jour de l'Agent d'administration.

L'installation de l'Agent d'administration à partir du paquet MSI n'est possible qu'en mode silencieux, l'installation interactive à partir du paquet MSI n'est pas prise en charge.

Pour installer l'Agent d'administration sur un appareil local en mode silencieux :

1. Lisez le Contrat de licence utilisateur final. Utilisez la commande ci-dessous uniquement si vous comprenez et acceptez les conditions du Contrat de licence utilisateur final.

2. exécutez la commande

   ```
   msiexec /i "Kaspersky Network Agent.msi" /qn <setup_parameters>
   ```

   où `setup_parameters` est une liste des paramètres et de leurs valeurs, séparés l'un de l'autre par un espace (`PROP1=PROP1VAL PROP2=PROP2VAL`).

   Dans la liste de paramètres, vous devez inclure `EULA=1`. Sinon, l'Agent d'administration ne sera pas installé.

Si vous utilisez les paramètres de connexion standard pour Kaspersky Security Center, et pour l'Agent d'administration sur les appareils distants, exécutez la commande suivante :

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
SERVERADDRESS=kscserver.mycompany.com EULA=1
```

`/l*vx` est la clé pour écrire les journaux. Le journal est créé lors de l'installation de l'Agent d'administration et enregistré dans C:\windows\temp\nag_inst.log.

En plus du fichier nag_inst.log, l'application crée le fichier $klssinstlib.log, qui contient le journal d'installation. Ce fichier est stocké dans le dossier %windir%\temp ou %temp%. À des fins de dépannage, vous ou un spécialiste du Support Technique de Kaspersky pouvez avoir besoin des deux fichiers journaux suivants : nag_inst.log et $klssinstlib.log.

Si vous devez en outre spécifier le port de connexion au Serveur d'administration, exécutez la commande suivante :

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
SERVERADDRESS=kscserver.mycompany.com EULA=1 SERVERPORT=14000
```

Le paramètre `SERVERPORT` correspond au numéro de port pour la connexion au Serveur d'administration.

Les noms et les valeurs possibles des paramètres qui peuvent être utilisés lors de l'installation de l'Agent d'administration en mode silencieux sont cités dans la section Paramètres d'installation de l'Agent d'administration.

Si vous souhaitez mettre à niveau l'Agent d'administration à l'aide du programme d'installation de Windows, exécutez la commande suivante :

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
REINSTALL=ALL REINSTALLMODE=vomus /norestart
```

Installation de l'Agent d'administration pour Linux en mode silencieux (avec un fichier de réponse)

Vous pouvez installer l'Agent d'administration sur des appareils Linux à l'aide d'un fichier de réponse. Il s'agit d'un fichier texte qui contient un ensemble personnalisé de paramètres d'installation : les variables et leurs valeurs respectives. L'utilisation de ce fichier de réponse vous permet d'exécuter une installation en mode silencieux, c'est-à-dire sans la participation de l'utilisateur.

Pour effectuer l'installation de l'Agent d'administration pour Linux en mode silencieux, procédez comme suit :

1. Préparez l'appareil Linux approprié pour l'installation à distance. Téléchargez et créez le paquet d'installation à distance à l'aide d'un paquet .deb ou .rpm de l'Agent d'administration, au moyen de tout système de gestion de paquets approprié.

2. Si vous souhaitez installer l'Agent d'administration sur des appareils dotés du système d'exploitation SUSE Linux Enterprise Server 15, installer le paquet insserv-compat en premier pour configurer l'Agent d'administration.

   Si vous souhaitez installer l'Agent d'administration sur des appareils qui utilisent le système d'exploitation RED OS 7.3.4 ou une version ultérieure ou MSVSPHERE 9.2 ou une version ultérieure, installez le paquet libxcrypt-compat pour assurer le bon fonctionnement de l'Agent d'administration.

3. Lisez le Contrat de licence utilisateur final. Suivez les étapes ci-dessous uniquement si vous comprenez et acceptez les conditions du Contrat de licence utilisateur final.

4. Créez le fichier de réponse (au format TXT). Ajoutez au fichier de réponse une liste de variables au format VARIABLE_NAME=variable_value, chaque variable sur une ligne distincte.

   Pour assurer une utilisation correcte du fichier de réponse, vous devez y inclure un ensemble minimum des trois variables requises :

   - KLNAGENT_SERVER
   - KLNAGENT_AUTOINSTALL
   - EULA_ACCEPTED

   Vous pouvez également ajouter des variables facultatives pour utiliser des paramètres plus spécifiques de votre installation à distance. Le tableau suivant affiche toutes les variables pouvant être incluses dans le fichier de réponse :

   Variables du fichier de réponse utilisées comme paramètres de l'installation de l'Agent d'administration pour Linux en mode silencieux

Variables du fichier de réponse utilisées comme paramètres de l'installation de l'Agent d'administration pour Linux en mode silencieux

Nom de la variable	Requis	Description	Valeurs possibles
KLNAGENT_SERVER	Oui	Contient le nom du Serveur d'administration présenté comme nom de domaine pleinement qualifié (FQDN) ou adresse IP.	Nom DNS ou adresse IP.
KLNAGENT_AUTOINSTALL	Oui	Définit si le mode d'installation silencieux est activé.	1 : le mode silencieux est activé ; l'utilisateur n'est invité à aucune action lors de l'installation. Autre : le mode silencieux est désactivé ; l'utilisateur peut être invité à effectuer des actions lors de l'installation.
EULA_ACCEPTED	Oui	Définit si l'utilisateur accepte le Contrat de licence utilisateur final (CLUF) de l'Agent d'administration ; lorsqu'il est manquant, il peut être interprété comme une non-acceptation du CLUF.	1 : je confirme que j'ai entièrement lu le présent Contrat de licence utilisateur final, que je le comprends et que j'accepte toutes ses conditions. Autre valeur ou valeur non définie : je refuse les conditions du Contrat de licence (l'installation n'aura pas lieu).
KLNAGENT_PROXY_USE	Non	Définit si la connexion avec le Serveur d'administration utilisera les paramètres du proxy. La valeur par défaut est égale à 0.	1 : les paramètres du proxy sont utilisés. Autre : les paramètres du proxy ne sont pas utilisés.
KLNAGENT_PROXY_ADDR	Non	Définit l'adresse du serveur proxy utilisé pour la connexion avec le Serveur d'administration.	Nom DNS ou adresse IP.
KLNAGENT_PROXY_LOGIN	Non	Définit le nom d'utilisateur utilisé pour établir la connexion au serveur proxy.	Tout nom d'utilisateur existant.
KLNAGENT_PROXY_PASSWORD	Non	Définit le mot de passe d'utilisateur utilisé pour établir la connexion au serveur proxy.	Tout jeu de caractères alphanumériques autorisé par le format du mot de passe dans le système d'exploitation.
KLNAGENT_VM_VDI	Non	Définit si l'Agent d'administration est installé sur une image pour la création de machines virtuelles dynamiques.	1 : l'Agent d'administration est installé sur une image, qui est ensuite utilisée pour la création de machines virtuelles dynamiques. Autre : aucune image n'est utilisée pendant l'installation.
KLNAGENT_VM_OPTIMIZE	Non	Définit si les paramètres de l'Agent d'administration sont optimaux pour l'hyperviseur.	1 : les paramètres locaux par défaut de l'Agent d'administration sont modifiés afin de permettre une utilisation optimisée sur l'hyperviseur.
KLNAGENT_TAGS	Non	Répertorie les balises attribuées à l'instance de l'Agent d'administration.	Un ou plusieurs noms de balises séparés par un point-virgule.
KLNAGENT_UDP_PORT	Non	Définit le port UDP utilisé par l'Agent d'administration. La valeur par défaut est égale à 15000.	Tout numéro de port existant.
KLNAGENT_PORT	Non	Définit le port non TLS utilisé par l'Agent d'administration. La valeur par défaut est égale à 14000.	Tout numéro de port existant.

KLNAGENT_SSLPORT	Non	Définit le port TLS utilisé par l'Agent d'administration. La valeur par défaut est égale à 13000.	Tout numéro de port existant.
KLNAGENT_USESSL	Non	Définit si le protocole TLS (Transport Layer Security ou Sécurité de la couche de transport) est utilisé pour établir la connexion.	1 (par défaut) : le protocole TLS est utilisé. Autre : le protocole TLS n'est pas utilisé.
KLNAGENT_GW_MODE	Non	Définit si la passerelle de connexion est utilisée.	1 (par défaut) : les paramètres actuels ne sont pas modifiés (au premier appel, aucune passerelle de connexion n'est définie). 2 : aucune passerelle de connexion n'est utilisée. 3 : une passerelle de connexion est utilisée. KLNAGENT_GW_ADDRESS est requis. 4 : l'instance de l'Agent d'administration est utilisée comme passerelle de connexion dans la zone démilitarisée (DMZ). Un certificat de serveur est requis.
KLNAGENT_GW_ADDRESS	Non	Définit l'adresse de la passerelle de connexion. La valeur n'est applicable que si KLNAGENT_GW_MODE=3.	Nom DNS ou adresse IP.
KLNAGENT_DEVICEOWNER_REGISTRATION_START	Non	Permet d'exécuter l'enregistrement de l'utilisateur en tant que propriétaire de l'appareil après l'installation de l'Agent d'administration. Si cette option est désactivée, l'enregistrement en tant que propriétaire de l'appareil n'est pas disponible pour l'utilisateur.	1 : l'enregistrement de l'utilisateur en tant que propriétaire de l'appareil sera lancé après l'installation de l'Agent d'administration. Autre : désactivé.

5. Installez l'Agent d'administration. La variable d'environnement KLAUTOANSWERS, qui spécifie le chemin d'accès au fichier de réponse, est transmise à la commande d'installation. Exécutez l'une des commandes suivantes :

   - Pour installer l'Agent d'administration à partir d'un paquet RPM sur un système d'exploitation 32 bits, exécutez la commande suivante :
     `sudo KLAUTOANSWERS=<chemin vers le fichier de réponse> yum install ./klnagent-<numéro de build>.i386.rpm`

   - Pour installer l'Agent d'administration à partir d'un paquet RPM sur un système d'exploitation 64 bits, exécutez la commande suivante :
     `sudo KLAUTOANSWERS=<chemin vers le fichier de réponse> yum install ./klnagent64-<numéro de build>.x86_64.rpm`

   - Pour installer l'Agent d'administration à partir d'un paquet RPM sur un système d'exploitation 64 bits pour l'architecture ARM, exécutez la commande suivante :
     `sudo KLAUTOANSWERS=<chemin vers le fichier de réponse> yum install ./klnagent64-<numéro de build>.aarch64.rpm`

   - Pour installer l'Agent d'administration à partir d'un paquet DEB sur un système d'exploitation 32 bits, exécutez la commande suivante :
     `sudo KLAUTOANSWERS=<chemin du fichier de réponse> apt install ./klnagent_<numéro de build>_i386.deb`

- Pour installer l'Agent d'administration à partir d'un paquet DEB dans un système d'exploitation 64 bits, exécutez la commande suivante :
  `sudo KLAUTOANSWERS=<chemin vers le fichier de réponse> apt install ./klnagent64_<numéro de build>_amd64.deb`

- Pour installer l'Agent d'administration à partir d'un paquet DEB sur un système d'exploitation 64 bits pour l'architecture ARM, exécutez la commande suivante :
  `sudo KLAUTOANSWERS=<chemin vers le fichier de réponse> apt install ./klnagent64_<numéro de build>_arm64.deb`

Selon la configuration du système d'exploitation, vous pouvez également utiliser les gestionnaires de paquets rpm, dpkg ou dnf pour installer l'Agent d'administration.

L'installation de l'Agent d'administration pour Linux démarre en mode silencieux ; l'utilisateur n'est invité à aucune action pendant le processus.

Préparation d'un appareil exécutant Astra Linux dans l'environnement logiciel fermé mode pour l'installation de l'Agent d'administration

Avant l'installation de l'Agent d'administration sur un appareil exécutant Astra Linux en mode environnement logiciel fermé, vous devez effectuer deux procédures de préparation : celle des instructions ci-dessous et les étapes générales de préparation pour tout appareil Linux.

Exécutez les commandes fournies dans cette instruction sous un compte avec des privilèges root.

Pour préparer un appareil exécutant Astra Linux dans l'environnement logiciel fermé mode en vue de l'installation de l'Agent d'administration, procédez comme suit :

1. Ouvrez le fichier `/etc/digsig/digsig_initramfs.conf`, puis définissez le paramètre suivant :
   `DIGSIG_ELF_MODE=1`

2. Dans la ligne de commande, exécutez la commande suivante pour installer le paquet de compatibilité :
   `apt install astra-digsig-oldkeys`

3. Créez un répertoire pour la clé de l'application :
   `mkdir -p /etc/digsig/keys/legacy/kaspersky/`

4. Placez la clé de l'application /opt/kaspersky/klnagent64/share/kaspersky_astra_pub_key.gpg dans le répertoire créé à l'étape précédente :
   `cp kaspersky_astra_pub_key.gpg /etc/digsig/keys/legacy/kaspersky/`

   Si le kit de distribution de Kaspersky Security Center n'inclut pas la clé de l'application kaspersky_astra_pub_key.gpg, vous pouvez le télécharger en cliquant sur le lien : https://media.kaspersky.com/utilities/CorporateUtilities/kaspersky_astra_pub_key.gpg.

5. Mettez à jour les disques RAM :
   `update-initramfs -u -k all`
   Redémarrez le système.

L'appareil Linux est prêt pour l'installation de l'Agent d'administration. Vous pouvez installer l'Agent d'administration à distance, en mode interactif ou en mode silencieux.

Installation de l'Agent d'administration pour Linux en mode interactif

Cet article décrit comment installer l'Agent d'administration sur les appareils Linux en mode interactif en définissant les paramètres d'installation pas à pas. Vous pouvez installer l'Agent d'administration sur des appareils Linux à l'aide d'un fichier de réponse. Il s'agit d'un fichier texte qui contient un ensemble personnalisé de paramètres d'installation : les variables et leurs valeurs respectives. L'utilisation de ce fichier de réponse vous permet d'exécuter une installation en mode silencieux, c'est-à-dire sans la participation de l'utilisateur.

> Si vous souhaitez installer l'Agent d'administration sur des appareils qui utilisent le système d'exploitation RED OS 7.3.4 ou une version ultérieure ou MSVSPHERE 9.2 ou une version ultérieure, installez le paquet libxcrypt-compat pour assurer le bon fonctionnement de l'Agent d'administration.

Pour installer l'Agent d'administration en mode interactif, procédez comme suit :

1. Installez l'Agent d'administration. En fonction de votre distribution Linux, exécutez l'une des commandes suivantes :

   - Pour installer l'Agent d'administration à partir d'un paquet RPM dans le système d'exploitation 32 bits :

     ```
     # yum -i klnagent-<numéro de build>.i386.rpm
     ```

   - Pour installer l'Agent d'administration à partir d'un paquet RPM dans le système d'exploitation 64 bits :

     ```
     # yum -i klnagent64-<numéro de build>.x86_64.rpm
     ```

   - Pour installer l'Agent d'administration à partir d'un paquet RPM dans le système d'exploitation 64 bits pour architecture Arm :

     ```
     # yum -i klnagent64-<numéro de build>.aarch64.rpm
     ```

   - Pour installer l'Agent d'administration à partir d'un paquet DEB dans le système d'exploitation 32 bits :

     ```
     # apt install ./klnagent_<numéro de build>_i386.deb
     ```

   - Pour installer l'Agent d'administration à partir d'un paquet DEB dans le système d'exploitation 64 bits :

     ```
     # apt install ./klnagent64_<numéro de build>_amd64.deb
     ```

   - Pour installer l'Agent d'administration à partir d'un paquet DEB dans le système d'exploitation 64 bits pour architecture Arm :

     ```
     # apt install ./klnagent64_<numéro de build>_arm64.deb
     ```

2. Configurez l'Agent d'administration :

   ```
   # /opt/kaspersky/klnagent64/lib/bin/setup/postinstall.pl
   ```

3. Lisez le Contrat de licence utilisateur final (CLUF). Le texte s'affiche dans la fenêtre de ligne de commande. Appuyez sur la barre espace pour afficher le segment de texte suivant. Ensuite, lorsque vous y êtes invité, saisissez l'une des valeurs suivantes :

   - Saisissez `y` si vous comprenez et acceptez les termes du CLUF.
   - Saisissez `n` si vous n'acceptez pas les conditions de la Politique de confidentialité. Pour utiliser l'Agent d'administration, vous devez accepter les conditions du Contrat de licence utilisateur final.
   - Saisissez `r` pour afficher de nouveau le CLUF.

4. Saisissez le nom DNS ou l'adresse IP du Serveur d'administration.
5. Entrez le numéro de port du Serveur d'administration. Le numéro de port est de 14000 par défaut.
6. Entrez le numéro de port SSL du Serveur d'administration. Le numéro de port est de 13000 par défaut.
7. Saisissez `y` si vous souhaitez utiliser le chiffrement SSL pour le trafic entre l'Agent d'administration et le Serveur d'administration. Dans le cas contraire, saisissez `n`.
8. Sélectionnez un des moyens suivants de configuration de l'Agent d'administration :

   - `[1]` : ne pas configurer de passerelle de connexion.

     Votre appareil agira en tant que passerelle de connexion et ne se connectera pas au Serveur d'administration par l'intermédiaire d'une passerelle de connexion.

   - `[2]` : ne pas utiliser de passerelle de connexion.

     Votre appareil ne se connectera pas au Serveur d'administration via une passerelle de connexion.

   - `[3]` : se connecter au Serveur via une passerelle de connexion.

     Votre appareil se connectera au Serveur d'administration via une passerelle de connexion.

   - `[4]` : utiliser comme passerelle de connexion.

     Votre appareil agira en tant que passerelle de connexion.

L'Agent d'administration est installé sur un appareil Linux.

Installation locale du plug-in d'administration des applications

Afin de lancer le plug-in d'administration des applications,

Lancez le fichier exécutable klcfginst.exe, repris dans le paquet de distribution de cette application, sur l'appareil où est installée la Console d'administration.

Le fichier klcfginst.exe fait partie de toutes les applications administrées par Kaspersky Security Center. L'installation se produit via l'Assistant et ne requiert aucune configuration manuelle des paramètres.

Installation des applications en mode silencieux

Afin d'effectuer l'installation de l'application en mode silencieux, procédez comme suit :

1. Ouvrez la fenêtre principale de Kaspersky Security Center.
2. Dans le dossier **Installation à distance** de l'arborescence de la console, dans le sous-dossier joint **Paquets d'installation**, sélectionnez le paquet d'installation de l'application concernée ou créez en un pour cette application.

   Le paquet d'installation sera enregistré sur le Serveur d'administration dans le dossier partagé dans le dossier de service Packages. Avec cela, le sous-dossier isolé correspond à chaque paquet d'installation.

3. Ouvrez le dossier du paquet d'installation nécessaire grâce à un des modes suivants :

   - Copiez le dossier correspondant au paquet d'installation requis depuis le Serveur d'administration vers l'appareil client. Ouvrez ensuite le dossier copié sur l'appareil client.
   - Depuis l'appareil client, ouvrez le dossier partagé qui correspond au paquet d'installation requis sur le Serveur d'administration.

   Si le dossier partagé se trouve sur un appareil doté du système d'exploitation Microsoft Windows Vista, il faut attribuer la valeur **Désactivé** au paramètre **Contrôle de compte d'utilisateur : tous les administrateurs fonctionnent en mode d'approbation par l'administration** (**Démarrer** → **Panneau de configuration** → **Administration** → **Stratégie locale de sécurité** → **Paramètres de sécurité**).

4. Selon l'application sélectionnée, procédez comme suit :

   - Pour Kaspersky Anti-Virus for Windows Workstations, Kaspersky Anti-Virus for Windows Servers et Kaspersky Security Center passez au sous-dossier exec et lancez le fichier exécutable (fichier avec extension .exe) avec la clé /s.
   - Pour autres applications de Kaspersky lancez du dossier ouvert le fichier exécutable (fichier avec extension .exe) avec la clé /s.

   Le lancement du fichier exécutable avec les arguments `EULA=1` et `PRIVACYPOLICY=1` signifie que vous avez entièrement lu, compris et accepté les conditions du Contrat de licence utilisateur final et de la Politique de confidentialité, respectivement. Vous êtes également conscient que vos données seront traitées et transmises (y compris à des pays tiers) comme décrit dans la Politique de confidentialité. Le texte du Contrat de licence utilisateur final et le texte de la Politique de confidentialité font partie de la distribution Kaspersky Security Center. L'acceptation des dispositions du Contrat de licence utilisateur final et la Politique de confidentialité est une condition indispensable pour installer l'application ou pour actualiser la version précédente de l'application.

Installation de l'application à l'aide des paquets autonomes

Kaspersky Security Center permet de former les paquets d'installation autonomes des applications. Le paquet d'installation autonome est un fichier exécutable qui peut être hébergé sur un Serveur Web, envoyé par courrier ou transmis via une autre méthode à l'appareil client. Le fichier reçu peut être lancé localement sur un appareil client afin d'installer l'application sans l'intervention de Kaspersky Security Center.

L'Agent d'administration autonome pour Linux dépend, en option, de l'utilitaire nmap. Si l'utilitaire nmap n'existe pas ou est antérieur à la version 6.0, la fonctionnalité Broadcast DHCP Discover n'est pas prise en charge.

Pour installer l'application à l'aide du paquet d'installation autonome, procédez comme suit :

1. Connectez-vous au Serveur d'administration nécessaire.
2. Dans l'arborescence de la console, dans le dossier **Installation à distance**, sélectionnez le sous-dossier **Paquets d'installation**.
3. Dans l'espace de travail, sélectionnez le paquet d'installation de l'application nécessaire.
4. Lancez le processus de création d'un paquet d'installation autonome par un des moyens suivants :
   - En sélectionnant l'option **&Créer un paquet d'installation autonome** dans le menu contextuel du paquet d'installation.
   - En cliquant sur le lien **Créer un paquet d'installation autonome** dans l'espace de travail du paquet d'installation.

   Finalement, l'Assistant de création du paquet d'installation autonome se lance. Suivez les instructions de l'assistant.

   A la dernière étape de l'Assistant, sélectionnez le mode de transmission du paquet d'installation autonome à l'appareil client.
5. Envoyez le paquet d'installation autonome de l'application à l'appareil client.
6. Lancez le paquet d'installation autonome sur l'appareil client.

L'application est alors installée sur l'appareil client selon les paramètres définis dans le paquet autonome.

Lors de la création, le paquet d'installation autonome est automatiquement publié sur le Serveur Web. Le lien pour télécharger le paquet autonome s'affiche dans la liste des paquets d'installation autonomes créés. En cas de nécessité, vous pouvez annuler la publication du paquet autonome sélectionné et le publier de nouveau sur le Serveur Web. Par défaut, le port 8060 est utilisé pour télécharger les paquets d'installation autonomes.

Paramètres du paquet d'installation de l'Agent d'administration

Pour configurer les paramètres du paquet d'installation de l'Agent d'administration, procédez comme suit :

1. Dans l'arborescence de la console, dans le dossier **Installation à distance**, sélectionnez le sous-dossier **Paquets d'installation**.

   Le dossier **Installation à distance** est un sous-dossier par défaut du dossier **Avancé**.
2. Dans le menu contextuel du paquet d'installation de l'Agent d'administration, sélectionnez l'option **Propriétés**.

La fenêtre des propriétés du paquet d'installation de l'Agent d'administration s'ouvre.

Général

La section **Général** affiche des informations générales sur le paquet d'installation :

- Nom du paquet d'installation
- Nom et version de l'application pour laquelle un paquet d'installation est créé
- Volume du paquet d'installation
- Date de création du paquet d'installation
- Chemin d'accès au dossier de placement du paquet d'installation

Paramètres

Cette section permet de configurer les paramètres nécessaires afin de garantir le fonctionnement de l'Agent d'administration tout de suite après son installation. Les paramètres de cette section sont disponibles uniquement sur les appareils qui tournent sous Windows.

Dans le groupe des paramètres **Dossier de destination**, vous pouvez sélectionner le dossier de l'appareil client où l'Agent d'administration sera installé.

- **Installer dans le dossier par défaut**

  Si cette option a été sélectionnée, l'Agent d'administration sera installé dans le dossier <Drive>:\Program Files\Kaspersky Lab\NetworkAgent. Si ce dossier n'existe pas, alors il sera créé automatiquement.

  Cette option est sélectionnée par défaut.

- **Installer dans un dossier défini**

  Si cette option a été sélectionnée, l'Agent d'administration sera installé dans le dossier indiqué dans le champ de saisie.

Le groupe des paramètres du bas permet de définir le mot de passe pour la tâche d'installation à distance de l'Agent d'administration.

- **Utiliser un mot de passe de désinstallation**

  Si cette option est activée, cliquez sur le bouton **Modifier** pour saisir le mot de passe de désinstallation de l'application (accessible uniquement pour l'Agent d'administration sur les appareils tournant sous des systèmes d'exploitation Windows).

  Cette option est Inactif par défaut.

- **État**

  État du mot de passe : **Mot de passe défini** ou **Mot de passe non défini**.

  Par défaut, le mot de passe n'est pas appliqué.

- **Protéger le service de l'Agent &d'administration contre la suppression ou l'arrêt non autorisé et empêcher la modification des paramètres**

  Lorsque cette option est activée, après l'installation de l'Agent d'administration sur un appareil administré, le module ne peut pas être supprimé ou reconfiguré sans les privilèges requis. Il est impossible d'arrêter le service de l'Agent d'administration. Cette option n'a aucun effet sur les contrôleurs de domaine.

  Activez cette option pour protéger l'Agent d'administration sur les postes de travail exploités avec des privilèges d'administrateur local.

  Cette option est Inactif par défaut.

- **Installer automatiquement les mises à jour et les correctifs nécessaires pour les modules dont l'état est Non défini**

  Si l'option est activée, les mises à jour et les correctifs pour le Serveur d'administration, l'Agent d'administration, la Console d'administration et le Serveur MDM iOS téléchargés sont installés automatiquement.

  Si l'option est désactivée, les mises à jour et les correctifs téléchargés sont installés uniquement après que l'administrateur a modifié leur état pour qu'il soit *Approuvé*. Les mises à jour et les correctifs avec l'état *Non défini* ne sont pas installés.

  Cette option est activée par défaut.

Connexion

Cette section permet de configurer les paramètres de connexion de l'Agent d'administration au Serveur d'administration. Pour établir une connexion, vous pouvez utiliser le protocole SSL ou UDP. Pour configurer la connexion, spécifiez les paramètres suivants :

- **Serveur d'administration**

  Adresse de l'appareil sur lequel est installé le Serveur d'administration.

- **Port**

  Numéro du port utilisé pour la connexion.

- **Port SSL**

  Numéro de port utilisé pour la connexion par protocole SSL.

- **Utiliser le certificat serveur**

  Si l'option est activée, l'authentification de l'accès de l'Agent d'administration au Serveur d'administration s'opère à l'aide d'un fichier du certificat que vous pouvez désigner en cliquant sur le bouton **Parcourir**.

  Si l'option est désactivée, le fichier du certificat est envoyé par le Serveur d'administration à la première connexion de l'Agent d'administration à l'adresse reprise dans le champ **Adresse du serveur**.

  Il est déconseillé de désactiver l'option, car la réception automatique du certificat du Serveur d'administration par l'Agent d'administration lors de la connexion au Serveur n'est pas sûre.

  Par défaut, la case est cochée.

- **Utiliser SSL**

  Si l'option est activée, la connexion au Serveur d'administration est établie via le port sécurisé à l'aide du protocole SSL.

  Cette option est Inactif par défaut. Nous vous recommandons de ne pas désactiver cette option afin que votre connexion reste sécurisée.

- **Utiliser un port UDP**

  Si l'option est activée, la connexion de l'Agent d'administration au Serveur d'administration est établie via le port UDP. Cela permet d'administrer les appareils clients et de recevoir des informations à leur sujet.

  Le port UDP doit être ouvert sur les appareils administrés sur lesquels l'Agent d'administration est installé. Par conséquent, nous vous recommandons de ne pas désactiver cette option.

  Cette option est activée par défaut.

- **Port UDP**

  Dans ce champ, vous pouvez spécifier le port pour connecter le Serveur d'administration à l'Agent d'administration en utilisant le protocole UDP.

  Le numéro de port UDP est de 15000 par défaut.

- **&Ouvrir les ports de l'Agent d'administration dans le pare-feu Microsoft Windows**

  Quand l'option est activée, les ports utilisés par l'Agent d'administration sont ajoutés à la liste des exclusions du Pare-feu Microsoft Windows.

  Cette option est activée par défaut.

- **Utiliser un serveur proxy**

  Si cette option est activée, définissez les paramètres du serveur proxy :

  - **Adresse du serveur proxy**
  - **Port du serveur proxy**

  Si votre serveur proxy requiert une authentification, activez l'option **Authentification du serveur proxy** et indiquez le **Nom d'utilisateur** et le **Mot de passe** du compte à partir duquel la connexion au serveur proxy est effectuée. Nous vous recommandons de spécifier les informations d'identification d'un compte disposant des privilèges minimaux requis uniquement pour l'authentification sur le serveur proxy.

Pour des raisons de compatibilité, il est déconseillé d'indiquer les paramètres de connexion par proxy dans les paramètres du paquet d'installation de l'Agent d'administration.

Avancé

Dans la section **Avancé**, vous pouvez configurer comment utiliser la passerelle de connexion. Pour ce faire, vous pouvez procéder comme suit :

- Utilisez l'Agent d'administration comme passerelle de connexion dans la zone démilitarisée (DMZ) pour vous connecter au Serveur d'administration, communiquer avec lui et conserver les données sur l'Agent d'administration en toute sécurité pendant la transmission des données.

- Connectez-vous au Serveur d'administration en utilisant une passerelle de connexion pour réduire le nombre de connexions au Serveur d'administration. Dans ce cas, entrez l'adresse de l'appareil qui servira de passerelle de connexion dans le champ **Adresse de la passerelle de connexion**.

- Configurez la connexion pour Virtual Desktop Infrastructure (VDI) si votre réseau comprend des machines virtuelles. Pour ce faire, vous pouvez procéder comme suit :

  - **Activer le mode dynamique pour VDI**

    Si cette option est activée, pour l'Agent d'administration installé sur la machine virtuelle, le mode dynamique pour Virtual Desktop Infrastructure (VDI) sera activé.

    Cette option est Inactif par défaut.

  - **Optimiser les paramètres pour VDI**

    Si cette option est activée, les fonctionnalités suivantes sont désactivées dans les paramètres de l'Agent d'administration :

    - Réception d'informations sur les logiciels installés
    - Réception d'informations sur la configuration matérielle
    - Réception d'informations sur la présence de vulnérabilités
    - Réception d'informations sur les mises à jour nécessaires

    Cette option est Inactif par défaut.

- **Autoriser l'exécution de l'utilitaire d'enregistrement des utilisateurs après l'installation de l'Agent d'administration**

  Si cette option est activée, l'enregistrement de l'utilisateur en tant que propriétaire de l'appareil sera lancé après l'installation de l'Agent d'administration. Cette option est Inactif par défaut.

Modules complémentaires

Cette section permet de sélectionner les modules complémentaires pour l'installation collective avec l'Agent d'administration.

Tags

La section **Tags** affiche la liste des mots clés (tags) qui peuvent être ajoutés aux appareils clients après l'installation de l'Agent d'administration. Vous pouvez ajouter des tags à la liste, en supprimer ou les renommer.

Si la case en regard d'un tag est cochée, ce tag sera ajouté automatiquement aux appareils administrés lors de l'installation de l'Agent d'administration sur ces derniers.

Si la case en regard d'un tag est décochée, ce tag ne sera pas ajouté automatiquement aux appareils administrés lors de l'installation de l'Agent d'administration sur ces derniers. Ce tag peut être ajouté manuellement aux appareils.

Quand un tag est supprimé de la liste, il est retiré automatiquement de tous les appareils auxquels il avait été ajouté.

Historique des révisions

Cette section vous permet de consulter l'historique des révisions du paquet d'installation. Vous pouvez comparer les révisions, consulter les révisions, enregistrer les révisions au fichier, ajouter et modifier des descriptions de révision.

Les paramètres de paquet d'installation de l'Agent d'administration disponibles pour un système d'exploitation particulier sont repris dans le tableau ci-dessous.

Paramètres du paquet d'installation de l'Agent d'administration

Section Propriété	Windows	Mac	Linux
Général	✓	✓	✓
Paramètres	✓	—	—
Connexion	✓	✓ (sauf pour les options **&Ouvrir les ports de l'Agent d'administration dans le pare-feu Microsoft Windows** et **Utiliser uniquement la définition automatique du serveur proxy**)	✓ (sauf pour les options **&Ouvrir les ports de l'Agent d'administration dans le pare-feu Microsoft Windows** et **Utiliser uniquement la détection automatique du serveur proxy**)
Avancé	✓	✓	✓
Modules complémentaires	✓	✓	✓
Tags	✓	✓ (sauf pour les règles d'attribution des tags automatique)	✓ (sauf pour les règles d'attribution des tags automatique)
Historique des révisions	✓	✓	✓

Consultation de la politique de confidentialité

La politique de confidentialité est accessible en ligne à l'adresse https://www.kaspersky.com/products-and-services-privacy-policy, mais également hors ligne. Vous pouvez lire la politique de confidentialité, par exemple, avant d'installer l'Agent d'administration.

Pour lire la politique de confidentialité hors ligne, procédez comme suit :

1. Démarrez le programme d'installation de Kaspersky Security Center.
2. Dans la fenêtre du programme d'installation, accédez au lien **Extraire les paquets d'installation**.
3. Dans la liste qui s'ouvre, sélectionnez Agent d'administration de Kaspersky Security Center, puis cliquez sur **Suivant**.

   Le fichier privacy_policy.txt s'affiche sur votre appareil, dans le dossier que vous avez défini, dans le sous-dossier NetAgent.

Déploiement des systèmes d'administration des appareils mobiles

Cette section décrit le déploiement des systèmes d'administration des appareils mobiles selon les protocoles MDM iOS et Kaspersky Endpoint Security.

Déploiement du système d'administration selon le protocole MDM iOS

Kaspersky Security Center permet d'administrer les appareils mobiles sous iOS. Les appareils MDM iOS sont les appareils iOS connectés au Serveur MDM iOS et administrés par un Serveur d'administration.

La connexion des appareils mobiles au Serveur MDM iOS est exécutée comme suit :

1. L'administrateur installe le Serveur MDM iOS.
2. L'administrateur reçoit le certificat du service Apple Push Notification Service (APNs) (Réception d'un certificat APNs, https://support.kaspersky.com/help/KSMM/4.1/en-US/64900.htm).

   Le certificat APNs permet au Serveur d'administration de se connecter au serveur APNs pour envoyer des notifications push vers les appareils MDM iOS.
3. L'administrateur installe le certificat APNs sur le Serveur MDM iOS.
4. L'administrateur établit le profil MDM iOS pour l'utilisateur de l'appareil mobile iOS.

   Le profil MDM iOS contient l'ensemble des paramètres de connexion des appareils mobiles iOS au Serveur d'administration.

Après l'installation du profil MDM iOS et après la synchronisation de l'appareil MDM iOS avec le Serveur d'administration, l'appareil est affiché dans le dossier **Appareils mobiles**, lui-même sous-dossier du dossier **Administration des appareils mobiles** de l'arborescence de la console.

Installer le Serveur MDM iOS

Pour installer le Serveur MDM iOS sur un appareil local, procédez comme suit :

1. Lancez le fichier exécutable setup.exe.

   La fenêtre de sélection des applications Kaspersky s'ouvre pour l'installation.

   Dans la fenêtre de sélection des applications, cliquez sur le lien **Installer le Serveur MDM iOS** pour lancer l'Assistant d'installation du Serveur MDM iOS.
2. Sélectionnez le dossier de destination.

   Le dossier de destination par défaut est <Disk>:\Program Files\Kaspersky Lab\Mobile Device Management for iOS. Si ce dossier n'existe pas, alors il sera créé automatiquement pendant l'installation. Vous pouvez modifier le dossier de destination à l'aide du bouton **Parcourir**.
3. Dans la fenêtre de l'Assistant **Définition des paramètres de connexion au Serveur MDM iOS** dans le champ **Port de connexion externe au service MDM iOS**, indiquez le port externe pour connecter les appareils mobiles au service MDM iOS.

   Le port externe 5223 est utilisé par les appareils mobiles pour communiquer avec le serveur APNs. Assurez-vous que le port 5223 est ouvert dans le pare-feu pour la connexion à la plage d'adresses 17.0.0.0/8.

   Le port 443 est utilisé par défaut pour la connexion de l'appareil au Serveur MDM iOS. Si le port 443 est déjà utilisé par un autre service ou une autre application, il est possible de le modifier (par exemple, avec le port 9443).

   Le serveur MDM iOS utilise le port externe 2197 pour envoyer des notifications au serveur APNs.

   Les serveurs APNs fonctionnent en mode de charge équilibrée. Les appareils mobiles ne se connectent pas toujours aux mêmes adresses IP pour la réception des notifications. La plage d'adresses 17.0.0.0/8 est attribuée par la société Apple. Il est donc conseillé d'autoriser l'ensemble de cette plage dans les paramètres du Pare-feu.

4. Si vous voulez configurer manuellement les ports d'interaction entre les modules de l'application, sélectionnez l'option **Configurer manuellement les ports locaux**, puis indiquez les valeurs des paramètres suivants :

   - **Port de connexion à l'Agent d'administration**. Indiquez dans le champ le port de connexion du service MDM iOS à l'Agent d'administration. Le numéro de port par défaut est 9799.
   - **Port de connexion local au service MDM iOS**. Indiquez dans le champ le port de connexion local de l'Agent d'administration au service MDM iOS. Le numéro de port par défaut est 9899.

   Il est conseillé d'utiliser les valeurs par défaut.

5. Dans la fenêtre **Adresse externe du Serveur des appareils mobiles** de l'Assistant, dans le champ **Adresse Internet de connexion à distance avec le Serveur des appareils mobiles**, indiquez l'adresse de l'appareil client sur lequel le serveur MDM iOS doit être installé.

   Cette adresse sera utilisée pour la connexion des appareils mobiles administrés au service MDM iOS. Les appareils MDM iOS doivent pouvoir se connecter à l'appareil client.

   Vous pouvez indiquer l'adresse de l'appareil client dans un des formats suivants :

   - Nom FQDN de l'appareil (par exemple, mdm.example.com)
   - Nom NetBIOS de l'appareil

   Il ne faut pas inclure le schéma URL et le numéro du port dans la ligne avec l'adresse : ces valeurs seront ajoutées automatiquement.

A l'issue du fonctionnement de l'Assistant, le serveur MDM iOS est installé sur l'appareil local. Le Serveur MDM iOS s'affichera dans le dossier **Administration des appareils mobiles** de l'arborescence de la console.

Installation du Serveur MDM iOS en mode silencieux

Kaspersky Security Center permet d'installer un serveur MDM iOS sur l'appareil local en mode silencieux, c'est-à-dire sans saisie interactive des paramètres d'installation.

Pour installer le serveur MDM iOS sur l'appareil local en mode silencieux :

1. Lisez le Contrat de licence utilisateur final. Utilisez la commande ci-dessous uniquement si vous comprenez et acceptez les conditions du Contrat de licence utilisateur final.

2. Exécutez la commande suivante :

   ```
   .\exec\setup.exe /s /v"DONT_USE_ANSWER_FILE=1 EULA=1 < setup_parameters >"
   ```

   où `setup_parameters` est une liste des paramètres et de leurs valeurs, séparés l'un de l'autre par un espace (`PROP1=PROP1VAL PROP2=PROP2VAL`). Le fichier setup.exe se trouve dans le dossier Server à l'intérieur de la distribution de Kaspersky Security Center.

Les noms et les valeurs possibles des paramètres qui peuvent être utilisés lors de l'installation du Serveur MDM iOS en mode silencieux sont cités dans le tableau ci-dessous. Les paramètre peuvent être définis dans n'importe quel ordre.

Paramètre d'installation du Serveur MDM iOS en mode silencieux

Nom du paramètre	Description du paramètre	Valeurs possibles
CLUF	Acceptation des conditions du Contrat de licence utilisateur final. Ce paramètre est obligatoire.	• 1 : j'ai entièrement lu, compris et accepté les conditions du Contrat de licence utilisateur final. • Une autre valeur ou non définie - Je refuse les conditions du Contrat de licence (l'installation n'aura pas lieu).
DONT_USE_ANSWER_FILE	Utiliser ou non le fichier xml contenant les paramètres d'installation du Serveur MDM iOS. Le fichier xml est compris dans le paquet d'installation ou se trouve sur le Serveur d'administration. Il n'est pas nécessaire d'indiquer en plus le chemin d'accès au fichier. Ce paramètre est obligatoire.	• 1 : ne pas utiliser le fichier xml contenant les paramètres d'. • Autre valeur ou non défini : utiliser le fichier xml contenant les paramètres d'.
INSTALLDIR	Dossier d'Installation du Serveur MDM iOS. Ce paramètre est facultatif.	Valeur de chaîne, par exemple, `INSTALLDIR=\"C:\install\"`.
CONNECTORPORT	Port local de connexion du service MDM iOS à l'Agent d'administration. Le numéro de port par défaut est 9799. Ce paramètre est facultatif.	Valeur numérique.
LOCALSERVERPORT	Port local de connexion de l'Agent d'administration au service MDM iOS. Le numéro de port par défaut est 9899. Ce paramètre est facultatif.	Valeur numérique.
EXTERNALSERVERPORT	Port pour la connexion de l'appareil au Serveur MDM iOS. Le numéro de port par défaut est 443. Ce paramètre est facultatif.	Valeur numérique.
EXTERNAL_SERVER_URL	Adresse externe de l'appareil client sur lequel le serveur MDM iOS est installé. Cette adresse sera utilisée pour la connexion des appareils mobiles administrés au service MDM iOS. L'appareil client doit accepter les connexions MDM iOS. L'adresse ne doit pas comporter de schéma URL ou de numéro de port : ces valeurs seront ajoutées automatiquement. Ce paramètre est facultatif.	• Nom FQDN de l'appareil (par exemple, mdm.example.com) • Nom NetBIOS de l'appareil • Adresse IP de l'appareil
WORKFOLDER	Dossier de travail du Serveur MDM iOS. Si aucun dossier de travail n'est défini, les données seront enregistrées dans le dossier par défaut. Ce paramètre est facultatif.	Valeur de chaîne, par exemple, `WORKFOLDER=\"C:\work\"`.
MTNCY	Utilisation du Serveur MDM iOS par plusieurs Serveurs virtuels. Ce paramètre est facultatif.	• 1 : le Serveur MDM iOS sera utilisé par plusieurs Serveurs d'administration virtuels. • Autre valeur ou non : le Serveur MDM iOS ne sera pas utilisé par plusieurs Serveurs d'administration virtuels.

Exemple :

```
\exec\setup.exe /s /v"EULA=1 DONT_USE_ANSWER_FILE=1 EXTERNALSERVERPORT=9443 EXTERNAL_SERVER_URL=\"www.test-mdm.com\""
```

Pour une description détaillée des paramètres d'installation du Serveur MDM iOS, reportez-vous à la section "Installation du Serveur MDM iOS".

Schémas du déploiement du Serveur MDM iOS

La quantité de copies installées du Serveur MDM iOS peut être choisie en fonction de la configuration matérielle disponible ou en fonction du nombre total d'appareils mobiles desservis.

Toutefois, il ne faut pas oublier qu'il est conseillé de se limiter à 50 000 appareils mobiles sur une installation de Kaspersky Device Management for iOS. En vue de réduire la charge, l'ensemble des appareils peut être répartis entre plusieurs serveurs dotés du Serveur MDM iOS.

L'authentification des appareils MDM iOS s'opère à l'aide des certificats des utilisateurs (le profil installé sur l'appareil contient le certificat du propriétaire de l'appareil). C'est pourquoi il existe deux schémas de déploiement du Serveur MDM iOS :

- Schéma simplifié
- Schéma de déploiement avec utilisation de la délégation forcée Kerberos (KCD)

Schéma de déploiement simplifié

Lors du déploiement du Serveur MDM iOS selon le schéma simplifié, les appareils mobiles sont connectés directement au service Internet MDM iOS. Et l'authentification des appareils s'opère uniquement sur la base des certificats utilisateurs émis par le Serveur d'administration. L'intégration à la Public Key Infrastructure (PKI) pour les certificats utilisateurs est impossible.

Schéma de déploiement avec utilisation de la délégation forcée Kerberos (KCD)

Pour utiliser le schéma de déploiement avec la délégation restreinte Kerberos (KCD), les conditions suivantes doivent être remplies :

- Le Serveur d'administration et le Serveur MDM iOS se trouvent sur le réseau interne de l'entreprise.
- Un proxy inversé avec prise en charge de KCD est utilisé.

Ce schéma de déploiement suppose :

- Intégration avec le proxy inversé qui prend en charge KCD
- Utilisation pour l'authentification des appareils mobiles de la délégation forcée Kerberos Constrained Delegation
- Intégration à l'infrastructure à clés publiques (PKI) pour l'utilisation des certificats utilisateurs

Lors de l'utilisation de ce schéma de déploiement, il faut tenir compte des points suivants :

- Dans la Console d'administration, cochez la case **Assurer la conformité avec Kerberos Constraint Delegation** dans les paramètres du service Internet MDM iOS.
- En guise de certificat du service Internet MDM iOS, il faut désigner le certificat spécial (personnalisé), défini sur le proxy inversé lors de la publication du service Internet MDM iOS.
- Les certificats utilisateurs pour les appareils iOS doivent être émis par l'Autorité de certification du domaine (ci-après, l'AC). S'il existe plusieurs AC racine dans le domaine, les certificats utilisateurs doivent être émis par l'AC indiquée lors de la publication du service Internet MDM iOS sur le proxy inversé.

  Il existe plusieurs moyens pour garantir la conformité du certificat utilisateur avec cette exigence :

  - Désigner le certificat utilisateur dans l'Assistant de création du profil MDM iOS et dans l'Assistant d'installation des certificats.
  - Intégrer le Serveur d'administration à la PKI du domaine et configurer le paramètre correspondant dans les règles d'émission des certificats :

    1. Dans l'arborescence de la console, développez le dossier **Administration des appareils mobiles** et sélectionnez le sous-dossier **Certificats**.
    2. Dans l'espace de travail du dossier **Certificats**, cliquez sur le bouton **Configurer les règles d'émission des certificats** pour ouvrir la fenêtre **Règles d'émission des certificats**.
    3. Configurez l'intégration à l'infrastructure à clé publique dans la section **Intégration avec PKI**.
    4. Dans la section **Émission des certificats de messagerie**, indiquez la source des certificats.

Voyons l'exemple de configuration de la délégation restreinte KCD avec les conditions suivantes :

- Le service Internet MDM iOS est lancé sur le port 443.
- Le nom de l'appareil doté du proxy inversé est firewall.mydom.local.
- Le nom de l'appareil avec le service Internet MDM iOS est iosmdm.mydom.local.
- Le nom de la publication extérieure du service Internet MDM iOS est iosmdm.mydom.global.

Service Principal Name pour http/iosmdm.mydom.local

Dans le domaine, il faut désigner Service Principal Name (SPN) pour l'appareil doté du service Internet MDM iOS (iosmdm.mydom.local) :

```
setspn -a http/iosmdm.mydom.local iosmdm
```

Configuration des propriétés du domaine de l'appareil doté du proxy inversé (firewall.mydom.local)

Pour déléguer le trafic, confier l'appareil avec le proxy inversé (firewall.mydom.local) au service défini selon SPN (http/iosmdm.mydom.local).

Pour confier l'appareil avec le proxy inversé au service défini selon SPN (http/iosmdm.mydom.local), l'administrateur doit exécuter les actions suivantes :

1. Dans le module logiciel enfichable de Microsoft Management Console "Active Directory Users and Computers", il faut choisir l'appareil doté du proxy inversé (firewall.mydom.local).

2. Dans les propriétés de l'appareil, sous l'onglet **Delegation**, choisir l'option **Use any authentication protocol** pour le commutateur **Trust this computer for delegation to specified service only**.

3. Dans la liste **Services to which this account can present delegated credentials** ajouter SPN http/iosmdm.mydom.local.

Certificat spécial (personnalisé) pour le service Internet publié (iosmdm.mydom.global)

Il faut émettre le certificat spécial (personnalisé) pour le service Internet MDM iOS sur le nom de domaine complet iosmdm.mydom.global et le désigner comme substitution du certificat par défaut dans les paramètres du service Internet MDM iOS dans la Console d'administration.

N'oubliez pas que le conteneur où se trouve le certificat (fichier avec extension p12 ou pfx) doit également contenir la chaîne de certificats racines (les parties publiques).

Publications du service Internet MDM iOS sur le proxy inversé

Sur le proxy inversé, pour le trafic allant du côté de l'appareil mobile sur le port 443 port iosmdm.mydom.global, il faut configurer KCD sur SPN http/iosmdm.mydom.local avec l'utilisation du certificat émis pour le nom de domaine complet iosmdm.mydom.global. N'oubliez pas qu'il faut prévoir le même certificat serveur pour les publications et pour le service Internet publié.

Réception du certificat APNs

> Si vous avez déjà un certificat APNs, veuillez considérer le renouveler au lieu d'en créer un nouveau. Lorsque vous remplacez le certificat APNs existant par un nouveau, le Serveur d'administration perd la capacité d'administrer les appareils mobiles iOS actuellement connectés.

Après la création d'une requête Certificate Signing Request (ci-après la requête CSR) à la première étape de l'Assistant de récupération du certificat APNs, la clé privée du certificat est enregistrée dans la mémoire RAM de l'appareil. C'est pourquoi toutes les étapes de l'Assistant doivent être terminées dans le cadre d'une session d'utilisation de l'application.

Pour obtenir le certificat APNs, procédez comme suit :

1. Dans le dossier **Administration des appareils mobiles**, sélectionnez le sous-dossier **Serveurs des appareils mobiles**.

2. Dans l'espace de travail du dossier **Serveurs des appareils mobiles**, sélectionnez le Serveur MDM iOS.

3. Dans le menu contextuel du Serveur MDM iOS, sélectionnez l'option **Propriétés**.

   La fenêtre des propriétés du Serveur MDM iOS s'ouvre.

4. Dans la fenêtre des propriétés du Serveur MDM iOS, sélectionnez la section **Certificats**.

5. Dans la section **Certificats**, dans le groupe de paramètres **Certificat Apple Push Notification**, cliquez sur le bouton **Obtenir un nouveau**.

   L'Assistant d'obtention du certificat APNs démarre et la fenêtre **Obtenir un nouveau** s'ouvre.

6. Créez une requête Certificate Signing Request (ci-après, CSR). Pour cela, exécutez les opérations suivantes :

   a. Cliquez sur **Créer CSR**.

   b. Dans la fenêtre ouverte **Création de CSR**, indiquez le nom de la demande, le nom de l'entreprise ou du département, la ville, la région et le pays.

   c. Cliquez sur le bouton **Enregistrer** et indiquez le nom du fichier à enregistrer la CSR.

   La clé privée du certificat à venir est enregistrée dans la mémoire de l'appareil.

7. Envoyez le fichier créé avec la CSR de signature à Kaspersky via votre CompanyAccount.

   > La signature de la CSR est accessible uniquement après le téléchargement sur le portail CompanyAccount de la clé qui autorise l'utilisation de la Administration des appareils mobiles.

   Après le traitement de votre demande électronique, vous recevrez le fichier de la demande CSR signé par Kaspersky.

8. Envoyez le fichier signé de la demande CSR sur le site Internet Apple Inc., en, utilisant un Apple ID aléatoire.

   > Il n'est pas recommandé d'utiliser l'Apple ID personnalisé. Créez un Apple ID séparé pour l'utiliser en tant que corporatif. Attachez l'Apple ID créé à la boîte aux lettres de la société et non pas à un employé séparé.

   Après le traitement de la CSR dans Apple Inc., vous recevrez la clé publique du certificat APNs. Enregistrez le fichier obtenu sur disque.

9. Exportez le certificat APNs avec une clé privée créée lors de la formation de la CSR dans un fichier au format PFX. Pour ce faire :

   a. Dans la fenêtre **Demande du nouveau certificat APNs**, cliquez sur le bouton **Quitter CSR**.

   b. Dans la fenêtre ouverte **Ouvrir**, sélectionnez le fichier avec la clé publique du certificat reçu après le traitement d'une CSR chez Apple Inc., puis cliquez sur le bouton **Ouvrir**.

      L'exportation du certificat est lancée.

   c. Dans la fenêtre ouverte, saisissez le mot de passe pour la clé privée, cliquez sur le bouton **OK**.

      Le mot de passe spécifié est utilisé pour installer le certificat APNs sur le serveur MDM iOS.

   d. Dans la fenêtre **Enregistrement du certificat APNs**, indiquez un nom de fichier de certificat APNs, sélectionnez un dossier, puis cliquez sur **Enregistrer**.

La partie privée et publique du certificat seront unies, le certificat APNs sera enregistré dans un fichier au format PFX. Ensuite, vous pouvez installer le certificat APNs reçu sur le Serveur MDM iOS.

Mise à jour du certificat APNs

Pour mettre à jour le certificat APNs, procédez comme suit :

1. Dans le dossier **Administration des appareils mobiles**, sélectionnez le sous-dossier **Serveurs des appareils mobiles**.
2. Dans l'espace de travail du dossier **Serveurs des appareils mobiles**, sélectionnez le Serveur MDM iOS.
3. Dans le menu contextuel du Serveur MDM iOS, sélectionnez l'option **Propriétés**.

   La fenêtre des propriétés du Serveur MDM iOS s'ouvre.
4. Dans la fenêtre des propriétés du Serveur MDM iOS, sélectionnez la section **Certificats**.
5. Dans la section **Certificats**, dans le groupe de paramètres **Certificat Apple Push Notification**, cliquez sur le bouton **Actualiser**.

   L'Assistant de la mise à jour du certificat APN se lance et la fenêtre certificat APNs **Mise à jour du certificat APNs** s'ouvre.
6. Créez une requête Certificate Signing Request (ci-après, CSR). Pour cela, exécutez les opérations suivantes :

   a. Cliquez sur **Créer CSR**.

   b. Dans la fenêtre ouverte **Création de CSR**, indiquez le nom de la demande, le nom de l'entreprise ou du département, la ville, la région et le pays.

   c. Cliquez sur le bouton **Enregistrer** et indiquez le nom du fichier à enregistrer la CSR.

   La clé privée du certificat à venir est enregistrée dans la mémoire de l'appareil.
7. Envoyez le fichier créé avec la CSR de signature à Kaspersky via votre CompanyAccount.

   > La signature de la CSR est accessible uniquement après le téléchargement sur le portail CompanyAccount de la clé qui autorise l'utilisation de la Administration des appareils mobiles.

   Après le traitement de votre demande électronique, vous recevrez le fichier de la demande CSR signé par Kaspersky.
8. Envoyez le fichier signé de la demande CSR sur le site Internet Apple Inc., en, utilisant un Apple ID aléatoire.

   > Il n'est pas recommandé d'utiliser l'Apple ID personnalisé. Créez un Apple ID séparé pour l'utiliser en tant que corporatif. Attachez l'Apple ID créé à la boîte aux lettres de la société et non pas à un employé séparé.

   Après le traitement de la CSR dans Apple Inc., vous recevrez la clé publique du certificat APNs. Enregistrez le fichier obtenu sur disque.

9. Demandez la clé publique du certificat. Pour cela, exécutez les opérations suivantes :

    a. Accédez au portail des certificats Apple Push. L'autorisation sur le portail nécessite Apple Id, reçu lors de la première demande de certificat.

    b. Dans la liste des certificats, choisissez le certificat, dont le nom APSP (nom au format « APSP:<number> ») correspond au nom APSP du certificat utilisé par le Serveur MDM iOS, et cliquez sur le bouton **Actualiser**.

    Le certificat APNs est actualisé.

    c. Enregistrez le certificat créé par le portail.

10. Exportez le certificat APNs avec une clé privée créée lors de la formation de la CSR dans un fichier au format PFX. Pour cela, exécutez les opérations suivantes :

    a. Dans la fenêtre **Mise à jour du certificat APNs**, cliquez sur le bouton **Quitter CSR**.

    b. Dans la fenêtre ouverte **Ouvrir**, sélectionnez le fichier avec la clé publique du certificat reçu après le traitement d'une CSR chez Apple Inc., et cliquez sur le bouton **Ouvrir**.

    L'exportation du certificat sera lancée.

    c. Dans la fenêtre ouverte, saisissez le mot de passe pour la clé privée, cliquez sur le bouton **OK**.

    Le mot de passe spécifié est utilisé pour installer le certificat APNs sur le serveur MDM iOS.

    d. Dans la fenêtre **Mise à jour du certificat APNs** qui s'ouvre, indiquez un nom de fichier pour le certificat APNs, sélectionnez le dossier à enregistrer ce fichier et cliquez sur **Enregistrer**.

La partie privée et publique du certificat seront unies, le certificat APNs sera enregistré dans un fichier au format PFX.

Configurer un certificat de Serveur MDM iOS de réserve

La fonctionnalité du serveur MDM iOS vous permet d'émettre un certificat de réserve. Ce certificat est destiné à être utilisé dans les profils MDM iOS, afin de garantir une commutation transparente des appareils iOS administrés après l'expiration du certificat du serveur MDM iOS.

Si votre serveur MDM iOS utilise un certificat par défaut émis par Kaspersky, vous pouvez émettre un certificat de réserve (ou spécifier votre propre certificat personnalisé comme réserve) avant l'expiration du certificat du serveur MDM iOS. Par défaut, le certificat de réserve est automatiquement émis 60 jours avant l'expiration du certificat du serveur MDM iOS. Le certificat de réserve du serveur MDM iOS devient le certificat principal immédiatement après l'expiration du certificat du serveur MDM iOS. La clé publique est distribuée à tous les appareils administrés via des profils de configuration, vous n'avez donc pas à la transmettre manuellement.

Pour émettre un certificat de Serveur MDM iOS de réserve ou spécifier un certificat de réserve personnalisé :

1. Dans l'arborescence de la console, dans le dossier **Administration des appareils mobiles**, sélectionnez le sous-dossier **Serveurs des appareils mobiles**.

2. Dans la liste des serveurs d'appareils mobiles, sélectionnez le serveur MDM iOS approprié, et dans le volet droit, cliquez sur le bouton **Configurer les paramètres du serveur MDM iOS**.

3. Dans la fenêtre de paramètres du Serveur MDM iOS qui s'ouvre, sélectionnez la section **Certificats**.

4. Dans le bloc de paramètres **Certificat de réserve**, effectuez une des opérations suivantes :

   - Si vous prévoyez de continuer à utiliser un certificat auto-signé (c'est-à-dire celui émis par Kaspersky) :

     a. Cliquez sur le bouton **Problème**.

     b. Dans la fenêtre **Date d'activation** qui s'ouvre, sélectionnez l'une des deux options pour la date à laquelle le certificat de réserve doit être appliqué :

        - Si vous souhaitez appliquer le certificat de réserve au moment de l'expiration du certificat actuel, sélectionnez l'option **Lorsque le certificat actuel expire**.

        - Si vous souhaitez appliquer le certificat de réserve avant l'expiration du certificat actuel, sélectionnez l'option **Après une période déterminée (jours)**. Dans le champ de saisie à côté de cette option, spécifiez la durée de la période après laquelle le certificat de réserve doit remplacer le certificat actuel.

        La période de validité du certificat de réserve que vous spécifiez ne peut pas dépasser la durée de validité du certificat du serveur MDM iOS actuel.

     c. Cliquez sur le bouton **OK**.

     Le certificat de Serveur MDM iOS de réserve est émis.

   - Si vous prévoyez d'utiliser un certificat personnalisé émis par votre autorité de certification :

     a. Cliquez sur le bouton **Ajouter**.

     b. Dans la fenêtre Explorateur de fichier Windows qui s'ouvre, spécifiez un fichier de certificat au format PEM, PFX ou P12, qui est stocké sur votre appareil, puis cliquez sur le bouton **Ouvrir**.

     Votre certificat personnalisé est spécifié comme certificat de Serveur MDM iOS de réserve

Vous avez spécifié un certificat de Serveur MDM iOS de réserve. Les détails du certificat de réserve sont affichés dans le bloc de paramètres **Certificat de réserve** (nom du certificat, nom de l'émetteur, date d'expiration et date à laquelle le certificat de réserve doit être appliqué, le cas échéant).

Installation du certificat APNs sur le Serveur MDM iOS

Après l'obtention du certificat APNs, il faut installer le certificat APNs reçu sur le Serveur MDM iOS.

Pour installer le certificat APNs sur le Serveur MDM iOS, procédez comme suit :

1. Dans le dossier **Administration des appareils mobiles**, sélectionnez le sous-dossier **Serveurs des appareils mobiles**.

2. Dans l'espace de travail du dossier **Serveurs des appareils mobiles**, sélectionnez le Serveur MDM iOS.

3. Dans le menu contextuel du Serveur MDM iOS, sélectionnez l'option **Propriétés**.

   La fenêtre des propriétés du Serveur MDM iOS s'ouvre.

4. Dans la fenêtre des propriétés du Serveur MDM iOS, sélectionnez la section **Certificats**.

5. Dans la section **Certificats**, dans le groupe de paramètres **Certificat Apple Push Notification**, cliquez sur le bouton **Installer**.

6. Sélectionnez le fichier au format PFX contenant le certificat APNs.

7. Saisissez le mot de passe de la clé privée renseigné lors de l'exportation du certificat APNs.

Finalement, le certificat APNs sera installé sur le Serveur MDM iOS. Les informations sur le certificat seront affichées dans la fenêtre des propriétés du Serveur MDM iOS dans la section **Certificats**.

Configuration de l'accès au service Apple Push Notification

Pour garantir le bon fonctionnement du service Internet MDM iOS ainsi que la réaction opportune des appareils mobiles aux commandes de l'administrateur, il faut définir le certificat Apple Push Notification Service (ci-après le certificat APNs) dans les paramètres du serveur MDM iOS.

Dans le cadre de la coopération avec le service Apple Push Notification (ci-après APNs), le service Internet MDM iOS se connecte à l'adresse externe api.push.apple.com selon le port 2197 (sortant). C'est pourquoi le service Internet MDM iOS doit avoir accès au port TCP 2197 pour la plage d'adresses 17.0.0.0/8. Du côté des appareils iOS, l'accès au port TCP 5223 pour la plage d'adresses 17.0.0.0/8.

S'il est prévu d'octroyer l'accès à APNs du côté du service Internet MDM iOS via un serveur proxy, il convient d'exécuter les actions suivantes sur l'appareil doté du service Internet MDM iOS :

1. Écrire les lignes suivantes dans le registre :

   - Pour les systèmes d'exploitation 32 bits :

```
HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\Connectors\KLIOSMDM\1.0.0.0\Conset
"ApnProxyHost"="<Proxy Host Name>"
"ApnProxyPort"="<Proxy Port>"
"ApnProxyLogin"="<Proxy Login>"
"ApnProxyPwd"="<Proxy Password>"
```

   - Pour les systèmes d'exploitation de 64 bits :

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\Connectors\KLIOSMDM\1.0.0.0\Conset
"ApnProxyHost"="<Proxy Host Name>"
"ApnProxyPort"="<Proxy Port>"
"ApnProxyLogin"="<Proxy Login>"
"ApnProxyPwd"="<Proxy Password>"
```

2. Relancer le service Internet MDM iOS.

Émission et installation d'un certificat général sur l'appareil mobile

Pour émettre un certificat général à l'attention de l'utilisateur et l'installer, procédez comme suit :

1. Sélectionnez un compte utilisateur dans le dossier **Comptes utilisateurs** de l'arborescence de la console.
2. Dans le menu contextuel du compte utilisateur, sélectionnez l'option **Installer le certificat**.

   L'Assistant d'installation des certificats démarre. Suivez les instructions de l'assistant.

A la fin de l'exécution de l'Assistant, le certificat sera créé et ajouté à la liste des certificats de l'utilisateur.

L'utilisateur télécharge le certificat émis en même temps que le paquet d'installation comportant le profil MDM iOS.

Après la connexion de l'appareil mobile au Serveur MDM iOS, les paramètres du profil MDM iOS seront appliqués sur l'appareil de l'utilisateur. L'administrateur pourra administrer l'appareil connecté.

L'appareil mobile de l'utilisateur connecté au Serveur MDM iOS s'affichera dans le sous-dossier **Appareils mobiles** du dossier **Administration des appareils mobiles** de l'arborescence de la console.

Ajout d'un appareil KES à la liste des appareils administrés

Pour ajouter l'appareil KES d'un utilisateur à la liste des appareils administrés à l'aide du lien vers Google Play™, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le dossier **Comptes utilisateurs**.

   Par défaut, le dossier **Comptes utilisateurs** est placé dans un sous-dossier du dossier **Avancé**.
2. Sélectionnez le compte utilisateur, et l'appareil mobile que vous souhaitez ajouter à la liste des appareils administrés.
3. Dans le menu contextuel du compte utilisateur, sélectionnez l'option **Ajouter un appareil mobile**.

   L'Assistant de connexion d'un nouvel appareil mobile démarre. Dans la fenêtre de l'Assistant **Source du certificat**, il faut indiquer le mode de création du certificat commun à l'aide duquel le Serveur d'administration identifie un appareil mobile. Il existe deux manières de fournir un certificat commun :

   - Créer automatiquement un certificat commun à l'aide du Serveur d'administration et l'ajouter à l'appareil.
   - Indiquer le fichier du certificat commun.
4. Dans la fenêtre **Type d'appareil** de l'Assistant, sélectionnez l'option **Lien vers Google Play**.
5. Dans la fenêtre **Mode de notification des utilisateurs** de l'Assistant, configurez les paramètres de notification de l'utilisateur d'un appareil mobile à propos de la création du certificat (par message SMS, par email ou via l'affichage des informations au terme de l'exécution de l'Assistant).
6. Dans la fenêtre Informations relatives au certificat de l'Assistant, cliquez sur le bouton **Terminer** pour fermer l'Assistant.

Suite à l'exécution de l'Assistant sur l'appareil de l'utilisateur, un lien et un code QR seront envoyés pour télécharger Kaspersky Endpoint Security depuis Google Play. L'utilisateur peut accéder à la boutique d'applications Google Play en suivant le lien ou en lisant le code QR. Ensuite, le système d'exploitation de l'appareil demande à l'utilisateur son accord pour l'installation de Kaspersky Endpoint Security for Android. Après le téléchargement et l'installation de Kaspersky Endpoint Security for Android, l'appareil mobile se connecte au Serveur d'administration et télécharge le certificat commun. Après l'installation du certificat sur l'appareil mobile, celui-ci apparaît dans le sous-dossier **Appareils mobiles** du dossier **Administration des appareils mobiles** de l'arborescence de la console.

Si l'application Kaspersky Endpoint Security for Android est déjà installée sur l'appareil, l'utilisateur doit saisir lui-même les paramètres de connexion au Serveur d'administration après les avoir obtenus auprès de l'administrateur. Une fois la configuration des paramètres de connexion effectuée, l'appareil mobile se connecte au Serveur d'administration. L'administrateur émet un certificat général pour l'appareil et envoie à l'utilisateur un message électronique ou un SMS contenant le nom d'utilisateur et le mot de passe de téléchargement du certificat. L'utilisateur télécharge et installe le certificat commun. Après l'installation du certificat sur l'appareil mobile, celui-ci apparaît dans le sous-dossier **Appareils mobiles** du dossier **Administration des appareils mobiles** de l'arborescence de la console. Dans ce cas, Kaspersky Endpoint Security for Android n'est ni téléchargé à nouveau, ni installé.

Connexion des appareils KES au Serveur d'administration

En fonction du mode de connexion des appareils au Serveur d'administration, il existe deux schémas de déploiement de Kaspersky Device Management for iOS pour les appareils KES :

- schéma de déploiement avec utilisation de la connexion directe des appareils au Serveur d'administration
- Schéma de déploiement impliquant un proxy inversé qui prend en charge la délégation restreinte Kerberos

Connexion directe des appareils au Serveur d'administration

Les appareils KES peuvent se connecter directement au port 13292 du Serveur d'administration.

En fonction du mode d'authentification, il existe deux options de connexion des appareils KES au Serveur d'administration :

- Connexion des appareils avec utilisation du certificat utilisateur
- Connexion des appareils sans certificat utilisateur

Connexion d'un appareil avec utilisation du certificat utilisateur

Lors de la connexion de l'appareil avec un certificat utilisateur, cet appareil est associé au compte utilisateur auquel les outils du Serveur d'administration ont attribué le certificat correspondant.

Dans ce cas, c'est l'authentification bilatérale SSL (authentification mutuelle) qui est utilisée. Aussi bien le Serveur d'administration que l'appareil sont authentifiés à l'aide de certificats.

Connexion d'un appareil sans certificat utilisateur

Lors de la connexion d'un appareil sans certificat utilisateur, l'appareil n'est associé à aucun compte utilisateur sur le Serveur d'administration. Mais dès que l'appareil reçoit un certificat quelconque, cet appareil est associé à l'utilisateur auquel les outils du Serveur d'administration ont attribué le certificat correspondant.

Lors de la connexion de l'appareil au Serveur d'administration, l'authentification utilisée est l'authentification unilatérale SSL (one-way SSL authentication) dans le cadre de laquelle seul le Serveur d'administration est authentifié à l'aide du certificat. Après l'appareil a reçu un certificat utilisateur, le type d'authentification devient l'authentification bilatérale SSL (2-way SSL authentication, mutual authentication).

Schéma de la connexion des appareils KES au serveur avec utilisation de la délégation forcée Kerberos (KCD)

Le schéma de connexion des appareils KES au Serveur d'administration avec utilisation de Kerberos Constrained Delegation (KCD) suppose :

- Intégration avec un proxy inversé qui prend en charge KCD.
- L'utilisation de la délégation forcée Kerberos Constrained Delegation (ci-après KCD) pour l'authentification des appareils mobiles.
- L'intégration à l'infrastructure à clés publiques (Public Key Infrastructure, ci-après) pour l'utilisation des certificats utilisateurs.

Lors de l'utilisation de ce schéma de connexion, il faut tenir compte des points suivants :

- Le type de connexion des appareils KES au proxy inversé doit être une authentification bilatérale SSL (« two-way SSL authentication »), à savoir que l'appareil doit se connecter au proxy inversé selon son certificat utilisateur. Pour cela, il faut intégrer le certificat utilisateur au paquet d'installation de Kaspersky Endpoint Security for Android installé sur l'appareil. Ce paquet KES doit être créé par le Serveur d'administration spécialement pour cet appareil (utilisateur).

- Au lieu du certificat de serveur, il faut indiquer par défaut pour le protocole mobile un certificat spécial (personnalisé) :

  1. Dans la section **Paramètres** de la fenêtre des propriétés du Serveur d'administration, cocher la case **Ouvrir le port pour les appareils mobiles**, puis choisir **Ajouter un certificat** dans la liste déroulante.

  2. Dans la fenêtre qui s'ouvre, indiquer le même certificat que celui désigné sur le proxy inversé lors de la publication du point d'accès au protocole mobile sur le Serveur d'administration.

- Les certificats utilisateurs pour les appareils KES doivent être émis par l'Autorité de certification du domaine (AC). De plus, il ne faut pas oublier que si le domaine compte plusieurs AC racine, les certificats utilisateurs doivent être émis par l'AC indiqué dans la publication sur le proxy inversé.

  Il existe plusieurs moyens pour garantir la conformité du certificat utilisateur avec l'exigence présentée ci-dessus :

  - Désigner le certificat utilisateur spécial dans l'Assistant de création du paquet d'installation et dans l'Assistant d'installation des certificats.

  - Intégrer le Serveur d'administration à la PKI du domaine et configurer le paramètre correspondant dans les règles d'émission des certificats :

    1. Dans l'arborescence de la console, développez le dossier **Administration des appareils mobiles** et sélectionnez le sous-dossier **Certificats**.

    2. Dans l'espace de travail du dossier **Certificats**, cliquez sur le bouton **Configurer les règles d'émission des certificats** pour ouvrir la fenêtre **Règles d'émission des certificats**.

    3. Configurez l'intégration à l'infrastructure à clé publique dans la section **Intégration avec PKI**.

    4. Dans la section **Émission des certificats de messagerie**, indiquez la source des certificats.

Voyons l'exemple de configuration de la délégation restreinte KCD avec les conditions suivantes :

- Le point d'accès au protocole mobile sur le Serveur d'administration est offert sur le port 13292.

- Le nom de l'appareil doté du proxy inversé est firewall.mydom.local.

- Le nom de l'appareil avec le Serveur d'administration est ksc.mydom.local.

- Le nom de la publication externe du point d'accès au protocole mobile est kes4mob.mydom.global.

Compte utilisateur de domaine pour le Serveur d'administration

Il faut créer un compte utilisateur de domaine (par exemple, KSCMobileSrvcUsr) sous lequel le service du Serveur d'administration va fonctionner. Il est possible d'indiquer le compte utilisateur du service du Serveur d'administration lors de l'installation du Serveur d'administration ou à l'aide de l'utilitaire klsrvswch. L'utilitaire klsrvswch se trouve dans le dossier d'installation du Serveur d'administration. Chemin d'installation par défaut : <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

Il faut désigner le compte utilisateur de domaine pour les raisons suivantes :

- La fonction d'administration des appareils KES est une partie intégrante du Serveur d'administration.
- Pour garantir le bon fonctionnement de la délégation forcée (KCD), la partie réceptrice, qui est le Serveur d'administration, doit fonctionner sous un compte utilisateur de domaine.

Service Principal Name pour http/kes4mob.mydom.local

Dans le domaine, il faut prescrire sous le compte utilisateur KSCMobileSrvcUsr Service Principal Name (SPN) pour la publication du service du protocole mobile sur le port 13292 de l'appareil avec le Serveur d'administration. Pour l'appareil kes4mob.mydom.local avec le Serveur d'administration, cela ressemble à ceci :

```
setspn -a http/kes4mob.mydom.local:13292 mydom\KSCMobileSrvcUsr
```

Configuration des propriétés du domaine de l'appareil doté du proxy inversé (firewall.mydom.local)

Pour déléguer le trafic, il faut confier l'appareil avec le proxy inversé (firewall.mydom.local) au service défini selon SPN (http/kes4mob.mydom.local:13292).

Pour confier l'appareil avec le proxy inversé au service défini selon SPN (http/kes4mob.mydom.local:13292), l'administrateur doit exécuter les actions suivantes :

1. Dans le module logiciel enfichable de Microsoft Management Console "Active Directory Users and Computers", il faut choisir l'appareil doté du proxy inversé (firewall.mydom.local).
2. Dans les propriétés de l'appareil, sous l'onglet **Delegation**, choisir l'option **Use any authentication protocol** pour le commutateur **Trust this computer for delegation to specified service only**.
3. Dans la liste **Services to which this account can present delegated credentials** ajouter SPN http/kes4mob.mydom.local:13292.

Certificat spécial (personnalisé) pour la publication (kes4mob.mydom.global)

Pour la publication du protocole mobile du Serveur d'administration il faut octroyer un certificat spécial (personnalisé) au nom de domaine complet kes4mob.mydom.global et le désigner en substitution au certificat serveur par défaut dans les paramètres du protocole mobile du Serveur d'administration dans la Console d'administration. Pour cela, dans la section **Paramètres** de la fenêtre des propriétés du Serveur d'administration, il faut cocher la case **Ouvrir le port pour les appareils mobiles**, puis choisir **Ajouter un certificat** dans la liste déroulante.

N'oubliez pas que le conteneur où se trouve le certificat serveur (fichier avec extension p12 ou pfx) doit également contenir la chaîne de certificats racines (les parties publiques).

Configuration de la publication sur le pare-feu d'entreprise

Sur le proxy inversé, pour le trafic allant du côté de l'appareil mobile sur le port 13292 port kes4mob.mydom.global, il faut configurer KCD sur SPN kes4mob.mydom.global:13292 avec l'utilisation du certificat serveur émis pour le nom de domaine complet kes4mob.mydom.global. N'oubliez pas qu'il faut prévoir le même certificat serveur pour les publications et pour le point d'accès publié (port 13292 du Serveur d'administration).

Utilisation de Firebase Cloud Messaging

Pour une livraison opportune des commandes sur les appareils KES sous le système d'exploitation Android, le mécanisme des notifications push est utilisé dans Kaspersky Security Center. Les notifications push entre les appareils KES et le Serveur d'Administration sont échangées à l'aide de Firebase Cloud Messaging (ci-après dénommé FCM). La Console d'administration de Kaspersky Security Center permet d'indiquer les paramètres du service Firebase Cloud Messaging pour connecter les appareils KES à ce service.

Pour obtenir les paramètres de Firebase Cloud Messaging, vous devez avoir un compte utilisateur Google.

Pour activer FCM, procédez comme suit :

1. Dans la Console d'administration, sélectionnez l'entrée **Administration des appareils mobiles**, puis le dossier **Appareils mobiles**.
2. Dans le menu contextuel du dossier **Appareils mobiles**, sélectionnez l'option **Propriétés**.
3. Dans les propriétés du dossier, sélectionnez la section **Paramètres de Firebase Cloud Messaging**.
4. Dans le champ **Numéro de projet Firebase**, indiquez l'identificateur de l'expéditeur de FCM.
5. Dans le champ **Fichier clé privé (au format JSON)**, sélectionnez le fichier de clé privée.

   Lors de la synchronisation suivantes avec le Serveur d'administration, les appareils administrés KES sous le système d'exploitation Android seront connectés au service Firebase Cloud Messaging.

Vous pouvez modifier les paramètres de Firebase Cloud Messaging à l'aide du bouton **Abandonner les paramètres**.

Lorsque vous passez à un autre projet Firebase, vous devez attendre 10 minutes que FCM reprenne.

Le service FCM fonctionne sur les plages d'adresses suivantes :

- Du côté de l'appareil KES, il faut octroyer l'accès aux ports 443 (HTTPS), 5228 (HTTPS), 5229 (HTTPS), 5230 (HTTPS) des adresses suivantes :
  - google.com
  - fcm.googleapis.com
  - android.apis.google.com
  - ou sur toutes les adresses IP de la liste " Google ASN 15169 "
- Du côté du Serveur d'administration, il faut octroyer l'accès sur le port 443 (HTTPS) des adresses suivantes :
  - fcm.googleapis.com
  - ou sur toutes les adresses IP de la liste « Google ASN 15169 »

Si les paramètres du serveur proxy ont été définis dans les propriétés du Serveur d'administration de la Console d'administration (**Avancé** / **Paramètres d'accès au réseau Internet**), ils seront utilisés pour coopérer avec FCM.

Configuration de FCM : obtention de l'identificateur de l'expéditeur et du fichier de clé privée

Pour configurer FCM, procédez comme suit :

1. S'inscrire sur le portail Google.
2. Accéder à la console Firebase.
3. Exécutez une des actions suivantes :
   - Pour créer un projet, cliquez sur **Créer un projet** et suivez les instructions à l'écran.
   - Ouvrez un projet existant.
4. Cliquez sur l'icône en forme d'engrenage et choisissez **Paramètres du projet**.

   La fenêtre **Paramètres du projet** s'ouvre.
5. Sélectionnez l'onglet **Messagerie Cloud**.
6. Récupérez l'identificateur de l'expéditeur dans le champ **Identificateur de l'expéditeur** dans la section **API de Firebase Cloud Messaging (V1)**.
7. Sélectionnez l'onglet **Comptes de services** et cliquez sur **Générer une nouvelle clé privée**.
8. Dans la fenêtre qui s'ouvre, cliquez sur **Générer une clé** pour générer et télécharger un fichier de clé privée.

Firebase Cloud Messaging est maintenant configuré.

Intégration avec l'infrastructure à clé publique

L'intégration à l'infrastructure à clés publiques (Public Key Infrastructure, ensuite PKI) sert avant tout à simplifier l'émission des certificats utilisateurs de domaine par le Serveur d'administration.

L'administrateur peut attribuer à l'utilisateur un certificat de domaine dans la Console d'administration. Pour cela, il a le choix entre les méthodes suivantes :

- Attribuer à l'utilisateur un certificat spécial (personnalisé) depuis un fichier dans l'Assistant d'installation des certificats.
- Exécuter l'intégration avec PKI et désigner la PKI comme source du certificat pour le type concret de certificat ou pour tous les types de certificat.

Les paramètres d'intégration avec PKI sont accessibles dans l'espace de travail du dossier **Administration des appareils mobiles** / **Certificats** via le lien **Intégrer à l'infrastructure de clés ouvertes**.

Principe général de l'intégration avec PKI pour l'émission des certificats de domaine des utilisateurs

Dans la Console d'administration, cliquez sur le lien **Intégrer à l'infrastructure de clés ouvertes** de l'espace de travail du dossier **Administration des appareils mobiles** / **Certificats** pour désigner le compte de domaine que le Serveur d'administration va utiliser pour émettre les certificats utilisateurs de domaine via l'AC de domaine (ci-après, le compte utilisateur sous lequel l'intégration avec PKI a lieu).

Il faut tenir compte des points suivants :

- Dans les paramètres de l'intégration avec PKI, il est possible de désigner une modèle par défaut pour tous les types de certificat. Sachez que les règles d'émission des certificats (disponibles dans l'espace de travail du dossier **Administration des appareils mobiles** / **Certificats** en cliquant sur le bouton **Configurer les règles d'émission des certificats**) permettent de définir un modèle pour chaque type de certificat séparément.
- Sur l'appareil doté du Serveur d'administration, le certificat spécial Enrollment Agent (EA) doit être installé dans le stockage des certificats du compte utilisateur sous lequel l'intégration avec PKI a lieu. Le certificat Enrollment Agent (EA) est émis par l'administrateur de l'AC (autorité de certification) de domaine.

Le compte utilisateur sous lequel l'intégration avec PKI a lieu doit répondre aux critères suivants :

- Est l'utilisateur de domaine.
- Est l'administrateur local de l'appareil doté du Serveur d'administration depuis lequel l'intégration avec PKI a lieu.
- Possède le droit *Connexion en tant que service*.
- Pour créer le profil permanent de l'utilisateur, il faut lancer au moins une fois sous ce compte utilisateur l'appareil doté du Serveur d'administration.

Serveur Web de Kaspersky Security Center

Le Serveur Web de Kaspersky Security Center (si après le Serveur Web) est un module de Kaspersky Security Center. Le Serveur Web intervient dans la publication des paquets d'installation autonomes, des paquets d'installation autonomes pour les appareils mobiles, des profils MDM iOS, ainsi que des fichiers du dossier partagé.

Les profils MDM iOS et les paquets d'installation créés sont publiés automatiquement sur le serveur Web et sont supprimés après le premier chargement. L'administrateur peut transférer à l'utilisateur le lien formé à l'aide d'un moyen commode quelconque, par exemple, via email.

A l'aide du lien reçu, l'utilisateur peut télécharger les informations sur l'appareil mobile.

Paramètres du Serveur Web

Pour permettre la configuration fine du Serveur Web, les propriétés du Serveur Web de la Console d'administration prévoient la possibilité de remplacer les ports pour les protocoles HTTP (8060) et HTTPS (8061). De plus, outre la substitution des ports, il est possible de substituer le certificat serveur pour le protocole HTTPS et de remplace le nom de domaine complet du Serveur Web pour le protocole HTTP.

Installation de Kaspersky Security Center

La procédure d'installation des modules de Kaspersky Security Center. Si vous souhaitez installer l'application localement sur un seul appareil, deux options d'installation sont disponibles :

- **Standard**. Cette option est recommandée si vous voulez découvrir l'application Kaspersky Security Center, par exemple, tester son fonctionnement sur un petit segment de votre réseau. Dans le cadre de l'installation standard, vous configurez uniquement les paramètres de la base de données. Vous pouvez également installer uniquement l'ensemble par défaut de plug-ins d'administration des applications de Kaspersky. Vous pouvez aussi vous servir de l'installation standard si vous avez déjà l'habitude d'utiliser Kaspersky Security Center et pouvez spécifier tous les paramètres nécessaires après l'installation standard.

- **Personnalisée**. Cette option est recommandée si vous envisagez de modifier les paramètres de Kaspersky Security Center, comme un chemin vers le dossier en accès public, les comptes utilisateurs et les ports de connexion au Serveur d'administration, ainsi que les paramètres de la base de données. L'installation personnalisée vous permet de désigner les plug-ins d'administration des applications de Kaspersky à installer. En cas de nécessité, vous pouvez lancer l'installation personnalisée en mode silencieux.

Si au moins un Serveur d'administration est installé dans le réseau, les Serveurs sur les autres appareils du réseau peuvent être installés à l'aide d'une tâche d'installation à distance selon la méthode de l'installation forcée. Lors de la création de la tâche d'installation à distance, vous devez utiliser le paquet d'installation du Serveur d'administration : ksc_<numéro_version>.<numéro de version>_full_<langue de localisation>.exe.

Choisissez ce paquet si vous voulez installer tous les composants nécessaires au fonctionnement complet de Kaspersky Security Center ou mettre à jour les versions existantes de ces composants.

Si vous souhaitez déployer le cluster de basculement Kaspersky Security Center, vous devez installer Kaspersky Security Center sur tous les nœuds du cluster.

Préparation de l'installation

Avant de lancer l'installation, vous devez réaliser les actions suivantes.

- **Vérifier la configuration matérielle et logicielle requise**

  Confirmez que l'appareil répond aux exigences de configuration matérielle et logicielle applicables au Serveur d'administration et à la Console d'administration.

- **Sélectionnez et installez le système de gestion de base de données (SGBD)**

  Kaspersky Security Center stocke ses informations dans une base de données administrée par un SGBD. Installez le SGBD sur le réseau avant Kaspersky Security Center (découvrez comment sélectionner un SGBD). Si vous décidez d'installer le SGBD PostgreSQL ou Postgres Pro, indiquez un mot de passe de superutilisateur. Si le mot de passe n'est pas indiqué, le Serveur d'administration risque de ne pas pouvoir se connecter à la base de données.

  Il est recommandé d'installer le Serveur d'administration sur un serveur dédié au lieu d'un contrôleur de domaine. Toutefois, si vous installez Kaspersky Security Center sur un serveur qui joue le rôle du contrôleur de domaine en lecture seule (RODC), le serveur Microsoft SQL Server (SQL Express) ne doit pas être installé en local (sur le même appareil). Dans ce cas, nous vous recommandons d'installer Microsoft SQL Server (SQL Express) à distance (sur un autre appareil), ou, si vous devez installer le SGBD localement, d'utiliser MySQL, MariaDB ou PostgreSQL.

- **Préparer les dossiers pour le Serveur d'administration, l'Agent d'administration et la Console d'administration**

  Le Serveur d'administration, l'Agent d'administration et la Console d'administration doivent être installés dans des dossiers où la casse est désactivée. De plus, la sensibilité à la casse doit être désactivée pour le dossier partagé du Serveur d'administration et le dossier caché de Kaspersky Security Center (%ALLUSERSPROFILE%\KasperskyLab\adminkit).

- **Supprimer l'ancien Agent d'administration**

  Outre le module Serveur d'administration, la version serveur de l'Agent d'administration est installée sur l'appareil. L'installation du Serveur d'administration avec la version standard de l'Agent d'administration est impossible. Si la version serveur de l'Agent d'administration est déjà installée sur votre appareil, il faut la supprimer et lancer à nouveau l'installation du Serveur d'administration. Pour en savoir plus sur la version serveur de l'Agent d'administration, consultez la section Modifications du système après l'installation de Kaspersky Security Center.

- **Contrôle des comptes**

  L'installation de Kaspersky Security Center requiert des autorisations d'administrateur local sur l'appareil où l'installation a lieu.

  Kaspersky Security Center est compatible avec les comptes de service administrés et les comptes de service administrés de groupe. Si ces types de comptes sont utilisés dans votre domaine et que vous souhaitez en définir un comme compte du service Serveur d'administration, installez d'abord le compte sur le même appareil sur lequel vous souhaitez installer le Serveur d'administration. Pour plus de détails sur l'installation des comptes de services administrés sur un appareil local, consultez la documentation officielle de Microsoft.

Comptes utilisateur pour l'utilisation d'un SGBD

Pour installer et utiliser le Serveur d'administration, vous avez besoin d'un compte Windows sous lequel vous allez exécuter le programme d'installation du Serveur d'administration (ci-après également le programme d'installation), d'un compte Windows sous lequel vous lancerez le service du Serveur d'administration et d'un SGBD interne compte utilisateur pour accéder au SGBD. Vous pouvez créer de nouveaux comptes ou utiliser des comptes existants. Tous ces comptes nécessitent des droits spécifiques. L'ensemble des comptes requis et de leurs droits dépend des critères suivants :

- Type de SGBD :
  - Microsoft SQL Server (avec authentification Windows ou authentification SQL Server)
  - MySQL ou MariaDB
  - PostgreSQL ou Postgres Pro
- Emplacement du SGBD :
  - **SGBD local**. Un *SGBD local* est un SGBD installé sur le même appareil que le Serveur d'administration.
  - **SGBD distant**. Un *SGBD distant* est un SGBD installé sur un autre appareil.
- Méthode de création de la base de données du Serveur d'administration :
  - **Automatique**. Lors de l'installation du Serveur d'administration, vous pouvez créer automatiquement une base de données du Serveur d'administration (ci-après également appelée base de données du Serveur) à l'aide du programme d'installation.
  - **Manuel**. Vous pouvez utiliser une application tierce (par exemple, SQL Server Management Studio) ou un script pour créer une base de données vide. Après cela, vous pouvez spécifier cette base de données comme base de données du Serveur lors de l'installation du Serveur d'administration.

Suivez le principe du moindre privilège lorsque vous accordez des droits et des autorisations aux comptes. Cela signifie que les droits accordés doivent être suffisants uniquement pour exécuter les actions requises.

Les tableaux ci-dessous contiennent des informations sur les droits système et les droits SGBD que vous devez accorder aux comptes avant d'installer et de lancer le Serveur d'administration.

Microsoft SQL Server avec authentification Windows

Si vous choisissez SQL Server comme SGBD, vous pouvez utiliser l'authentification Windows pour accéder à SQL Server. Configurez les droits système d'un compte Windows utilisé pour exécuter le programme d'installation et d'un compte Windows utilisé pour lancer le service du Serveur d'administration. Sur SQL Server, créez des connexions pour ces deux comptes Windows. Selon le mode de création de la base de données Serveur, accordez à ces comptes les privilèges SQL Server requis, comme indiqué dans le tableau ci-dessous. Pour plus d'informations sur la configuration des droits des comptes, consultez la section Configuration des comptes pour l'utilisation de SQL Server (authentification Windows).

SGBD : Microsoft SQL Server (y compris Express Edition) avec authentification Windows

	Création automatique de la base de données (par le programme d'installation)	Création manuelle de la base de données (par l'administrateur)
Compte utilisateur sous lequel est exécuté le programme d'installation	• SGBD distant : uniquement un compte de domaine de l'appareil distant sur lequel le SGBD est installé. • SGBD local : un compte d'administrateur local ou un compte de domaine.	• SGBD distant : uniquement un compte de domaine de l'appareil distant sur lequel le SGBD est installé. • SGBD local : un compte d'administrateur local ou un compte de domaine.

Privilèges du compte utilisateur sous lequel est exécuté le programme d'installation	• Privilèges système : privilèges d'administrateur local.
	• Privilèges SQL Server :
	  • Rôle de niveau serveur : sysadmin.
		• Privilèges système : privilèges d'administrateur local.
		• Privilèges SQL Server :
		  • - Rôle de niveau serveur : public.
		  • Appartenance au rôle de base de données pour la base de données du serveur : db_owner, public.
		  • Schéma par défaut de la base de données du Serveur : dbo.

Compte utilisateur du service du Serveur d'administration	• SGBD distant : uniquement un compte de domaine de l'appareil distant sur lequel le SGBD est installé.
	• SGBD local :
	  • Un compte Windows choisi par l'administrateur.
	  • Un compte au format KL-AK-* que le programme d'installation crée automatiquement.
		• SGBD distant : uniquement un compte de domaine de l'appareil distant sur lequel le SGBD est installé.
		• SGBD local :
		  • Un compte Windows choisi par l'administrateur.
		  • Un compte au format KL-AK-* que le programme d'installation crée automatiquement (dans ce cas, il est déconseillé de créer un compte KL-AK-*).

Privilèges du compte utilisateur du service du Serveur d'administration	• Privilèges système : privilèges requis attribués par le programme d'installation
	• Privilèges SQL Server : privilèges requis attribués par le programme d'installation
		• Privilèges système : privilèges requis attribués par le programme d'installation
		• Privilèges SQL Server :
		  • - Rôle de niveau serveur : public.
		  • Appartenance au rôle de base de données pour la base de données du serveur : db_owner, public.
		  • Schéma par défaut de la base de données du Serveur : dbo.

Microsoft SQL Server avec authentification SQL Server

Si vous choisissez SQL Server comme SGBD, vous pouvez utiliser l'authentification SQL Server pour accéder à SQL Server. Configurez les privilèges système d'un compte Windows utilisé pour exécuter le programme d'installation et d'un compte Windows utilisé pour lancer le service du Serveur d'administration. Sur SQL Server, créez un identifiant avec un mot de passe pour l'utiliser pour l'authentification. Ensuite, accordez à ce compte SQL Server les droits requis répertoriés dans le tableau ci-dessous. Pour plus d'informations sur la configuration des droits des comptes, consultez Configuration des comptes pour l'utilisation de SQL Server (authentification SQL Server).

SGBD : Microsoft SQL Server (y compris Express Edition) avec authentification SQL Server

	Création automatique de la base de données (par le programme d'installation)	Création manuelle de la base de données (par l'administrateur)
Compte utilisateur sous lequel est exécuté le programme d'installation	• SGBD distant : uniquement un compte de domaine de l'appareil distant sur lequel le SGBD est installé. • SGBD local : un compte d'administrateur local ou un compte de domaine.	• SGBD distant : uniquement un compte de domaine de l'appareil distant sur lequel le SGBD est installé. • SGBD local : un compte d'administrateur local ou un compte de domaine.
Privilèges du compte utilisateur sous lequel est exécuté le programme d'installation	Privilèges système : privilèges d'administrateur local.	Privilèges système : privilèges d'administrateur local.

Compte utilisateur du service du Serveur d'administration	• SGBD distant : uniquement un compte de domaine de l'appareil distant sur lequel le SGBD est installé.
	• SGBD local :
	  • Un compte Windows choisi par l'administrateur.
	  • Un compte au format KL-AK-* que le programme d'installation crée automatiquement.
		• SGBD distant : uniquement un compte de domaine de l'appareil distant sur lequel le SGBD est installé.
		• SGBD local :
		  • Un compte utilisateur Windows choisi par l'administrateur.
		  • Un compte au format KL-AK-* que le programme d'installation crée automatiquement.

Privilèges du compte utilisateur du service du Serveur d'administration	Privilèges système : privilèges requis attribués par le programme d'installation	Privilèges système : privilèges requis attribués par le programme d'installation

Droits du login utilisé pour l'authentification SQL Server	Droits SQL Server requis pour créer une base de données et installer le Serveur d'administration :
	• Rôle de niveau serveur : public.
	• Appartenance au rôle de base de données pour la base de données *master* : db_owner.
	• Schéma par défaut de la base de données *master* : dbo.
	• Permissions :
	  • CONNECT ANY DATABASE
	  • CONNECT SQL
	  • CREATE ANY DATABASE
	  • VIEW ANY DATABASE
	  • VIEW SERVER STATE (si l'option **Always On** est activée)
	Droits SQL Server requis pour utiliser le Serveur d'administration :
	• Rôle de niveau serveur : public.
	• Appartenance au rôle de base de données pour la base de données du serveur : db_owner.
	• Schéma par défaut de la base de données du Serveur : dbo.
	• Permissions :
	  • CONNECTER SQL
	  • VIEW ANY DATABASE
	  • VIEW SERVER STATE (si l'option **Always On** est activée)
	  • VOIR N'IMPORTE QUELLE DÉFINITION
		Privilèges SQL Server :
		• Rôle de niveau serveur : public.
		• Appartenance au rôle de base de données pour la base de données du serveur : db_owner.
		• Schéma par défaut de la base de données du Serveur : dbo.
		• Permissions :
		  • CONNECTER SQL
		  • VOIR TOUTES LES BASE DE DONNÉES
		  • VOIR N'IMPORTE QUELLE DÉFINITION

Configuration des privilèges du serveur SQL pour la récupération des données du Serveur d'administration

Pour restaurer les données du Serveur d'administration à partir de la sauvegarde, exécutez l'utilitaire klbackup sous le compte utilisateur Windows employé pour installer le Serveur d'administration. Avant de lancer l'utilitaire klbackup, sur SQL Server, accordez à l'identifiant SQL Server les privilèges associés à ce compte Windows. Les privilèges du Serveur SQL différent selon la version du Serveur d'administration. Pour le Serveur d'administration version 14.2 ou suivante, vous pouvez attribuer le rôle au sysadmin au niveau du serveur ou le rôle dbcreator au niveau du serveur.

Privilèges SQL Server pour la récupération de la base de données du Serveur d'administration

Serveur d'administration 14.2 ou versions ultérieures	Autres versions du Serveur d'administration

• Privilèges SQL Server :
  • Rôle de niveau serveur : dbcreator.
• Permissions :
  • VOIR N'IMPORTE QUELLE DÉFINITION
Avant de lancer l'utilitaire klbackup, indiquez l'indicateur de serveur KLSRV_SKIP_ADJUSTING_DBMS_ACCESS. Exécutez l'invite de commande Windows en utilisant les droits d'administrateur, puis remplacez votre répertoire actuel par celui contenant l'utilitaire klscflag. L'utilitaire klsclag se trouve dans le dossier dans lequel le Serveur d'administration est installé. Chemin d'installation par défaut est <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center. Après cela, exécutez la commande suivante dans la ligne de commande :
`klscflag.exe -fset -pv klserver -n KLSRV_SKIP_ADJUSTING_DBMS_ACCESS -t d -v 1`	

MySQL et MariaDB

Si vous choisissez MySQL ou MariaDB comme SGBD, créez un compte interne de SGBD et accordez à ce compte les privilèges requis indiqués dans le tableau ci-dessous. Le programme d'installation et le service du Serveur d'administration utilisent ce compte utilisateur SGBD interne pour accéder au SGBD. Notez que la méthode de création de la base de données n'affecte pas l'ensemble des droits requis. Pour plus d'informations sur la configuration des privilèges du compte, consultez Configuration des comptes pour l'utilisation avec MySQL et MariaDB.

SGBD : MySQL et MariaDB

	Création automatique ou manuelle de la base de données
Compte utilisateur sous lequel est exécuté le programme d'installation	• SGBD distant : uniquement un compte de domaine de l'appareil distant avec le SGBD installé. • SGBD local : un compte d'administrateur local ou un compte de domaine.
Privilèges du compte utilisateur sous lequel est exécuté le programme d'installation	Privilèges système : privilèges d'administrateur local.

Compte utilisateur du service du Serveur d'administration	• SGBD distant : uniquement un compte de domaine de l'appareil distant avec le SGBD installé.
	• SGBD local :
	  • Un compte Windows choisi par l'administrateur.
	  • Un compte au format KL-AK-* que le programme d'installation crée automatiquement.

Privilèges du compte utilisateur du service du Serveur d'administration	Privilèges système : privilèges requis attribués par le programme d'installation
Droits du compte interne du SGBD	Privilèges du schéma : • Base de données du Serveur d'administration : ALL (sauf GRANT OPTION). • Schémas système (mysql et sys) : SELECT, SHOW VIEW. • La procédure stockée sys.table_exists : EXECUTE (si vous utilisez MariaDB 10.5 ou une version antérieure en tant que SGBD, vous n'avez pas besoin d'accorder le privilège EXECUTE). Privilèges globaux pour tous les schémas : PROCESS, SUPER.

Pour en savoir plus sur le déplacement des données d'un tablespace partagé vers un tablespace fichier par table, consultez Déplacement des données depuis un tablespace partagé vers un tablespace fichier par table dans les SGBD MySQL et MariaDB.

Configuration des privilèges pour la récupération des données du Serveur d'administration

Les droits que vous avez accordés au compte SGBD interne suffisent pour restaurer les données du Serveur d'administration à partir de la sauvegarde. Pour lancer la restauration, exécutez l'utilitaire klbackup sous le compte Windows utilisé pour installer le Serveur d'administration.

PostgreSQL ou Postgres Pro

Si vous choisissez PostgreSQL ou Postgres Pro comme SGBD, vous pouvez utiliser l'utilisateur *Postgres* (le rôle Postgres par défaut) ou créer un nouveau rôle Postgres (ci-après également appelé rôle) pour accéder au SGBD. Selon le mode de création de la base de données Serveur, accordez à ce rôle les privilèges requis, comme indiqué dans le tableau ci-dessous. Pour plus d'informations sur la configuration des privilèges du rôle, consultez la section Configuration des comptes pour l'utilisation avec PostgreSQL ou Postgres Pro.

SGBD : PostgreSQL ou Postgres Pro

	Création automatique de la base de données	Création manuelle de la base de données
Compte utilisateur sous lequel est exécuté le programme d'installation	• SGBD distant : uniquement un compte de domaine de l'appareil distant avec le SGBD installé. • SGBD local : un compte d'administrateur local ou un compte de domaine.	• SGBD distant : uniquement un compte de domaine de l'appareil distant avec le SGBD installé. • SGBD local : un compte d'administrateur local ou un compte de domaine.
Privilèges du compte utilisateur sous lequel est exécuté le programme d'installation	Privilèges système : privilèges d'administrateur local.	Privilèges système : privilèges d'administrateur local.

Compte utilisateur du service du Serveur d'administration	• SGBD distant : uniquement un compte de domaine de l'appareil distant avec le SGBD installé.
	• SGBD local :
	  • Un compte Windows choisi par l'administrateur.
	  • Un compte au format KL-AK-* que le programme d'installation crée automatiquement.
		• SGBD distant : uniquement un compte de domaine de l'appareil distant avec le SGBD installé.
		• SGBD local :
		  • Un compte Windows choisi par l'administrateur.
		  • Un compte au format KL-AK-* que le programme d'installation crée automatiquement.

Privilèges du compte utilisateur du service du Serveur d'administration	Privilèges système : privilèges requis attribués par le programme d'installation		Privilèges système : privilèges requis attribués par le programme d'installation
Privilèges du rôle Postgres	L'utilisateur *Postgres* n'a pas besoin de privilèges supplémentaires.	Privilèges pour un nouveau rôle : `CREATEDB`.	Pour un nouveau rôle : • Privilèges sur les bases de données du Serveur d'administration : `ALL`. • Privilèges sur toutes les tables du schéma public : `ALL`. • Privilèges sur toutes les séquences du schéma public : `ALL`.

Configuration des privilèges pour la récupération des données du Serveur d'administration

Pour restaurer les données du Serveur d'administration à partir de la sauvegarde, exécutez l'utilitaire klbackup sous le compte utilisateur Windows employé pour installer le Serveur d'administration. Notez que le rôle Postgres utilisé pour accéder au SGBD doit avoir les privilèges de propriétaire sur la base de données du Serveur d'administration.

Configuration des comptes pour l'utilisation avec SQL Server (authentification Windows)

Prérequis

Avant d'attribuer des droits aux comptes, exécutez les actions suivantes :

1. Assurez-vous que vous vous connectez au système sous le compte d'administrateur local.
2. Installez un environnement pour travailler avec SQL Server.
3. Assurez-vous que vous disposez d'un compte Windows sous lequel vous allez installer le Serveur d'administration.
4. Assurez-vous que vous disposez d'un compte Windows sous lequel vous allez lancer le service du Serveur d'administration.
5. Sur le serveur SQL, créez un login pour le compte Windows utilisé pour exécuter le programme d'installation du Serveur d'administration (ci-après également le programme d'installation). Créez également un identifiant pour le compte Windows utilisé pour lancer le service du Serveur d'administration.

Si vous utilisez SQL Server Management Studio, sur la page **Général** de la fenêtre des propriétés de connexion, sélectionnez l'option **Authentification Windows**.

Si vous souhaitez installer le Serveur d'administration et le Serveur SQL sur des appareils qui se trouvent dans des domaines Windows distincts, veuillez noter que ces domaines doivent entretenir des relations de confiance bilatérales pour garantir le bon fonctionnement du Serveur d'administration, y compris l'exécution des tâches et l'application des stratégies. Pour obtenir plus d'informations sur les comptes requis pour utiliser le SGBD et les privilèges des comptes, consultez Comptes utilisateur pour l'utilisation d'un SGBD.

Configuration des comptes utilisateur pour installer le Serveur d'administration (création automatique de la base de données du Serveur d'administration)

Pour configurer les comptes d'installation du Serveur d'administration, procédez comme suit :

1. Sur SQL Server, attribuez le rôle de niveau serveur sysadmin au login du compte Windows utilisé pour exécuter le programme d'installation.
2. Connectez-vous au système sous le compte utilisateur Windows utilisé pour exécuter le programme d'installation.
3. Exécutez le programme d'installation du Serveur d'administration.

   L'Assistant d'installation du Serveur d'administration démarre. Suivez les instructions de l'assistant.
4. Sélectionnez l'option d'installation personnalisée du Serveur d'administration.
5. Sélectionnez le serveur Microsoft SQL en tant que SGBD qui stocke la base de données du Serveur d'administration.
6. Sélectionnez le mode d'authentification Microsoft Windows pour établir une connexion entre le Serveur d'administration et le Serveur SQL via un compte Windows.
7. Indiquez le compte Windows utilisé pour démarrer le service du Serveur d'administration.

   Vous pouvez sélectionner le compte utilisateur Windows pour lequel vous avez créé un login SQL Server précédemment. Vous pouvez également créer automatiquement un nouveau compte Windows au format KL-AK-* à l'aide du programme d'installation. Dans ce cas, le programme d'installation crée automatiquement un login SQL Server pour ce compte. Quel que soit le choix du compte, le programme d'installation attribue les droits système et les droits SQL Server requis au compte de service du Serveur d'administration.

Une fois l'installation terminée, la base de données du Serveur est créée et tous les droits système requis et les droits SQL Server sont attribués au compte de service du Serveur d'administration. Le Serveur d'administration est prêt à l'emploi.

Configuration des comptes utilisateurs pour l'installation du Serveur d'administration (création manuelle de la base de données du Serveur d'administration)

Pour configurer les comptes d'installation du Serveur d'administration, procédez comme suit :

1. Sur SQL Server, créez une base de données vide. Cette base de données sera utilisée comme base de données du Serveur d'administration (ci-après également appelée base de données du Serveur).
2. Pour les deux logins SQL Server créés pour les comptes Windows, spécifiez le rôle de niveau serveur public, puis configurez le mappage à la base de données créée :
   - Rôle de niveau serveur : public
   - Appartenance au rôle de base de données : db_owner, public
   - Schéma par défaut : dbo
3. Connectez-vous au système sous le compte utilisateur Windows utilisé pour exécuter le programme d'installation.

4. Exécutez le programme d'installation du Serveur d'administration.

   L'Assistant d'installation du Serveur d'administration démarre. Suivez les instructions de l'assistant.

5. Sélectionnez l'option d'installation personnalisée du Serveur d'administration.

6. Sélectionnez le serveur Microsoft SQL en tant que SGBD qui stocke la base de données du Serveur d'administration.

7. Indiquez le nom de la base de données créée comme nom de la base de données du Serveur d'administration.

8. Sélectionnez le mode d'authentification Microsoft Windows pour établir une connexion entre le Serveur d'administration et le Serveur SQL via un compte Windows.

9. Indiquez le compte Windows utilisé pour démarrer le service du Serveur d'administration.

   Vous pouvez sélectionner le compte utilisateur Windows pour lequel vous avez créé une connexion SQL Server et configuré les droits de connexion précédemment.

Il est déconseillé de créer automatiquement un nouveau compte Windows au format KL-AK-*. Dans ce cas, le programme d'installation crée un nouveau compte Windows pour lequel vous n'avez pas créé et configuré de compte SQL Server. Le Serveur d'administration ne peut pas utiliser ce compte pour lancer le service du Serveur d'administration. S'il est nécessaire de créer un compte Windows KL-AK-*, ne lancez pas la Console d'administration après l'installation. Faites plutôt ce qui suit :

1. Arrêtez le service kladminserver.

2. Sur SQL Server, créez un login SQL Server pour le compte Windows KL-AK-* créé.

3. Accordez les droits à ce login SQL Server et configurez le mappage à la base de données créée :

   - Rôle de niveau serveur : public
   - Appartenance au rôle de base de données : db_owner, public
   - Schéma par défaut : dbo

4. Redémarrez le service kladminserver, puis lancez la Console d'administration.

Une fois l'installation terminée, le Serveur d'administration utilisera la base de données créée pour stocker les données du Serveur. Le Serveur d'administration est prêt à l'emploi.

Configuration des comptes pour l'utilisation avec SQL Server (authentification SQL Server)

Prérequis

Avant d'attribuer des droits aux comptes, exécutez les actions suivantes :

1. Assurez-vous que vous vous connectez au système sous le compte d'administrateur local.

2. Installez un environnement pour travailler avec SQL Server.

3. Assurez-vous que vous disposez d'un compte Windows sous lequel vous allez installer le Serveur d'administration.

4. Assurez-vous que vous disposez d'un compte Windows sous lequel vous allez lancer le service du Serveur d'administration.

5. Sur SQL Server, activez le mode d'authentification SQL Server.

   Si vous utilisez SQL Server Management Studio, dans la fenêtre Propriétés du serveur SQL, sur la page **Sécurité**, sélectionnez l'option **Mode d'authentification SQL Server et Windows**.

6. Sur SQL Server, créez un login avec un mot de passe. Le programme d'installation du Serveur d'administration (ci-après également le programme d'installation) et le service du Serveur d'administration utiliseront ce compte SQL Server pour accéder à SQL Server.

   Si vous utilisez SQL Server Management Studio, sur la page **Général** de la fenêtre des propriétés de connexion, sélectionnez l'option **Authentification du serveur SQL**.

Si vous souhaitez installer le Serveur d'administration et le Serveur SQL sur des appareils qui se trouvent dans des domaines Windows distincts, veuillez noter que ces domaines doivent entretenir des relations de confiance bilatérales pour garantir le bon fonctionnement du Serveur d'administration, y compris l'exécution des tâches et l'application des stratégies. Pour obtenir plus d'informations sur les comptes requis pour utiliser le SGBD et les privilèges des comptes, consultez Comptes utilisateur pour l'utilisation d'un SGBD.

Configuration des comptes utilisateur pour installer le Serveur d'administration (création automatique de la base de données du Serveur d'administration)

Pour configurer les comptes d'installation du Serveur d'administration, procédez comme suit :

1. Sur SQL Server, mappez le compte SQL Server sur la base de données *master* par défaut. La base de données *master* est un modèle pour la base de données du Serveur d'administration (ci-après également appelée base de données du Serveur). La base de données *master* est utilisée pour le mappage jusqu'à ce que le programme d'installation crée une base de données Serveur. Accordez les droits et autorisations suivants au compte SQL Server :

   - Rôle de niveau serveur : public
   - Appartenance au rôle de base de données pour la base de données *master* : db_owner
   - Schéma par défaut de la base de données *master* : dbo
   - Permissions :
     - CONNECT ANY DATABASE
     - CONNECT SQL
     - CREATE ANY DATABASE
     - VOIR TOUTES LES BASE DE DONNÉES

2. Connectez-vous au système sous le compte utilisateur Windows utilisé pour exécuter le programme d'installation.

3. Exécuter le programme d'installation.

   L'Assistant d'installation du Serveur d'administration démarre. Suivez les instructions de l'assistant.

4. Sélectionnez l'option d'installation personnalisée du Serveur d'administration.

5. Sélectionnez le serveur Microsoft SQL en tant que SGBD qui stocke la base de données du Serveur d'administration.

6. Renseignez le nom de la base de données du Serveur d'administration.

7. Sélectionnez le mode d'authentification du serveur SQL pour établir une connexion entre le Serveur d'administration et le Serveur SQL via le compte SQL Server créé. Ensuite, spécifiez les informations d'identification du compte SQL Server.

8. Indiquez le compte Windows utilisé pour démarrer le service du Serveur d'administration.

   Vous pouvez sélectionner un compte utilisateur Windows existant ou créer un nouveau compte Windows au format KL-AK-* à l'aide du programme d'installation. Quel que soit le compte choisi, le programme d'installation attribue les droits système requis au compte de service du Serveur d'administration.

Une fois l'installation terminée, la base de données du Serveur est créée et tous les droits système requis sont attribués au compte de service du Serveur d'administration. Le Serveur d'administration est prêt à l'emploi.

Vous pouvez annuler le mappage vers la base de données *master*, car le programme d'installation a créé une base de données Serveur et configuré le mappage vers cette base de données lors de l'installation du Serveur d'administration.

Étant donné que la création automatique de la base de données nécessite plus d'autorisations que le travail normal avec le Serveur d'administration, vous pouvez révoquer certaines autorisations. Sur SQL Server, sélectionnez le compte SQL Server, puis accordez les privilèges suivants pour utiliser le Serveur d'administration :

- Rôle de niveau serveur : public
- Appartenance au rôle de base de données pour la base de données du serveur : db_owner
- Schéma par défaut de la base de données du Serveur : dbo
- Permissions :
  - CONNECTER SQL
  - VOIR TOUTES LES BASE DE DONNÉES

Configuration des comptes utilisateurs pour l'installation du Serveur d'administration (création manuelle de la base de données du Serveur d'administration)

Pour configurer les comptes d'installation du Serveur d'administration, procédez comme suit :

1. Sur SQL Server, créez une base de données vide. Cette base de données sera utilisée comme base de données du Serveur d'administration.
2. Sur SQL Server, accordez les droits et autorisations suivants au compte SQL Server :
   - - Rôle de niveau serveur : public.
   - Appartenance au rôle de base de données pour la base de données créée : db_owner.
   - Schéma par défaut de la base de données créée : dbo.
   - Permissions :
     - CONNECTER SQL
     - VOIR TOUTES LES BASE DE DONNÉES
3. Connectez-vous au système sous le compte utilisateur Windows utilisé pour exécuter le programme d'installation.
4. Exécuter le programme d'installation.

   L'Assistant d'installation du Serveur d'administration démarre. Suivez les instructions de l'assistant.
5. Sélectionnez l'option d'installation personnalisée du Serveur d'administration.
6. Sélectionnez le serveur Microsoft SQL en tant que SGBD qui stocke la base de données du Serveur d'administration.
7. Indiquez le nom de la base de données créée comme nom de la base de données du Serveur d'administration.
8. Sélectionnez le mode d'authentification du serveur SQL pour établir une connexion entre le Serveur d'administration et le Serveur SQL via le compte SQL Server créé. Ensuite, spécifiez les informations d'identification du compte SQL Server.
9. Indiquez le compte Windows utilisé pour démarrer le service du Serveur d'administration.

   Vous pouvez sélectionner un compte utilisateur Windows existant ou créer un nouveau compte Windows au format KL-AK-* à l'aide du programme d'installation. Quel que soit le compte choisi, le programme d'installation attribue les droits système requis au compte de service du Serveur d'administration.

Une fois l'installation terminée, le Serveur d'administration utilisera la base de données créée pour stocker les données du Serveur d'administration. Tous les droits système requis sont attribués au compte de service du Serveur d'administration. Le Serveur d'administration est prêt à l'emploi.

Configuration des comptes pour l'utilisation avec MySQL et MariaDB

Prérequis

Avant d'attribuer des droits aux comptes, exécutez les actions suivantes :

1. Assurez-vous que vous vous connectez au système sous le compte d'administrateur local.
2. Installez un environnement pour travailler avec MySQL ou MariaDB.
3. Assurez-vous que vous disposez d'un compte Windows sous lequel vous allez installer le Serveur d'administration.
4. Assurez-vous que vous disposez d'un compte Windows sous lequel vous allez lancer le service du Serveur d'administration.

Configuration des comptes pour installer le Serveur d'administration

Pour configurer les comptes d'installation du Serveur d'administration, procédez comme suit :

1. Exécutez un environnement pour travailler avec MySQL ou MariaDB sous le compte utilisateur root que vous avez créé lors de l'installation du SGBD.

2. Créez un compte utilisateur SGBD interne avec un mot de passe. Le programme d'installation du Serveur d'administration (ci-après également le programme d'installation) et le service du Serveur d'administration utiliseront ce compte utilisateur interne du SGBD pour accéder au SGBD. Accordez les privilèges suivants à ce compte :

   - Privilèges du schéma :
     - Base de données du Serveur d'administration : ALL (sauf `GRANT OPTION`)
     - Schémas système (mysql et sys) : `SELECT`, `SHOW VIEW`
     - La procédure stockée sys.table_exists : `EXECUTE`
   - Privilèges globaux pour tous les schémas : `PROCESS`, `SUPER`

   Pour créer un compte SGBD interne et accorder les privilèges requis à ce compte, exécutez le script ci-dessous (dans ce script, le login au SGBD est *KSCAdmin* et le nom de la base de données du Serveur d'administration est *kav*) :

   ```
   /* Créer un utilisateur nommé KSCAdmin */
   CREATE USER 'KSCAdmin'
   /* Spécifiez un mot de passe pour KSCAdmin */
   IDENTIFIED BY '<mot de passe>';
   ```

   Si vous utilisez MySQL 8.0 ou une version antérieure comme SGBD, notez que pour ces versions, l'authentification " Caching SHA2 password " n'est pas prise en charge. Modifiez l'authentification par défaut de " Mise en cache du mot de passe SHA2 " en " Mot de passe natif MySQL " :

   - Pour créer un compte utilisateur dans le SGBD qui utilise l'authentification par "mot de passe natif MySQL", exécutez la commande suivante :

     ```
     CREATE USER 'KSCAdmin'@'%' IDENTIFIED WITH mysql_native_password BY '<mot de passe>';
     ```

   - Pour modifier l'authentification d'un compte SGBD existant, exécutez la commande suivante :

     ```
     ALTER USER 'KSCAdmin'@'%' IDENTIFIED WITH mysql_native_password BY '<mot de passe>';
     ```

   ```
   /* Accorder des privilèges à KSCAdmin */
   GRANT USAGE ON *.* TO 'KSCAdmin';
   GRANT ALL ON kav.* TO 'KSCAdmin';
   GRANT SELECT, SHOW VIEW ON mysql.* TO 'KSCAdmin';
   GRANT SELECT, SHOW VIEW ON sys.* TO 'KSCAdmin';
   GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'KSCAdmin';
   GRANT PROCESS ON *.* TO 'KSCAdmin';
   GRANT SUPER ON *.* TO 'KSCAdmin';
   ```

Si vous utilisez MariaDB 10.5 ou une version antérieure en tant que SGBD, vous n'avez pas besoin d'accorder le privilège EXECUTE. Dans ce cas, excluez la commande suivante du script : `GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'KSCAdmin'`.

3. Pour consulter la liste des privilèges accordés au compte SGBD, exécutez le script suivant :

   ```
   SHOW grants for 'KSCAdmin';
   ```

4. Pour créer manuellement une base de données du Serveur d'administration, exécutez le script suivant (dans ce script, le nom de la base de données du Serveur d'administration est *kav*) :

   ```
   CREATE DATABASE kav
   DEFAULT CHARACTER SET ascii
   DEFAULT COLLATE ascii_general_ci;
   ```

   Utilisez le même nom de base de données que vous avez indiqué dans le script qui crée le compte SGBD.

5. Connectez-vous au système sous le compte utilisateur Windows utilisé pour exécuter le programme d'installation.

6. Exécuter le programme d'installation.

   L'Assistant d'installation du Serveur d'administration démarre. Suivez les instructions de l'assistant.

7. Sélectionnez l'option d'installation personnalisée du Serveur d'administration.

8. Sélectionnez MySQL ou MariaDB comme SGBD qui stocke la base de données du Serveur d'administration.

9. Renseignez le nom de la base de données du Serveur d'administration. Utilisez le même nom de base de données que vous avez indiqué dans le script.

10. Indiquez les informations d'identification du compte SGBD que vous avez créé par le script.

11. Indiquez le compte Windows utilisé pour démarrer le service du Serveur d'administration.

    Vous pouvez sélectionner un compte utilisateur Windows existant ou créer automatiquement un nouveau compte Windows au format KL-AK-* à l'aide du programme d'installation. Quel que soit le compte choisi, le programme d'installation attribue les droits système requis au compte de service du Serveur d'administration.

Une fois l'installation terminée, la base de données du Serveur d'administration est créée et le Serveur d'administration est prêt à l'emploi.

Déplacement de données d'un tablespace partagé vers un tablespace fichier par table dans les SGBD MySQL ou MariaDB

Pour les SGBD MySQL et MariaDB, vous pouvez stocker les données comme suit :

- En tant que tablespace partagé, lorsque les données de toutes les bases de données utilisateur sont stockées dans un fichier unique (généralement, dans le fichier `ibdata1`).
- En tant que tablespace fichier par table, lorsqu'un espace de données distinct est créé pour chaque table en tant que fichier distinct.

L'utilisation d'un tablespace partagé augmente le risque de fragmentation du tablespace. L'opération `SHRINK` étant impossible, un fichier du tablespace partagé peut occuper environ 90 % de l'espace disque. Cela affecte négativement les performances du sous-système de disque. Il est donc utile d'opter pour un tablespace fichier par table.

Cet article explique comment déplacer des données d'un tablespace partagé vers un tablespace fichier par table. Si les SGBD MySQL ou MariaDB sont également utilisés par d'autres applications, vous devez déplacer les bases de données de ces applications dans le tablespace fichier par table.

> Nous vous recommandons d'effectuer cette procédure uniquement si vous utilisez le SGBD pour Serveur d'administration MySQL ou MariaDB.
> Le déplacement de données d'un tablespace partagé vers un tablespace fichier par table peut augmenter la charge sur le sous-système de disque.

Prérequis

Avant de commencer, assurez-vous que :

- Vous avez créé une copie de sauvegarde des données du Serveur d'administration en exécutant une tâche de sauvegarde des données ou l'utilitaire klbackup.
- Vous avez créé une copie de sauvegarde des autres applications dont les bases de données sont gérées par le SGBD MySQL ou MariaDB (le cas échéant).
- Sur l'appareil sur lequel le SGBD est installé, il y a de l'espace libre sur la partition avec la base de données.

L'espace disque requis représente 150 % de la taille totale actuelle des bases (taille actuelle du fichier `ibdata1`).

Traiter

Pour déplacer des données d'un tablespace partagé vers un tablespace fichier par table, procédez comme suit :

1. Arrêtez le service du Serveur d'administration de Kaspersky Security Center et les autres applications utilisant l'instance du SGBD pour lequel vous souhaitez exécuter cette procédure.

2. En fonction de la version du SGBD, connectez-vous à votre SGBD en tant que superutilisateur, puis, dans n'importe quelle application pratique, exécutez le script `fix_tablespace.sql`.

   Vous pouvez consulter les scripts `fix_tablespace.sql` en cliquant sur les liens suivants :

   Consultez le script pour MySQL 5.7 et MariaDB 10.1 ou toute version ultérieure

```
DROP PROCEDURE IF EXISTS upgd_alter_all_tables_for_all_databases_to_innodb;
DELIMITER //
CREATE PROCEDURE `upgd_alter_all_tables_for_all_databases_to_innodb` ()
BEGIN
    DECLARE __st_FETCH_STATUS INT;
    DECLARE `schemaName` VARCHAR(192);
    DECLARE `tableName` VARCHAR(192);
    DECLARE `curIX` CURSOR FOR
    SELECT `TABLE_SCHEMA` , `TABLE_NAME`
    FROM information_schema.TABLES
    WHERE `TABLE_SCHEMA` NOT IN ('mysql', 'performance_schema', 'sys') AND TABLE_TYPE = 'BASE TABLE';
    DECLARE CONTINUE HANDLER FOR SQLSTATE '02000' SET __st_FETCH_STATUS = 1;

    OPEN `curIX`;
    SET `__st_FETCH_STATUS` = 0; FETCH `curIX` INTO `schemaName`, `tableName`;
    while1 : WHILE (0 = 0 AND __st_FETCH_STATUS = 0 ) DO
        SET @`strSQL` = CONCAT( 'ALTER TABLE `' , `schemaName`, '`.`',`tableName`, '` ENGINE=''InnoDB'';'
);
        PREPARE stmt1 FROM @`strSQL`;
        EXECUTE stmt1;
        DEALLOCATE PREPARE stmt1;

        SET `__st_FETCH_STATUS` = 0; FETCH `curIX` INTO `schemaName`, `tableName`;
    END WHILE;
    CLOSE `curIX`;
END
//
DELIMITER ;
SET GLOBAL innodb_file_per_table = 1;
CALL upgd_alter_all_tables_for_all_databases_to_innodb();
DROP PROCEDURE IF EXISTS upgd_alter_all_tables_for_all_databases_to_innodb;
```

Consultez le script pour MySQL 8.0+

```
DROP PROCEDURE IF EXISTS upgd_alter_all_tables_for_all_databases_to_innodb;
DELIMITER //
CREATE PROCEDURE `upgd_alter_all_tables_for_all_databases_to_innodb` ()
BEGIN
    DECLARE __st_FETCH_STATUS INT;
    DECLARE `schemaName` VARCHAR(192);
    DECLARE `tableName` VARCHAR(192);
    DECLARE `curIX` CURSOR FOR
    SELECT `TABLE_SCHEMA` , `TABLE_NAME`
    FROM information_schema.TABLES
    WHERE `TABLE_SCHEMA` NOT IN ('mysql', 'performance_schema', 'sys') AND TABLE_TYPE = 'BASE TABLE';
    DECLARE CONTINUE HANDLER FOR SQLSTATE '02000' SET __st_FETCH_STATUS = 1;

    OPEN `curIX`;
    SET `__st_FETCH_STATUS` = 0; FETCH `curIX` INTO `schemaName`, `tableName`;
    while1 : WHILE (0 = 0 AND __st_FETCH_STATUS = 0 ) DO
        SET @`strSQL` = CONCAT( 'ALTER TABLE `' , `schemaName`, '`.`',`tableName`, '` ENGINE=''InnoDB'';'
);
        PREPARE stmt1 FROM @`strSQL`;
        EXECUTE stmt1;
        DEALLOCATE PREPARE stmt1;

        SET @`strSQL` = CONCAT( 'ALTER TABLE `' , `schemaName`, '`.`',`tableName`, '` TABLESPACE =
innodb_file_per_table;' );
        PREPARE stmt2 FROM @`strSQL`;
        EXECUTE stmt2;
        DEALLOCATE PREPARE stmt2;

        SET `__st_FETCH_STATUS` = 0; FETCH `curIX` INTO `schemaName`, `tableName`;
    END WHILE;
    CLOSE `curIX`;
END
//
DELIMITER ;
SET GLOBAL innodb_file_per_table = 1;
CALL upgd_alter_all_tables_for_all_databases_to_innodb();
DROP PROCEDURE IF EXISTS upgd_alter_all_tables_for_all_databases_to_innodb;
```

Vous ne devez pas arrêter l'exécution du script.
Si aucune erreur de SGBD ne s'est produite, mais que vous avez interrompu l'exécution du script, soit exécutez à nouveau le script, soit arrêtez d'exécuter les étapes de cette procédure, redémarrez le service SGBD et restaurez les données du Serveur d'administration à partir de la sauvegarde.

3. Dans la section `[mysqld]` du fichier my.cnf, définissez le paramètre `innodb_file_per_table` sur `1`.

4. Redémarrez le service MySQL ou MariaDB.

5. Relancez le service du Serveur d'administration de Kaspersky Security Center.

Les données sont déplacées d'un tablespace partagé vers un tablespace fichier par table.

Configuration des comptes pour l'utilisation avec PostgreSQL et Postgres Pro

Prérequis

Avant d'attribuer des droits aux comptes, exécutez les actions suivantes :

1. Assurez-vous que vous vous connectez au système sous le compte d'administrateur local.
2. Installez un environnement pour l'utilisation avec PostgreSQL et Postgres Pro.
3. Configurez le serveur PostgreSQL ou Postgres Pro pour fonctionner avec Kaspersky Security Center 15.1.
4. Assurez-vous que vous disposez d'un compte Windows sous lequel vous allez installer le Serveur d'administration.
5. Assurez-vous que vous disposez d'un compte Windows sous lequel vous allez lancer le service du Serveur d'administration.

Configuration des comptes utilisateur pour installer le Serveur d'administration (création automatique de la base de données du Serveur d'administration)

Pour configurer les comptes d'installation du Serveur d'administration, procédez comme suit :

1. Exécutez un environnement pour l'utilisation avec PostgreSQL et Postgres Pro.
2. Choisissez un rôle Postgres pour accéder au SGBD. Vous avez le choix parmi les rôles suivants :
   - L'utilisateur *Postgres* (le rôle Postgres par défaut).

     Si vous utilisez l'utilisateur *Postgres*, vous n'avez pas besoin de lui accorder des privilèges supplémentaires.
   - Un nouveau rôle Postgres.

     Si vous souhaitez utiliser un nouveau rôle Postgres, créez ce rôle et accordez-lui le privilège CREATEDB. Pour ce faire, exécutez le script suivant (dans ce script, le rôle est *KSCAdmin*) :

     ```
     CREATE USER "KSCAdmin" WITH PASSWORD '<mot de passe>' CREATEDB;
     ```

     Le rôle créé sera utilisé en tant que propriétaire de la base de données du Serveur d'administration (ci-après également appelée base de données du Serveur).
3. Connectez-vous au système sous le compte Windows utilisé pour exécuter le programme d'installation du Serveur d'administration (ci-après également le programme d'installation).
4. Exécuter le programme d'installation.

   L'Assistant d'installation du Serveur d'administration démarre. Suivez les instructions de l'assistant.
5. Sélectionnez l'option d'installation personnalisée du Serveur d'administration.
6. Sélectionnez PostgreSQL ou Postgres Pro en tant que SGBD qui stocke la base de données du Serveur d'administration.

7. Renseignez le nom de la base de données du Serveur. Le programme d'installation crée automatiquement la base de données du Serveur.

8. Indiquez les identifiants du rôle Postgres.

9. Indiquez le compte Windows utilisé pour démarrer le service du Serveur d'administration.

   Vous pouvez sélectionner un compte utilisateur Windows existant ou créer automatiquement un nouveau compte Windows au format KL-AK-* à l'aide du programme d'installation. Quel que soit le compte choisi, le programme d'installation attribue les droits système requis au compte de service du Serveur d'administration.

Une fois l'installation terminée, la base de données du Serveur d'administration est créée automatiquement et le Serveur d'administration est prêt à l'emploi.

Configuration des comptes utilisateurs pour l'installation du Serveur d'administration (création manuelle de la base de données du Serveur d'administration)

Pour configurer les comptes d'installation du Serveur d'administration, procédez comme suit :

1. Exécutez un environnement pour l'utilisation avec Postgres.

2. Connectez-vous sous l'utilisateur *Postgres* dans la base de données *Postgres*.

3. Créez un nouveau rôle Postgres (dans cet exemple, le rôle est *KSCAdmin*) :

   ```
   CREATE USER "KSCAdmin" WITH PASSWORD '< mot de passe >';
   ```

4. Créez une base de données de Serveur d'administration (dans cet exemple, le nom de la base de données du Serveur d'administration est *KAV*) :

   ```
   CREATE DATABASE "KAV" ENCODING 'UTF8' OWNER "KSCAdmin";
   ```

   Si l'erreur "Le nouvel encodage (UTF8) est incompatible avec l'encodage de la base de données modèle" se produit, créez une base de données à l'aide de la commande :
   `CREATE DATABASE "KAV" ENCODING 'UTF8' OWNER "KSCAdmin" TEMPLATE template0;`
   au lieu de :
   `CREATE DATABASE "KAV" ENCODING 'UTF8' OWNER "KSCAdmin";`

5. Accordez tous les privilèges au rôle dans la base de données du Serveur d'administration :

   ```
   GRANT ALL PRIVILEGES ON DATABASE "KAV" TO "KSCAdmin";
   ```

   Assurez-vous que le rôle dispose des privilèges CONNECT et TEMPORARY par défaut sur la base de données du Serveur d'administration.

6. Accordez les privilèges suivants au rôle Postgres créé :

   - Privilèges sur toutes les tables du schéma public : ALL.
   - Privilèges sur toutes les séquences du schéma public : ALL.

   Pour ce faire, connectez-vous sous l'utilisateur *Postgres* dans la base de données Serveur et exécutez le script suivant (dans ce script, le rôle est *KSCAdmin*) :

   ```
   GRANT ALL PRIVILEGES ON ALL TABLES IN SCHEMA "public" TO "KSCAdmin";
   GRANT ALL PRIVILEGES ON ALL SEQUENCES IN SCHEMA "public" TO "KSCAdmin";
   ```

7. Connectez-vous au système sous le compte utilisateur Windows utilisé pour exécuter le programme d'installation.

8. Exécutez le programme d'installation du Serveur d'administration.

   L'Assistant d'installation du Serveur d'administration démarre. Suivez les instructions de l'assistant.

9. Sélectionnez l'option d'installation personnalisée du Serveur d'administration.

10. Sélectionnez PostgreSQL ou Postgres Pro en tant que SGBD qui stocke la base de données du Serveur d'administration.

11. Renseignez le nom de la base de données du Serveur. Utilisez le même nom de base de données que vous avez indiqué dans le script. Notez que le nom de la base de données est sensible à la casse.

12. Indiquez les identifiants du rôle Postgres.

13. Indiquez le compte Windows utilisé pour démarrer le service du Serveur d'administration.

    Vous pouvez sélectionner un compte utilisateur Windows existant ou créer automatiquement un nouveau compte Windows au format KL-AK-* à l'aide du programme d'installation. Quel que soit le compte choisi, le programme d'installation attribue les droits système requis au compte de service du Serveur d'administration.

Une fois l'installation terminée, le Serveur d'administration utilisera la base de données créée pour stocker les données du Serveur d'administration. Le Serveur d'administration est prêt à l'emploi.

Scénario : authentification de Microsoft SQL Server

Les informations de cette section ne s'appliquent qu'aux configurations dans lesquelles Kaspersky Security Center utilise Microsoft SQL Server comme système de gestion de base de données.

Pour protéger les données de Kaspersky Security Center transférées vers la base de données et les données stockées dans la base de données contre tout accès non autorisé ou à partir de celles-ci, vous devez sécuriser la communication entre Kaspersky Security Center et le serveur SQL. Le moyen le plus fiable permettant d'assurer une communication sécurisée consiste à installer Kaspersky Security Center et le serveur SQL sur le même appareil et à utiliser le mécanisme de mémoire partagée pour les deux applications. Dans tous les autres cas, nous vous recommandons d'utiliser un certificat SSL ou TLS pour authentifier l'instance du serveur SQL. Vous pouvez utiliser un certificat d'une autorité de certification de confiance ou un certificat auto-signé. Nous vous recommandons d'utiliser un certificat provenant d'une autorité de certification de confiance, car un certificat auto-signé n'offre qu'une protection limitée.

L'authentification du serveur SQL se déroule par étapes :

1. **Génération d'un certificat SSL ou TLS auto-signé pour le serveur SQL conformément aux exigences du certificat**

   Si vous disposez déjà d'un certificat pour le serveur SQL, ignorez cette étape.

   Un certificat SSL s'applique uniquement aux versions de SQL Server antérieures à 2016 (13.x). Dans SQL Server 2016 (13.x) et versions ultérieures, utilisez un certificat TLS.

   Par exemple, pour générer un certificat TLS, entrez la commande suivante dans PowerShell :

   ```
   New-SelfSignedCertificate -DnsName SQL_HOST_NAME -CertStoreLocation cert:\LocalMachine
   -KeySpec KeyExchange
   ```

   Dans la commande, plutôt que d'entrer SQL_HOST_NAME, vous devez taper le nom d'hôte du serveur SQL si l'hôte est inclus dans le domaine ou taper le *nom de domaine pleinement qualifié* (FQDN) de l'hôte si l'hôte n'est pas inclus dans le domaine. Le même nom (nom d'hôte ou nom de domaine pleinement qualifié) doit être indiqué comme nom d'instance du serveur SQL dans l'Assistant d'installation du Serveur d'administration.

2. **Ajout du certificat sur l'instance du serveur SQL**

   Pour cette étape, les instructions dépendent de la plateforme sur laquelle le serveur SQL est exécuté. Pour plus d'informations, consultez la documentation du fournisseur :

   - Windows
   - Linux
   - Amazon Relational Database Service
   - Windows Azure

   Pour utiliser le certificat sur un cluster de basculement, vous devez installer le certificat sur chaque nœud du cluster de basculement. Pour plus de détails, consultez la documentation Microsoft.

3. **Attribution des autorisations de compte de service**

   Assurez-vous que le compte de service à partir duquel le service du serveur SQL est exécuté dispose de l'autorisation Contrôle total pour accéder aux clés privées. Pour plus de détails, consultez la documentation Microsoft.

4. **Ajout du certificat à la liste des certificats de confiance pour Kaspersky Security Center**

   Sur l'appareil du Serveur d'administration, ajoutez le certificat à la liste des certificats de confiance. Pour plus de détails, consultez la documentation Microsoft.

5. **Activation des connexions chiffrées entre l'instance du serveur SQL et Kaspersky Security Center**

   Sur l'appareil du Serveur d'administration, indiquez la valeur `1` pour la variable d'environnement `KLDBADO_UseEncryption`. Par exemple, dans Windows Server 2012 R2, vous pouvez modifier les variables d'environnement en cliquant sur **Variables d'environnement** sous l'onglet **Avancé** de la fenêtre **Propriétés système**. Ajoutez une nouvelle variable, intitulez-la `KLDBADO_UseEncryption`, puis indiquez la valeur `1`.

6. **Configuration supplémentaire pour l'utilisation du protocole TLS 1.2**

   Si vous utilisez le protocole TLS 1.2, procédez également comme suit :

   - Assurez-vous que la version installée du serveur SQL est une application 64 bits.
   - Installez Microsoft OLE DB Driver sur l'appareil du Serveur d'administration. Pour plus de détails, consultez la documentation Microsoft.

- Sur l'appareil du Serveur d'administration, indiquez la valeur `1` pour la variable d'environnement `KLDBADO_UseMSOLEDBSQL`. Par exemple, dans Windows Server 2012 R2, vous pouvez modifier les variables d'environnement en cliquant sur **Variables d'environnement** sous l'onglet **Avancé** de la fenêtre **Propriétés système**. Ajoutez une nouvelle variable, intitulez-la `KLDBADO_UseMSOLEDBSQL`, puis indiquez la valeur `1`.

  Si la version du pilote OLE DB est 19 ou plus récente, définissez également la valeur `MSOLEDBSQL19` sur la variable d'environnement `KLDBADO_ProviderName`.

7. **Activation de l'utilisation du protocole TCP/IP sur une instance nommée du serveur SQL**

   Si vous utilisez une instance nommée du serveur SQL, activez également l'utilisation du protocole TCP/IP et attribuez un numéro de port TCP/IP au moteur de base de données SQL Server. Lorsque vous configurez la connexion du serveur SQL dans l'Assistant d'installation du Serveur d'administration, indiquez le nom d'hôte du serveur SQL et le numéro de port dans le champ **Nom de l'instance du serveur SQL**.

Scénario : Authentification du serveur MySQL

Nous vous recommandons d'utiliser un certificat TLS pour authentifier le serveur MySQL. Vous pouvez utiliser un certificat d'une autorité de certification de confiance ou un certificat auto-signé.

Le Serveur d'administration prend en charge l'authentification SSL unidirectionnelle et bidirectionnelle pour MySQL.

Activer l'authentification SSL unidirectionnelle

Suivez ces étapes pour configurer l'authentification SSL unidirectionnelle pour MySQL :

1. **Générez un certificat TLS auto-signé pour le serveur MySQL**

   Dans PowerShell, remplacez le répertoire par le dossier dans lequel vous souhaitez stocker les certificats. Exécutez les commande suivantes :

```
$CertCA = New-SelfSignedCertificate `
-Subject "CN=CertCA" `
-CertStoreLocation "Cert:\CurrentUser\My" `
-HashAlgorithm "SHA256" `
-NotAfter (Get-Date).AddDays(365)

$CertCABase64 = [System.Convert]::ToBase64String($CertCA.RawData,
[System.Base64FormattingOptions]::InsertLineBreaks)

$CertLeaf = New-SelfSignedCertificate `
-Subject "CN=CertLeaf" `
-Signer $CertCA `
-CertStoreLocation "Cert:\CurrentUser\My" `
-HashAlgorithm "SHA256" `
-KeyExportPolicy Exportable `
-NotAfter (Get-Date).AddDays(365)

$CertLeafBase64 = [System.Convert]::ToBase64String($CertLeaf.RawData,
[System.Base64FormattingOptions]::InsertLineBreaks)

$CertLeafRSACng =
[System.Security.Cryptography.X509Certificates.RSACertificateExtensions]::GetRSAPrivateKey($CertLeaf)
$CertLeafKeyBytes =
$CertLeafRSACng.Key.Export([System.Security.Cryptography.CngKeyBlobFormat]::Pkcs8PrivateBlob)
$CertLeafKeyBase64 = [System.Convert]::ToBase64String($CertLeafKeyBytes,
[System.Base64FormattingOptions]::InsertLineBreaks)

$CertCAPemCert = @"
-----BEGIN CERTIFICATE-----
$CertCABase64
-----END CERTIFICATE-----
"@

$CertLeafPemKey = @"
-----BEGIN PRIVATE KEY-----
```

```
$CertLeafKeyBase64
-----END PRIVATE KEY-----
"@

$CertLeafPemCert = @"
-----BEGIN CERTIFICATE-----
$CertLeafBase64
-----END CERTIFICATE-----
"@

# Output to file

$CertCAPemCert | Out-File -FilePath ca-cert.pem -Encoding Ascii

$CertLeafPemKey | Out-File -FilePath server-key.pem -Encoding Ascii
$CertLeafPemCert | Out-File -FilePath server-cert.pem -Encoding Ascii
```

Ces commandes créent des certificats pour l'utilisateur actuel et exportent les certificats au format PEM. Pour authentifier le serveur, seul les fichiers PEM exportés sont nécessaires. Pour supprimer les certificats créés depuis Windows, exécutez la commande suivante dans PowerShell :

```
certmgr.msc
```

Dans le dossier **Personnel** → **Certificats**, localisez les certificats créés et supprimez-les.

2. **Créez un fichier indicateur de serveur**

   Exécutez l'invite de commande Windows en utilisant les droits d'administrateur, puis remplacez votre répertoire actuel par celui contenant l'utilitaire klscflag. L'utilitaire klsclag se trouve dans le dossier dans lequel le Serveur d'administration est installé. Chemin d'installation par défaut est <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

   Utilisez l'utilitaire klsclag pour créer l'indicateur de serveur KLSRV_MYSQL_OPT_SSL_CA et indiquez le chemin d'accès au certificat comme valeur.

   ```
   klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_CA -v <chemin vers ca-cert.pem> -t s
   ```

3. **Configurez la base de données**

   Spécifiez les certificats dans le fichier my.cnf. Ouvrez le fichier my.cnf dans un éditeur de texte et ajoutez les lignes suivantes dans la section [mysqld] :

   ```
   [mysqld]
   ssl-ca="...\mysqlcerts\ca-cert.pem"
   ssl-cert="...\mysqlcerts\server-cert.pem"
   ssl-key="...\mysqlcerts\server-key.pem"
   ```

Activer l'authentification SSL bidirectionnelle

Suivez ces étapes pour configurer l'authentification SSL bidirectionnelle pour MySQL :

1. **Créez les fichiers indicateurs de serveur**

   Exécutez l'invite de commande Windows en utilisant les droits d'administrateur, puis remplacez votre répertoire actuel par celui contenant l'utilitaire klscflag. L'utilitaire klsclag se trouve dans le dossier dans lequel le Serveur d'administration est installé. Chemin d'installation par défaut est <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

   Utilisez l'utilitaire klscflag pour créer les indicateurs de serveur et indiquez le chemin d'accès aux fichiers de certificat comme valeur :

   ```
   klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_CA -v <chemin vers ca-cert.pem> -t
   s
   ```

```
klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_CERT -v <chemin vers server-cert.pem> -t s
```

```
klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_KEY -v <chemin vers server-key.pem> -t s
```

2. **Indiquez la phrase secrète (facultatif)**

   Si server-key.pem requiert une phrase secrète, créez un indicateur KLSRV_MARIADB_OPT_TLS_PASPHRASE et indiquez la phrase secrète comme valeur :

   ```
   klscflag -fset -pv klserver -n KLSRV_MARIADB_OPT_TLS_PASPHRASE -v <phrase secrète> -t s
   ```

3. **Configurez la base de données**

   Spécifiez les certificats dans le fichier my.cnf. Ouvrez le fichier my.cnf dans un éditeur de texte et ajoutez les lignes suivantes dans la section [mysqld] :

   ```
   [mysqld]
   ssl-ca="...\ca-cert.pem"
   ssl-cert="...\server-cert.pem"
   ssl-key="...\server-key.pem"
   ```

Scénario : Authentification du serveur PostgreSQL

Nous vous recommandons d'utiliser un certificat TLS pour authentifier le serveur PostgreSQL. Vous pouvez utiliser un certificat d'une autorité de certification de confiance ou un certificat auto-signé. Utiliser un certificat provenant d'une autorité de certification de confiance, car un certificat auto-signé n'offre qu'une protection limitée.

Le Serveur d'administration prend en charge l'authentification SSL unidirectionnelle et bidirectionnelle pour PostgreSQL.

L'authentification du Serveur PostgreSQL se déroule par étapes :

1. **Générer un certificat pour le Serveur PostgreSQL**

   Dans un utilitaire multiplateforme basé sur OpenSSL, exécutez les commandes suivantes :

   ```
   openssl req -new -x509 -days 365 -nodes -text -out psql.crt -keyout psql.key -subj "/CN=psql"
   ```

   ```
   chmod og-rwx psql.key
   ```

2. **Générer un certificat pour le Serveur d'administration**

   Exécutez les commande suivantes. La valeur CN doit correspondre au nom de l'utilisateur qui se connecte à PostgreSQL au nom du Serveur d'administration. Le nom d'utilisateur est défini sur postgres par défaut.

   ```
   openssl req -new -x509 -days 365 -nodes -text -out postgres.crt -keyout postgres.key -subj "/CN=postgres"
   ```

   ```
   chmod og-rwx postgres.key
   ```

3. **Configurer l'authentification du certificat client**

   Modifiez pg_hba.conf comme suit :

```
hostssl all all 0.0.0.0/0 md5
```

Assurez-vous que pg_hba.conf n'inclut pas d'enregistrement commençant par `host`.

4. **Spécifier le certificat PostgreSQL**

   Authentification SSL unidirectionnelle

   Modifiez postgresql.conf comme suit (spécifiez le chemin correct vers les fichiers .crt et .key) :

   ```
   listen_addresses ='localhost, server-ip'
   ssl = on
   ssl_cert_file = '<psql.crt>'
   ssl_key_file = '<psql.key>'
   ```

   Authentification SSL bidirectionnelle

   Modifiez postgresql.conf comme suit (spécifiez le chemin correct vers les fichiers .crt et .key) :

   ```
   listen_addresses ='localhost, server-ip'
   ssl = on
   ssl_ca_file = '<postgres.crt>'
   ssl_cert_file = '<psql.crt>'
   ssl_key_file = '<psql.key>'
   ```

5. **Redémarrer PostgreSQL daemon**

   Exécutez la commande suivante :

   ```
   systemctl restart postgresql-14.service
   ```

6. **Spécifier l'indicateur de serveur pour le Serveur d'administration**

   Authentification SSL unidirectionnelle

   Utilisez l'utilitaire klsclag pour créer l'indicateur de serveur KLSRV_POSTGRES_OPT_SSL_CA et indiquez le chemin d'accès au certificat comme valeur.

   Exécutez l'invite de commande Windows en utilisant les droits d'administrateur, puis remplacez votre répertoire actuel par celui contenant l'utilitaire klscflag. L'utilitaire klsclag se trouve dans le dossier dans lequel le Serveur d'administration est installé. Chemin d'installation par défaut est <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

   Exécutez la commande suivante :

   ```
   klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_SSL_CA -v <chemin vers psql.crt> -t s
   ```

   Authentification SSL bidirectionnelle

Utilisez l'utilitaire klscflag pour créer les indicateurs de serveur et indiquez le chemin d'accès aux fichiers de certificat comme valeur.

Exécutez l'invite de commande Windows en utilisant les droits d'administrateur, puis remplacez votre répertoire actuel par celui contenant l'utilitaire klscflag. L'utilitaire klsclag se trouve dans le dossier dans lequel le Serveur d'administration est installé. Chemin d'installation par défaut est <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

Exécutez les commande suivantes :

```
klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_SSL_CA -v <chemin vers psql.crt> -t s
```

```
klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_SSL_CERT -v <chemin vers postgres.crt> -t s
```

```
klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_SSL_KEY -v <chemin vers postgres.key> -t s
```

Si `postgres.key` requiert une phrase secrète, créez un indicateur KLSRV_POSTGRES_OPT_TLS_PASPHRASE et indiquez la phrase secrète comme valeur :

```
klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_TLS_PASPHRASE -v <phrase secrète> -t s
```

7. **Relancer le service du Serveur d'administration**

Recommandations d'installation du Serveur d'administration

Cette section contient des recommandations sur l'installation du Serveur d'administration. La section contient aussi des scénarios d'utilisation du dossier partagé sur l'appareil doté du Serveur d'administration en vue du déploiement de l'Agent d'administration sur les appareils clients.

Création des comptes utilisateurs pour les services du Serveur d'administration sur un cluster haute disponibilité

Par défaut, le programme d'installation crée lui-même des comptes utilisateurs sans privilèges pour les services du Serveur d'administration. Ce comportement est parfaitement adapté à l'installation du Serveur d'administration sur un appareil normal.

Cependant, en cas d'installation du Serveur d'administration sur un cluster haute disponibilité, il faut procéder différemment :

1. Créer des comptes utilisateurs de domaine sans privilèges pour les services du Serveur d'administration et les ajouter au groupe de sécurité de domaine global KLAdmins.

2. Définir dans le programme d'installation du Serveur d'administration les comptes utilisateurs de domaine créés.

Désignation du dossier partagé

Lors de l'installation du Serveur d'administration, il est possible d'indiquer l'emplacement du dossier partagé. Vous pouvez également indiquer l'emplacement du dossier partagé après l'installation, dans les propriétés du Serveur d'administration. Le dossier partagé est créé par défaut sur l'appareil doté du Serveur d'administration (avec accès en lecture pour le groupe intégré **Everyone**). Cependant, dans certains cas (par exemple, charge élevée ou accès requis depuis un réseau isolé), il est préférable de placer le dossier partagé sur une ressource de fichiers spéciale.

Le dossier partagé intervient dans plusieurs scénarios de déploiement de l'Agent d'administration.

La casse pour le dossier partagé doit être désactivée.

Installation à distance à l'aide des outils du Serveur d'administration à l'aide de stratégies de groupe Active Directory

Si les appareils se trouvent dans un domaine Windows (il n'y a pas de groupes de travail), il est préférable de réaliser le déploiement initial (installation de l'Agent d'administration et de l'application de sécurité sur des appareils qui ne sont pas encore administrés) à l'aide de stratégies de groupe Active Directory. Le déploiement est exécuté à l'aide de la tâche normale d'installation à distance de Kaspersky Security Center. Si le réseau est grand, pour réduire la charge sur le sous-système de disque de l'appareil doté du Serveur d'administration, il est préférable de placer le dossier partagé sur une ressource de fichiers spéciale.

Installation à distance via la diffusion du chemin UNC vers le paquet autonome

Si les utilisateurs des appareils du réseau de l'entreprise possèdent les privilèges d'administrateur local, une autre méthode de déploiement local consiste à créer un paquet autonome de l'Agent d'administration (voire un paquet « en double » du paquet de l'Agent d'administration avec l'application de sécurité). Après la création du paquet autonome, il faut envoyer le lien d'accès au paquet hébergé dans le dossier partagé aux utilisateurs des appareils. Cliquez sur le lien pour lancer l'installation.

Mise à jour depuis le dossier partagé du Serveur d'administration

Il est possible de configurer la mise à jour depuis le dossier partagé du Serveur d'administration dans la tâche de mise à jour de l'Antivirus. Si la tâche est prévue pour un grand nombre d'appareils, il est préférable de placer le dossier partagé sur une ressource de fichiers spéciale.

Installation d'images des systèmes d'exploitation

L'installation des images des systèmes d'exploitation s'opère toujours via le dossier partagé : les appareils lisent l'image des systèmes d'exploitation depuis le dossier. S'il est prévu de déployer des images sur une grande quantité d'appareils de l'entreprise, il est conseillé de placer le dossier partagé sur une ressource de fichiers spéciale.

Indication de l'adresse du Serveur d'administration

Lors de l'installation du Serveur d'administration, vous pouvez indiquer l'adresse du Serveur d'administration. Cette adresse est utilisée par défaut lors de la création des paquets d'installation de l'Agent d'administration.

Comme adresse du Serveur d'administration, vous pouvez spécifier :

- Nom NetBIOS du Serveur d'administration, spécifié par défaut
- Nom de domaine complet (FQDN) du Serveur d'administration si le système de noms de domaine (DNS) sur le réseau de l'organisation a été configuré et fonctionne correctement
- Adresse externe si le Serveur d'administration est installé dans la zone démilitarisée (DMZ)

L'adresse du Serveur d'administration peut est modifiable par la suite à l'aide des outils de la Console d'administration, toutefois dans ce cas elle n'est pas modifiée automatiquement dans les paquets d'installation de l'Agent d'administration déjà créés.

Installation standard

L'installation standard désigne l'installation du Serveur d'administration qui utilise les chemins d'accès par défaut pour les fichiers de l'application, qui installe la sélection par défaut de plug-ins et qui n'active pas l'administration des appareils mobiles.

Pour installer le Serveur d'administration de Kaspersky Security Center sur un appareil local,

Lancez le fichier exécutable ksc_<version number>.<build number>_full_<localization language>.exe.

La fenêtre de sélection des applications Kaspersky s'ouvre pour l'installation. Dans la fenêtre de sélection de l'application, cliquez sur le lien **Installer le Serveur d'administration de Kaspersky Security Center** pour lancer l'Assistant d'installation du Serveur d'administration. Suivez les instructions de l'assistant.

Étape 1. Lecture du Contrat de licence utilisateur final et de la Politique de confidentialité

Cette étape de l'Assistant d'installation requiert la prise de connaissance du Contrat de licence utilisateur final conclu entre vous et AO Kaspersky et Politique de confidentialité.

Vous pouvez être invités à prendre connaissance des Contrats de licence utilisateur final et des Politiques de confidentialité des plug-ins d'administration des applications, inclus dans la distribution de Kaspersky Security Center.

Lisez attentivement le Contrat de licence utilisateur final conclu entre vous et Kaspersky, ainsi que la Politique de confidentialité. Si vous acceptez tous les termes du Contrat de licence et de la Politique de confidentialité, confirmez-le en cochant les cases appropriées.

L'installation de l'application se poursuit après que vous avez coché les deux cases.

Si vous n'êtes pas d'accord avec le Contrat de licence ou Politique de confidentialité, annulez l'installation en cliquant sur le bouton **Annuler**.

Étape 2. Sélection du type d'installation

Dans la fenêtre de sélection du type d'installation, choisissez le type **Standard**.

L'installation standard est recommandée si vous voulez découvrir l'application Kaspersky Security Center, par exemple, tester son fonctionnement sur un petit segment du réseau de votre société. Dans le cadre de l'installation standard, vous configurez uniquement les paramètres de la base de données. Les paramètres du Serveur d'administration ne se configurent pas : ils conservent les valeurs par défaut. L'installation standard ne permet pas de choisir les plug-ins d'administration à installer c'est la sélection de plug-ins par défaut qui est installée. Lors de l'installation standard, aucun paquet d'installation pour les appareils mobiles n'est créé. Vous pouvez toutefois les créer plus tard dans la Console d'administration.

Étape 3. Installation de Kaspersky Security Center Web Console

Cette étape s'affiche uniquement si vous utilisez un système d'exploitation de 64 bits. Sinon, cette étape ne s'affiche pas car Kaspersky Security Center Web Console ne fonctionne pas avec les systèmes d'exploitation de 32 bits.

Par défaut, Kaspersky Security Center Web Console et la Console d'administration basée sur MMC seront installées.

Si vous souhaitez installer uniquement Kaspersky Security Center Web Console :

1. Sélectionnez **Installer uniquement ceci**.
2. Choisissez **Console Web** dans la liste déroulante.

L'installation de Kaspersky Security Center Web Console démarre automatiquement une fois l'installation du Serveur d'administration terminée.

Si vous souhaitez installer uniquement la Console d'administration basée sur MMC :

1. Sélectionnez **Installer uniquement ceci**.
2. Choisissez **Console basée sur MMC** dans la liste déroulante.

Étape 4. Sélection de la taille du réseau

Indiquez la taille du réseau à installer Kaspersky Security Center. En fonction du nombre d'appareils sur le réseau, l'Assistant configure les paramètres d'installation et l'affichage de l'interface de l'application pour qu'ils correspondent.

Le tableau ci-dessous énumère les paramètres d'installation de l'application et d'affichage de l'interface lors de la sélection des tailles différentes du réseau.

Dépendance des paramètres d'installation de la sélection des tailles du réseau

Paramètres	1–100 appareils administrés	101–1 000 appareils administrés	1 001–5 000 appareils administrés	Plus de 5 000 appareils administrés
Affichage avec l'entrée des Serveurs d'administration virtuels et secondaires et de tous les paramètres, liés avec les Serveurs virtuels et secondaires, dans l'arborescence de la console (uniquement disponible dans la Console d'administration basée sur MMC)	Absent	Absent	Présent	Présent
Affichage avec les sections **Sécurité** dans les fenêtres des propriétés du Serveur et des groupes d'administration (disponible uniquement dans la Console d'administration basée sur MMC)	Absent	Absent	Présent	Présent
Répartition aléatoire du lancement de la tâche de mise à jour sur les appareils client	Absent	Selon un intervalle de 5 minutes	Selon un intervalle de 10 minutes	Selon un intervalle de 10 minutes

Lors de la connexion du Serveur d'administration au serveur de la base de données MySQL 5.7 et SQL Express, il est déconseillé d'utiliser l'application pour administrer plus de 10 000 appareils. Pour le système de gestion de base de données MariaDB, le nombre maximal recommandé d'appareils administrés est de 20 000.

Étape 5. Sélection d'une base de données

À cette étape de l'Assistant, sélectionnez un des systèmes de gestion de base de données qui servira au stockage de la base de données du Serveur d'administration :

- **Microsoft SQL Server ou SQL Server Express**
- **MySQL ou MariaDB**
- **PostgreSQL ou Postgres Pro**

Il est recommandé d'installer le Serveur d'administration sur un serveur dédié au lieu d'un contrôleur de domaine. Toutefois, si vous installez Kaspersky Security Center sur un serveur qui joue le rôle du contrôleur de domaine en lecture seule (RODC), le serveur Microsoft SQL Server (SQL Express) ne doit pas être installé en local (sur le même appareil). Dans ce cas, nous vous recommandons d'installer Microsoft SQL Server (SQL Express) à distance (sur un autre appareil), ou, si vous devez installer le SGBD localement, d'utiliser MySQL, MariaDB ou PostgreSQL.

La structure de la base de données du Serveur d'administration est décrite dans le fichier klakdb.chm qui figure dans le dossier d'installation de l'application Kaspersky Security Center. Ce fichier est également disponible dans une archive sur le portail de Kaspersky : klakdb.zip.

Étape 6. Configuration des paramètres du serveur SQL

À cette étape de l'Assistant, définissez les paramètres de connexion suivants en fonction du système de gestion de base de données (SGBD) que vous avez sélectionné :

- Si vous avez sélectionné **Microsoft SQL Server ou SQL Server Express** à l'étape précédente :

  - Indiquez dans le champ **Nom de l'instance du serveur SQL** le nom du serveur SQL installé dans le réseau. Le bouton **Parcourir** permet d'ouvrir la liste de tous les serveurs SQL installés dans le réseau. Par défaut, le champ est vide.

    Si vous vous connectez au serveur SQL via un port personnalisé, indiquez avec le nom d'hôte du serveur SQL le numéro de port séparé par une virgule, par exemple :

    ```
    Serveur_SQL_nom_hôte,1433
    ```

    Si vous sécurisez la communication entre le Serveur d'administration et le serveur SQL à l'aide d'un certificat, indiquez dans le champ **Nom de l'instance du serveur SQL** le même nom d'hôte que celui utilisé lors de la génération du certificat. Si vous utilisez une instance nommée du serveur SQL, indiquez avec le nom d'hôte du serveur SQL le numéro de port séparé par une virgule, par exemple :

    ```
    Serveur_SQL_nom,1433
    ```

    Si vous utilisez plusieurs instances de serveurs SQL sur le même hôte, indiquez également le nom de l'instance séparé par une barre oblique arrière, par exemple :

    ```
    Serveur_SQL_nom\Serveur_SQL_nom_instance,1433
    ```

    Si un serveur SQL sur le réseau d'entreprise a la fonction Always On activée, spécifiez le nom de l'écouteur du groupe de disponibilité dans le champ **Nom de l'instance du serveur SQL**. Notez que le Serveur d'administration ne prend en charge que le mode de disponibilité de validation synchrone lorsque la fonction Always On est activée.

  - Indiquez dans le champ **Nom de la base de données** le nom de DBMS créé pour héberger les informations du Serveur d'administration. La valeur par défaut est égale à *KAV*.

  Si vous souhaitez installer à cette étape un serveur SQL sur l'appareil depuis lequel vous installez Kaspersky Security Center, il faut interrompre l'installation et la lancer à nouveau après l'installation du serveur SQL. Serveurs SQL pris en charge figurant dans les exigences du système.

  Si vous souhaitez installer le serveur SQL sur un appareil distant, il n'est pas nécessaire d'interrompre l'Assistant d'installation de Kaspersky Security Center. Installez le serveur SQL et reprenez l'installation de Kaspersky Security Center.

- Si vous avez sélectionné **MySQL ou MariaDB** à l'étape précédente :

  - Indiquez dans le champ **Nom de l'instance du serveur SQL** le nom de l'instance du SGBD. Par défaut, l'adresse IP utilisée est celle de l'appareil sur lequel Kaspersky Security Center est installé.

  - Indiquez dans le champ **Port** le port de connexion du Serveur d'administration au SGBD. Le numéro de port par défaut est 3306.

  - Indiquez dans le champ **Nom de la base de données** le nom de DBMS créé pour héberger les informations du Serveur d'administration. La valeur par défaut est égale à *KAV*.

- Si vous avez sélectionné **PostgreSQL ou Postgres Pro** à l'étape précédente :

  - Indiquez dans le champ **PostgreSQL ou Postgres Pro Server** le nom de l'instance du SGBD. Par défaut, l'adresse IP utilisée est celle de l'appareil sur lequel Kaspersky Security Center est installé.

- Indiquez dans le champ **Port** le port de connexion du Serveur d'administration au SGBD. Le numéro de port par défaut est 5432.

- Indiquez dans le champ **Nom de la base de données** le nom de DBMS créé pour héberger les informations du Serveur d'administration. La valeur par défaut est égale à *KAV*.

Étape 7. Sélection de la méthode d'authentification

Définissez la méthode d'authentification à utiliser lors de la connexion du Serveur d'administration au système de gestion de base de données.

Selon le SGBD sélectionné, vous pouvez sélectionner parmi les modes d'authentification suivants :

- Pour SQL Express ou Microsoft SQL Server, sélectionnez une des options suivantes :

  - **Mode d'authentification Microsoft Windows**. Dans ce cas lors de la vérification des privilèges le compte utilisateur sera utilisé pour le lancement du Serveur d'administration.

  - **Mode d'authentification du serveur SQL**. Le compte utilisateur indiqué dans la fenêtre sera utilisé dans le cas de sélection de ce mode. Remplissez les champs **Compte utilisateur** et **Mot de passe**.

    Pour voir le mot de passe saisi, maintenez le bouton **Afficher** enfoncé.

  Dans les deux modes d'authentification, l'application vérifie si la base de données est disponible. Si la base de données n'est pas disponible, un message d'erreur s'affiche et vous devez saisir les identifiants corrects.

  Si la base de données du Serveur d'administration se trouve sur un autre appareil et le compte utilisateur du Serveur d'administration n'a pas l'accès au serveur de la base de données, il faut utiliser le mode d'authentification du serveur SQL lors de l'installation ou de la mise à jour du Serveur d'administration. Cela peut se produire lorsque l'appareil avec la base de données ne se trouve pas dans le domaine ou si le Serveur d'administration est installé sous le compte LocalSystem.

- Pour MySQL, MariaDB, PostgreSQL ou Postgres Pro, indiquez le compte et le mot de passe.

Étape 8. Décompression et installation des fichiers sur le disque dur

A la fin de la configuration des paramètres d'installation des modules de Kaspersky Security Center, vous pouvez lancer l'installation des fichiers sur le disque dur.

Si les applications supplémentaires sont nécessaires pour lancer l'installation, l'Assistant d'installation vous en notifiera avant l'installation de Kaspersky Security Center sur la page **Installation des modules nécessaires**. Les applications nécessaires seront automatiquement installées après avoir cliqué sur le bouton **Suivant**.

Sur la dernière page, vous pouvez sélectionner la console à démarrer pour utiliser Kaspersky Security Center :

- **Lancer la Console d'administration basée sur MMC**

- **Démarrer Kaspersky Security Center Web Console**

  Cette option est disponible uniquement si vous avez choisi d'installer Kaspersky Security Center Web Console à l'une des étapes précédentes.

Vous pouvez aussi cliquer sur **Terminer** pour quitter l'assistant sans commencer à utiliser Kaspersky Security Center. Vous pouvez commencer à travailler plus tard, à tout moment.

Vous pouvez réaliser la configuration initiale de l'application au premier lancement de la Console d'administration ou de Kaspersky Security Center Web Console.

A la fin du fonctionnement de l'Assistant d'installation, les modules suivants de l'application sont installés sur le disque dur avec le système d'exploitation installé :

- Serveur d'administration (avec la version serveur de l'Agent d'administration)
- Console d'administration basée sur la console de gestion Microsoft
- Kaspersky Security Center Web Console (si vous avez choisi de l'installer)
- Plug-ins d'administration des applications accessibles dans le paquet d'installation

De plus, l'application Microsoft Windows Installer version 4.5 sera installé si cette application n'a pas été installée auparavant.

Installation personnalisée

L'installation personnalisée est une installation du Serveur d'administration dans le cadre de laquelle vous pouvez choisir les modules à installer ainsi que le dossier d'installation de l'application.

A l'aide de ce type d'installation, vous pouvez configurer les paramètres de la base de données, les paramètres du Serveur d'administration, installer les modules qui ne sont pas compris dans l'installation standard et les plug-ins d'administration des applications de sécurité de Kaspersky. Vous pouvez également activer l'administration des appareils mobiles.

Pour installer le Serveur d'administration de Kaspersky Security Center sur un appareil local,

Lancez le fichier exécutable ksc_<version number>.<build number>_full_<localization language>.exe.

La fenêtre de sélection des applications Kaspersky s'ouvre pour l'installation. Dans la fenêtre de sélection de l'application, cliquez sur le lien **Installer le Serveur d'administration de Kaspersky Security Center** pour lancer l'Assistant d'installation du Serveur d'administration. Suivez les instructions de l'assistant.

Étape 1. Lecture du Contrat de licence utilisateur final et de la Politique de confidentialité

Cette étape de l'Assistant d'installation requiert la prise de connaissance du Contrat de licence utilisateur final conclu entre vous et AO Kaspersky et Politique de confidentialité.

Vous pouvez être invités à prendre connaissance des Contrats de licence utilisateur final et des Politiques de confidentialité des plug-ins d'administration des applications, inclus dans la distribution de Kaspersky Security Center.

Lisez attentivement le Contrat de licence utilisateur final conclu entre vous et Kaspersky, ainsi que la Politique de confidentialité. Si vous acceptez tous les termes du Contrat de licence et de la Politique de confidentialité, confirmez-le en cochant les cases appropriées.

L'installation de l'application se poursuit après que vous avez coché les deux cases.

Si vous n'êtes pas d'accord avec le Contrat de licence ou Politique de confidentialité, annulez l'installation en cliquant sur le bouton **Annuler**.

Étape 2. Sélection du type d'installation

Dans la fenêtre de sélection du type d'installation, choisissez le type **Personnalisée**.

L'installation personnalisée permet de configurer les paramètres de Kaspersky Security Center, comme le chemin du dossier en accès public, les comptes utilisateurs et les ports de connexion au Serveur d'administration, ainsi que les paramètres de la base de données. L'installation personnalisée permet de désigner les plug-ins d'administration des applications de Kaspersky à installer. Dans le cadre de l'installation personnalisée, vous pouvez créer des paquets d'installation pour appareils mobiles en désignant l'option correspondante.

Étape 3. Sélection des modules pour l'installation

Sélectionnez les modules du Serveur d'administration de Kaspersky Security Center que vous voulez installer :

- **Administration des appareils mobiles**. Cochez cette case s'il faut créer des paquets d'installation pour les appareils mobiles lors de l'exécution de l'Assistant d'installation de Kaspersky Security Center. Vous pouvez aussi créer des paquets d'installation pour les appareils mobiles manuellement à l'aide des outils de la Console d'administration, une fois le Serveur d'administration installé.

- **Agent SNMP**. Reçoit les statistiques pour le Serveur d'administration via le protocole SNMP. Le module est accessible lors de l'installation de l'application sur un appareil doté du module SNMP.

  > Après avoir installé Kaspersky Security Center, les fichiers .mib, nécessaires à l'obtention des données statistiques, seront situés dans le dossier d'installation de l'application dans le sous-dossier SNMP.

Les modules Agent d'administration et Console d'administration ne s'affichent pas dans la liste des modules. Ces modules s'installent automatiquement, il est impossible d'annuler leur installation.

A cette étape de l'Assistant, il faut aussi indiquer le dossier pour installer les modules du Serveur d'administration. Par défaut, les modules s'installent dans le dossier <Disk>:\Program Files\Kaspersky Lab\Kaspersky Security Center. Si le dossier avec ce nom n'existe pas, il sera automatiquement créé pendant l'installation. Vous pouvez modifier le dossier de destination à l'aide du bouton **Parcourir**.

Étape 4. Installation de Kaspersky Security Center Web Console

> Cette étape s'affiche uniquement si vous utilisez un système d'exploitation de 64 bits. Sinon, cette étape ne s'affiche pas car Kaspersky Security Center Web Console ne fonctionne pas avec les systèmes d'exploitation de 32 bits.

Par défaut, Kaspersky Security Center Web Console et la Console d'administration basée sur MMC seront installées.

Si vous souhaitez installer uniquement Kaspersky Security Center Web Console :

1. Sélectionnez **Installer uniquement ceci**.
2. Choisissez **Console Web** dans la liste déroulante.

L'installation de Kaspersky Security Center Web Console démarre automatiquement une fois l'installation du Serveur d'administration terminée.

Si vous souhaitez installer uniquement la Console d'administration basée sur MMC :

1. Sélectionnez **Installer uniquement ceci**.
2. Choisissez **Console basée sur MMC** dans la liste déroulante.

Étape 5. Sélection de la taille du réseau

Indiquez la taille du réseau à installer Kaspersky Security Center. En fonction du nombre d'appareils sur le réseau, l'Assistant configure les paramètres d'installation et l'affichage de l'interface de l'application pour qu'ils correspondent.

Le tableau ci-dessous énumère les paramètres d'installation de l'application et d'affichage de l'interface lors de la sélection des tailles différentes du réseau.

Dépendance des paramètres d'installation de la sélection des tailles du réseau

Paramètres	1–100 appareils administrés	101–1 000 appareils administrés	1 001–5 000 appareils administrés	Plus de 5 000 appareils administrés
Affichage avec l'entrée des Serveurs d'administration virtuels et secondaires et de tous les paramètres, liés avec les Serveurs virtuels et secondaires, dans l'arborescence de la console (uniquement disponible dans la Console d'administration basée sur MMC)	Absent	Absent	Présent	Présent
Affichage avec les sections **Sécurité** dans les fenêtres des propriétés du Serveur et des groupes d'administration (disponible uniquement dans la Console d'administration basée sur MMC)	Absent	Absent	Présent	Présent
Répartition aléatoire du lancement de la tâche de mise à jour sur les appareils client	Absent	Selon un intervalle de 5 minutes	Selon un intervalle de 10 minutes	Selon un intervalle de 10 minutes

Lors de la connexion du Serveur d'administration au serveur de la base de données MySQL 5.7 et SQL Express, il est déconseillé d'utiliser l'application pour administrer plus de 10 000 appareils. Pour le système de gestion de base de données MariaDB, le nombre maximal recommandé d'appareils administrés est de 20 000.

Étape 6. Sélection d'une base de données

À cette étape de l'Assistant, sélectionnez un des systèmes de gestion de base de données qui servira au stockage de la base de données du Serveur d'administration :

- **Microsoft SQL Server ou SQL Server Express**
- **MySQL ou MariaDB**
- **PostgreSQL ou Postgres Pro**

Il est recommandé d'installer le Serveur d'administration sur un serveur dédié au lieu d'un contrôleur de domaine. Toutefois, si vous installez Kaspersky Security Center sur un serveur qui joue le rôle du contrôleur de domaine en lecture seule (RODC), le serveur Microsoft SQL Server (SQL Express) ne doit pas être installé en local (sur le même appareil). Dans ce cas, nous vous recommandons d'installer Microsoft SQL Server (SQL Express) à distance (sur un autre appareil), ou, si vous devez installer le SGBD localement, d'utiliser MySQL, MariaDB ou PostgreSQL.

La structure de la base de données du Serveur d'administration est décrite dans le fichier klakdb.chm qui figure dans le dossier d'installation de l'application Kaspersky Security Center. Ce fichier est également disponible dans une archive sur le portail de Kaspersky : klakdb.zip.

Étape 7. Configuration des paramètres du serveur SQL

À cette étape de l'Assistant, définissez les paramètres de connexion suivants en fonction du système de gestion de base de données (SGBD) que vous avez sélectionné :

- Si vous avez sélectionné **Microsoft SQL Server ou SQL Server Express** à l'étape précédente :

  - Indiquez dans le champ **Nom de l'instance du serveur SQL** le nom du serveur SQL installé dans le réseau. Le bouton **Parcourir** permet d'ouvrir la liste de tous les serveurs SQL installés dans le réseau. Par défaut, le champ est vide.

    Si vous vous connectez au serveur SQL via un port personnalisé, indiquez avec le nom d'hôte du serveur SQL le numéro de port séparé par une virgule, par exemple :

    ```
    Serveur_SQL_nom_hôte,1433
    ```

    Si vous sécurisez la communication entre le Serveur d'administration et le serveur SQL à l'aide d'un certificat, indiquez dans le champ **Nom de l'instance du serveur SQL** le même nom d'hôte que celui utilisé lors de la génération du certificat. Si vous utilisez une instance nommée du serveur SQL, indiquez avec le nom d'hôte du serveur SQL le numéro de port séparé par une virgule, par exemple :

    ```
    Serveur_SQL_nom,1433
    ```

    Si vous utilisez plusieurs instances de serveurs SQL sur le même hôte, indiquez également le nom de l'instance séparé par une barre oblique arrière, par exemple :

    ```
    Serveur_SQL_nom\Serveur_SQL_nom_instance,1433
    ```

    Si un serveur SQL sur le réseau d'entreprise a la fonction Always On activée, spécifiez le nom de l'écouteur du groupe de disponibilité dans le champ **Nom de l'instance du serveur SQL**. Notez que le Serveur d'administration ne prend en charge que le mode de disponibilité de validation synchrone lorsque la fonction Always On est activée.

  - Indiquez dans le champ **Nom de la base de données** le nom de DBMS créé pour héberger les informations du Serveur d'administration. La valeur par défaut est égale à *KAV*.

  Si vous souhaitez installer à cette étape un serveur SQL sur l'appareil depuis lequel vous installez Kaspersky Security Center, il faut interrompre l'installation et la lancer à nouveau après l'installation du serveur SQL. Serveurs SQL pris en charge figurant dans les exigences du système.

  Si vous souhaitez installer le serveur SQL sur un appareil distant, il n'est pas nécessaire d'interrompre l'Assistant d'installation de Kaspersky Security Center. Installez le serveur SQL et reprenez l'installation de Kaspersky Security Center.

- Si vous avez sélectionné **MySQL ou MariaDB** à l'étape précédente :

  - Indiquez dans le champ **Nom de l'instance du serveur SQL** le nom de l'instance du SGBD. Par défaut, l'adresse IP utilisée est celle de l'appareil sur lequel Kaspersky Security Center est installé.

  - Indiquez dans le champ **Port** le port de connexion du Serveur d'administration au SGBD. Le numéro de port par défaut est 3306.

  - Indiquez dans le champ **Nom de la base de données** le nom de DBMS créé pour héberger les informations du Serveur d'administration. La valeur par défaut est égale à *KAV*.

- Si vous avez sélectionné **PostgreSQL ou Postgres Pro** à l'étape précédente :

  - Indiquez dans le champ **PostgreSQL ou Postgres Pro Server** le nom de l'instance du SGBD. Par défaut, l'adresse IP utilisée est celle de l'appareil sur lequel Kaspersky Security Center est installé.

- Indiquez dans le champ **Port** le port de connexion du Serveur d'administration au SGBD. Le numéro de port par défaut est 5432.

- Indiquez dans le champ **Nom de la base de données** le nom de DBMS créé pour héberger les informations du Serveur d'administration. La valeur par défaut est égale à *KAV*.

Étape 8. Sélection de la méthode d'authentification

Définissez la méthode d'authentification à utiliser lors de la connexion du Serveur d'administration au système de gestion de base de données.

Selon le SGBD sélectionné, vous pouvez sélectionner parmi les modes d'authentification suivants :

- Pour SQL Express ou Microsoft SQL Server, sélectionnez une des options suivantes :

  - **Mode d'authentification Microsoft Windows**. Dans ce cas lors de la vérification des privilèges le compte utilisateur sera utilisé pour le lancement du Serveur d'administration.

  - **Mode d'authentification du serveur SQL**. Le compte utilisateur indiqué dans la fenêtre sera utilisé dans le cas de sélection de ce mode. Remplissez les champs **Compte utilisateur** et **Mot de passe**.

    Pour voir le mot de passe saisi, maintenez le bouton **Afficher** enfoncé.

  Dans les deux modes d'authentification, l'application vérifie si la base de données est disponible. Si la base de données n'est pas disponible, un message d'erreur s'affiche et vous devez saisir les identifiants corrects.

  Si la base de données du Serveur d'administration se trouve sur un autre appareil et le compte utilisateur du Serveur d'administration n'a pas l'accès au serveur de la base de données, il faut utiliser le mode d'authentification du serveur SQL lors de l'installation ou de la mise à jour du Serveur d'administration. Cela peut se produire lorsque l'appareil avec la base de données ne se trouve pas dans le domaine ou si le Serveur d'administration est installé sous le compte LocalSystem.

- Pour MySQL, MariaDB, PostgreSQL ou Postgres Pro, indiquez le compte et le mot de passe.

Étape 9. Sélection du compte utilisateur pour lancer le Serveur d'administration

Choisissez le compte utilisateur sous lequel le Serveur d'administration va être lancé en tant que service.

- **Créer un compte utilisateur automatiquement**. Le programme crée le compte utilisateur local KL-AK-*, sous lequel le service du Serveur d'administration kladminserver sera exécuté.

  Vous pouvez sélectionner cette option, si vous envisagez de placer le dossier partagé et le SGBD sur le même appareil que le Serveur d'administration.

- **Sélectionner un compte utilisateur**. Le service du Serveur d'administration (kladminserver) sera lancé sous le compte utilisateur que vous avez sélectionné.

  Il vous faudra sélectionner un compte utilisateur de domaine si, par exemple, vous envisagez d'utiliser en tant que SGBD un serveur SQL, quelle que soit sa version, y compris SQL-express, situé sur un autre appareil, et / ou si vous envisagez de placer le dossier partagé sur un autre appareil.

  Kaspersky Security Center est compatible avec les comptes de service administrés (MSA) et les comptes de service administrés de groupe (gMSA). Si ces comptes utilisateurs sont utilisés dans votre domaine, vous pouvez en choisir un comme compte pour le service du Serveur d'administration.

  Avant de définir MSA ou gMSA, vous devez installer le compte sur le même appareil que celui sur lequel vous souhaitez installer le Serveur d'administration. Si le compte n'est pas encore installé, annulez l'installation du Serveur d'administration, installez le compte, puis redémarrez l'installation du Serveur d'administration. Pour plus de détails sur l'installation des comptes de services administrés sur un appareil local, consultez la documentation officielle de Microsoft.

  Pour définir MSA ou gMSA :

  1. Cliquez sur le bouton **Parcourir**.
  2. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Type d'objet**.
  3. Sélectionnez le type **Compte utilisateur pour les services**, puis cliquez sur **OK**.
  4. Sélectionnez le compte utilisateur nécessaire et cliquez sur le bouton **OK**.

Le compte utilisateur que vous avez sélectionné doit disposer de droits différents en fonction du SGBD que vous prévoyez d'utiliser.

Pour des raisons de sécurité, ne faites pas du compte utilisateur sous lequel est exécuté le Serveur d'administration un compte privilégié.

Le compte du Serveur d'administration ne peut pas être modifié ultérieurement. Vous devez réinstaller le cluster de basculement pour utiliser un autre compte de Serveur d'administration.

Étape 10. Sélection du compte utilisateur pour lancer les services de Kaspersky Security Center

Choisissez le compte utilisateur sous lequel les services de Kaspersky Security Center vont être lancés sur cet appareil :

- **Créer un compte utilisateur automatiquement**. Kaspersky Security Center crée le compte utilisateur local KlScSvc sur cet appareil dans le groupe kladmins. Les services du Kaspersky Security Center se lanceront sous le compte utilisateur créé.

- **Sélectionner un compte utilisateur**. Les services de Kaspersky Security Center se lanceront sous le compte utilisateur que vous avez sélectionné.

  Il vous faudra choisir un compte utilisateur de domaine si, par exemple, vous envisagez de conserver les rapports dans un dossier situé sur un autre appareil, ou si cela est exigé par la stratégie de sécurité de votre organisation. Il peut également être nécessaire de choisir le compte utilisateur de domaine lors de l'installation du Serveur d'administration sur un cluster haute disponibilité.

Pour des raisons de sécurité, ne faites pas du compte utilisateur sous lequel sont lancés les services un compte privilégié.

Le compte utilisateur sélectionné servira à lancer le service KSN proxy (ksnproxy), le service du serveur proxy d'activation de Kaspersky (klactprx) et le service du portail d'authentification de Kaspersky (klwebsrv).

Étape 11. Définition du dossier partagé

Définissez le placement et le nom du dossier public, qui sera utilisé pour :

- La sauvegarde des fichiers pour l'installation à distance des applications (les fichiers sont copiés sur le Serveur d'administration lors de la création des paquets d'installation).

- Le stockage des mises à jour téléchargées depuis la source des mises à jour sur le Serveur d'administration.

L'accès public pour la lecture pour tous les utilisateurs sera ouvert à cette ressource.

Choisissez l'une des deux options suivantes :

- **Créer un dossier partagé**. Création du nouveau dossier. Indiquez le chemin d'accès au dossier dans le champ ci-après.

- **Sélectionner un dossier partagé existant**. La sélection du dossier partagé parmi les dossiers déjà existants.

Le dossier partagé peut être local sur l'appareil d'où l'installation a été réalisée ou distant sur n'importe lequel des appareils clients qui appartiennent au réseau de la société. Vous pouvez indiquer le dossier partagé à l'aide du bouton **Parcourir**, aussi que manuellement, en saisissant le chemin UNC dans le champ correspondant (par exemple, \\server\Share).

Le sous-dossier local KLSHARE est créé par défaut dans le dossier de l'application contenant des modules de Kaspersky Security Center.

Vous pouvez définir un dossier partagé ultérieurement si nécessaire.

Étape 12. Configuration des paramètres de connexion au Serveur d'administration

Configurez les paramètres de connexion au Serveur d'administration :

- **Port**

  Numéro de port utilisé pour se connecter au Serveur d'administration.

  Le numéro de port par défaut est 14000.

- **Port SSL**

  Numéro du port SSL : Affiche le numéro de port SSL utilisé pour établir une connexion sécurisée avec le Serveur d'administration.

  Le numéro de port par défaut est 13000.

- **Longueur de la clé de chiffrement**

  Choisissez la longueur de la clé de chiffrement : 1 024 ou 2 048 bits.

  Une clé de chiffrement de 1024 bits exerce une charge moins importante sur le processeur mais est considérée dépassée et, d'après ses caractéristiques techniques, peut ne pas assurer un chiffrement sûr. Il se peut également que l'équipement disponible ne soit pas compatible avec des certificats SSL qui utilisent une clé de 1 024 bits.

  Une clé de chiffrement de 2 048 bits répond aux standards modernes de chiffrement. Toutefois, l'utilisation d'une clé de chiffrement de 2 048 bits peut augmenter la charge sur le processeur.

  Par défaut, l'option **2048 bits (meilleure sécurité)** est sélectionnée.

Vous pouvez également modifier les paramètres de connexion ultérieure au Serveur d'administration comme suit :

- Vous pouvez modifier les numéros de port et les numéros de port SSL dans la section **Ports de connexion** des propriétés du Serveur d'administration. Pour en savoir plus sur les ports de connexion du Serveur d'administration, consultez la section Ports utilisés par Kaspersky Security Center.

- Vous pouvez modifier la longueur de la clé de chiffrement lors du remplacement du certificat du Serveur d'administration avec l'utilitaire klsetsrvcert en utilisant le paramètre `-o RsaKeyLen:<key length>`.

Étape 13. Définition de l'adresse du Serveur d'administration

Spécifiez l'adresse du Serveur d'administration de l'une des manières suivantes :

- **Nom du domaine DNS**. Vous pouvez utiliser cette méthode si le réseau comprend un serveur DNS et que les appareils clients peuvent l'utiliser pour recevoir l'adresse du Serveur d'administration.
- **Nom NetBIOS**. Vous pouvez utiliser cette méthode si les appareils clients reçoivent l'adresse du Serveur d'administration via le protocole NetBIOS ou si un serveur WINS est disponible sur le réseau.
- **Adresse IP**. Vous pouvez utiliser cette méthode si le Serveur d'administration possède une adresse IP statique qui ne sera pas modifiée par la suite.

Si vous installez Kaspersky Security Center sur le nœud actif du cluster de basculement Kaspersky Security Center et que vous avez créé un adaptateur réseau secondaire lors de la préparation des nœuds du cluster, indiquez l'adresse IP de cet adaptateur. Dans le cas contraire, saisissez l'adresse IP du répartiteur de charge tiers que vous utilisez.

Étape 14. Adresse du Serveur d'administration pour la connexion des appareils mobiles

Cette étape de l'Assistant d'installation est disponible au cas où vous auriez sélectionné Administration des appareils mobiles à installer.

Dans la fenêtre **Adresse pour la connexion des appareils mobiles**, indiquez l'adresse externe du Serveur d'administration pour la connexion des appareils mobiles qui se trouvent en dehors du réseau local. Vous pouvez spécifier l'adresse IP ou le système de nom de domaine (DNS) du Serveur d'administration.

Étape 15. Sélection des plug-ins d'administration des applications

Sélectionnez les plug-ins d'administration des applications Kaspersky qui requièrent l'installation conjointement avec Kaspersky Security Center.

Pour simplifier la recherche, les plug-ins sont organisés en groupes en fonction du type d'objet protégé.

Étape 16. Décompression et installation des fichiers sur le disque dur

A la fin de la configuration des paramètres d'installation des modules de Kaspersky Security Center, vous pouvez lancer l'installation des fichiers sur le disque dur.

Si les applications supplémentaires sont nécessaires pour lancer l'installation, l'Assistant d'installation vous en notifiera avant l'installation de Kaspersky Security Center sur la page **Installation des modules nécessaires**. Les applications nécessaires seront automatiquement installées après avoir cliqué sur le bouton **Suivant**.

Sur la dernière page, vous pouvez sélectionner la console à démarrer pour utiliser Kaspersky Security Center :

- **Lancer la Console d'administration basée sur MMC**
- **Démarrer Kaspersky Security Center Web Console**

  Cette option est disponible uniquement si vous avez choisi d'installer Kaspersky Security Center Web Console à l'une des étapes précédentes.

Vous pouvez aussi cliquer sur **Terminer** pour quitter l'assistant sans commencer à utiliser Kaspersky Security Center. Vous pouvez commencer à travailler plus tard, à tout moment.

Vous pouvez réaliser la configuration initiale de l'application au premier lancement de la Console d'administration ou de Kaspersky Security Center Web Console.

Déploiement du cluster de basculement Kaspersky Security Center

Cette section contient à la fois des informations générales à propos du cluster de basculement Kaspersky Security Center, et des instructions à propos de la préparation et du déploiement du cluster de basculement Kaspersky Security Center sur votre réseau.

Scénario : Déploiement du cluster de basculement Kaspersky Security Center

Un cluster de basculement Kaspersky Security Center assure la haute disponibilité de Kaspersky Security Center et minimise les temps d'arrêt du Serveur d'administration en cas de panne. Le cluster de basculement repose sur deux instances identiques de Kaspersky Security Center installées sur deux ordinateurs. L'une des instances fonctionne comme un nœud actif et l'autre est un nœud passif. Le nœud actif gère la protection des appareils clients, tandis que le nœud passif est prêt à assumer toutes les fonctions du nœud actif en cas de panne du nœud actif. Lorsqu'une panne se produit, le nœud passif devient actif et le nœud actif devient passif.

Prérequis

Vous disposez d'un matériel conforme aux conditions requises pour le cluster de basculement.

Étapes

Le déploiement des applications Kaspersky se déroule par étapes :

1. **Création d'un compte pour les services Kaspersky Security Center**

   Créez un nouveau groupe de domaine, (dans ce scénario, le nom « KLAdmins » est utilisé pour ce groupe) puis accordez les autorisations de l'administrateur local au groupe sur les deux nœuds et sur le serveur de fichiers. Créez ensuite deux nouveaux comptes utilisateur de domaine (dans ce scénario, les noms « ksc » et « rightless » sont utilisés pour ces comptes), puis ajoutez les comptes au groupe de domaine KLAdmins.

   Ajoutez le compte utilisateur sous lequel Kaspersky Security Center sera installé au groupe de domaine KLAdmins créé auparavant.

2. **Préparation du serveur de fichiers**

   Préparez le serveur de fichiers de manière à ce qu'il fonctionne en tant que composant du cluster de basculement Kaspersky Security Center. Assurez-vous que le serveur de fichiers répond aux exigences matérielles et logicielles, créez deux dossiers partagés pour les données de Kaspersky Security Center et configurez les autorisations pour accéder aux dossiers partagés.

   Instructions pratiques : Préparation d'un serveur de fichiers pour le cluster de basculement Kaspersky Security Center

3. **Préparation des nœuds actifs et passifs**

   Préparez deux appareils présentant des caractéristiques matérielles et logicielles identiques pour qu'ils fonctionnent en tant que nœuds actif et passif.

   Instructions pratiques : Préparation des nœuds pour le cluster de basculement Kaspersky Security Center

4. **Installation du Système de gestion de base de données (SGBD)**

   Sélectionnez l'un des SGBD pris en charge, puis installez le SGBD sur un appareil dédié. Pour en savoir plus sur l'installation du SGBD, consultez sa documentation.

5. **Installation de Kaspersky Security Center**

   Installez Kaspersky Security Center en mode cluster de basculement sur les deux nœuds. Vous devez d'abord installer Kaspersky Security Center sur l'appareil que vous souhaitez utiliser comme hôte actif, puis l'installer sur l'hôte passif.

   Vous devez installer Kaspersky Security Center Web Console sur un appareil distinct qui n'est pas un nœud de cluster.

   Instructions pratiques : Installation de Kaspersky Security Center sur les nœuds du cluster de basculement Kaspersky Security Center

6. **Test du cluster de basculement**

   Vérifiez que vous avez correctement configuré le cluster de basculement et qu'il fonctionne correctement. Par exemple, vous pouvez arrêter l'un des services de Kaspersky Security Center sur le nœud actif : kladminserver, klnagent, ksnproxy, klactprx ou klwebsrv. Après l'arrêt du service, la gestion de la protection doit être automatiquement basculée vers le nœud passif.

Résultats

Le cluster de basculement Kaspersky Security Center est déployé. Veuillez vous familiariser avec les événements qui conduisent au basculement entre les nœuds actifs et passifs.

À propos du cluster de basculement Kaspersky Security Center

Un cluster de basculement Kaspersky Security Center assure la haute disponibilité de Kaspersky Security Center et minimise les temps d'arrêt du Serveur d'administration en cas de panne. Le cluster de basculement repose sur deux instances identiques de Kaspersky Security Center installées sur deux ordinateurs. L'une des instances fonctionne comme un nœud actif et l'autre est un nœud passif. Le nœud actif gère la protection des appareils clients, tandis que le nœud passif est prêt à assumer toutes les fonctions du nœud actif en cas de panne du nœud actif. Lorsqu'une panne se produit, le nœud passif devient actif et le nœud actif devient passif.

L'utilisation du cluster de basculement est sans incidence sur les calculs basés sur le guide de dimensionnement.

Utilisez la fonctionnalité Journal des événements Kaspersky pour le dépannage.

Conditions de basculement

Le cluster de basculement bascule la gestion de la protection des appareils clients du nœud actif au nœud passif si l'un des événements suivants se produit sur le nœud actif :

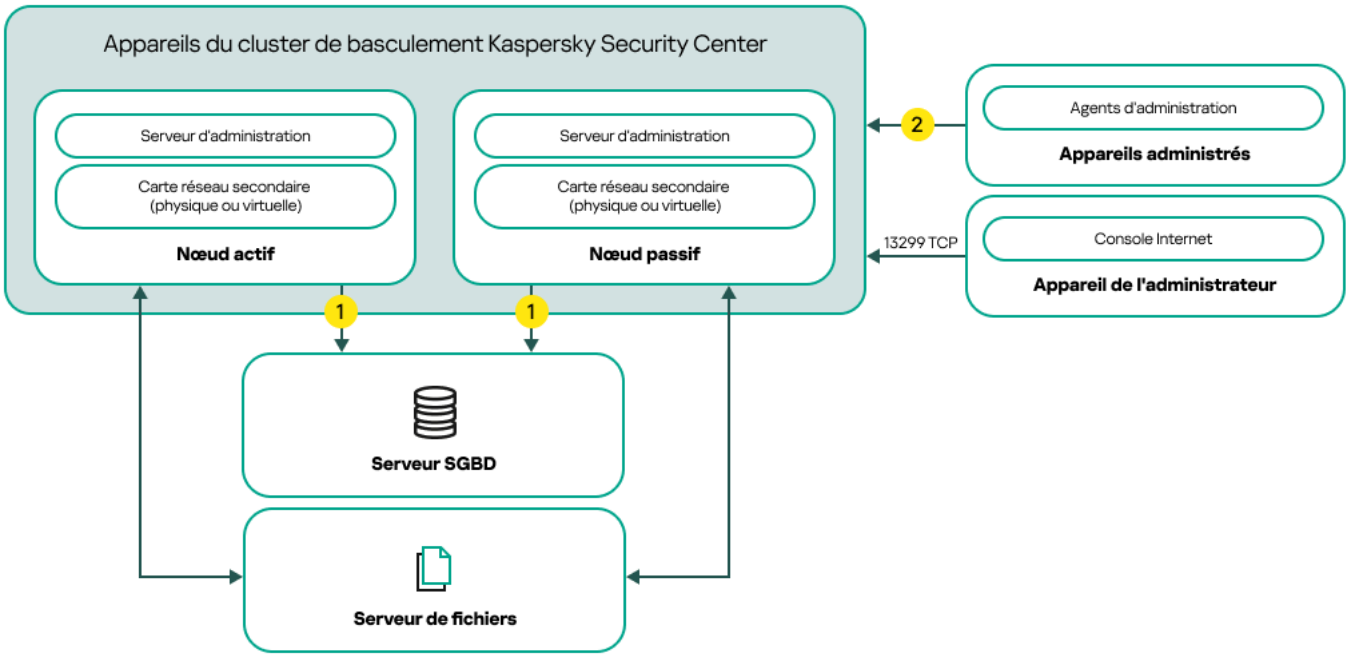
- Le nœud actif tombe en panne en raison d'une défaillance logicielle ou matérielle.
- Le nœud actif a été temporairement arrêté dans le cadre d'activités de maintenance.
- Au moins un des services (ou processus) de Kaspersky Security Center a échoué ou a été délibérément interrompu par l'utilisateur. Les services de Kaspersky Security Center sont les suivants : kladminserver, klnagent, klactprx et klwebsrv.
- La connexion réseau entre le nœud actif et le stockage sur le serveur de fichiers a été interrompue ou arrêtée.

Le cluster de basculement de Kaspersky Security Center gère automatiquement tous les services de Kaspersky Security Center. Ne redémarrez pas les services manuellement.

Schémas de déploiement

Vous pouvez choisir l'un des schémas suivants pour déployer le cluster de basculement Kaspersky Security Center :

- Un schéma qui utilise une carte réseau secondaire.
- Un schéma qui utilise un équilibreur de charge tiers.

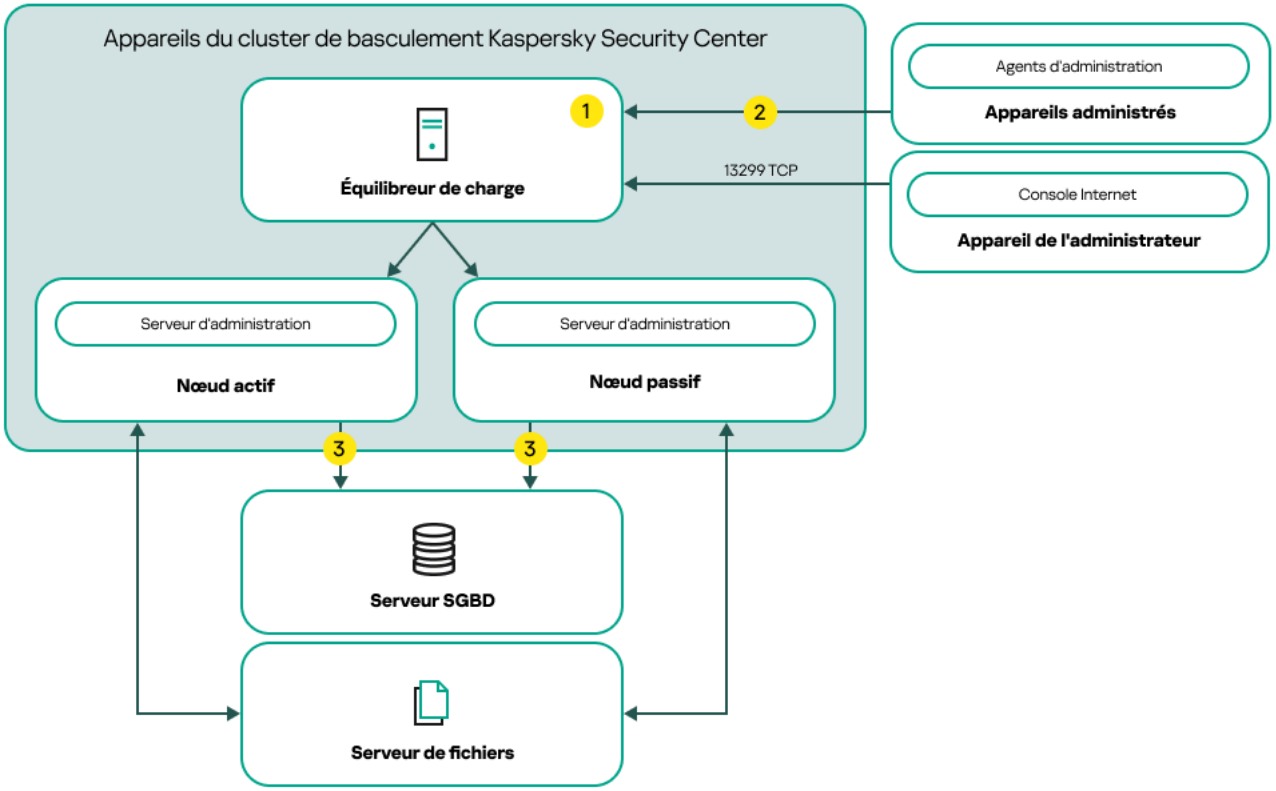


Un schéma qui utilise une carte réseau secondaire.

Légende du schéma :

1 Le Serveur d'administration envoie des données à la base de données. Ouvrez les ports nécessaires sur l'appareil où se trouve la base de données, par exemple, le port 3306 pour le serveur MySQL ou le port 1433 pour le serveur Microsoft SQL. Veuillez vous référer à la documentation du SGBD pour les informations pertinentes.

2 Sur les appareils administrés, ouvrez les ports suivants : TCP 13000, UDP 13000 et TCP 17000.



Un schéma qui utilise un équilibreur de charge tiers

Légende du schéma :

1 Sur l'équilibreur de charge, ouvrez tous les ports du Serveur d'administration : TCP 13000, UDP 13000, TCP 13299 et TCP 17000.

> Si vous souhaitez utiliser l'utilitaire klakaut pour l'automatisation, vous devez également ouvrir le port TCP 13291.

2 Sur les appareils administrés, ouvrez les ports suivants : TCP 13000, UDP 13000 et TCP 17000.

3 Le Serveur d'administration envoie des données à la base de données. Ouvrez les ports nécessaires sur l'appareil où se trouve la base de données, par exemple, le port 3306 pour le serveur MySQL ou le port 1433 pour le serveur Microsoft SQL. Veuillez vous référer à la documentation du SGBD pour les informations pertinentes.

Préparation d'un serveur de fichiers pour un cluster de basculement Kaspersky Security Center

Un serveur de fichiers fonctionne comme un module obligatoire d'un cluster de basculement Kaspersky Security Center.

Pour préparer un serveur de fichiers, procédez comme suit :

1. Assurez-vous que le serveur de fichiers est conforme à la configuration matérielle et logicielle.
2. Assurez-vous que le serveur de fichiers et les deux nœuds (actifs et passifs) sont inclus dans le même domaine ou que le serveur de fichiers est le contrôleur de domaine.

3. Sur le serveur de fichiers, créez deux dossiers partagés. L'un d'eux est utilisé pour conserver des informations sur l'état du cluster de basculement. L'autre est utilisé pour stocker les données et les paramètres de Kaspersky Security Center. Vous indiquerez les chemins d'accès aux dossiers partagés lors de la configuration de l'installation de Kaspersky Security Center.

4. Accordez des autorisations d'accès complet (à la fois des autorisations de partage et des autorisations NTFS) aux dossiers partagés créés pour les comptes utilisateurs et les groupes suivants :

   - Groupe de domaine KLAdmins.
   - Comptes utilisateurs $<nœud1> et $<nœud2>. Ici,<nœud1> et <nœud2> sont les noms d'appareil des nœuds actifs et passifs.

Le serveur de fichiers est préparé. Pour déployer le cluster de basculement Kaspersky Security Center, suivez les instructions supplémentaires de ce scénario.

Préparation des nœuds pour un cluster de basculement Kaspersky Security Center

Préparez deux appareils qui fonctionneront en tant que nœuds actifs et passifs pour un cluster de basculement Kaspersky Security Center.

Pour préparer des nœuds pour un cluster de basculement Kaspersky Security Center, procédez comme suit :

1. Assurez-vous que vous disposez de deux appareils répondant aux exigences matérielles et logicielles. Ces appareils agiront en tant que nœuds actifs et passifs du cluster de basculement.

2. Assurez-vous que le serveur de fichiers et les deux nœuds sont inclus dans le même domaine.

3. Exécutez une des actions suivantes :

   - Sur chacun des nœuds, configurez une carte réseau secondaire.

     Une carte réseau secondaire peut être physique ou virtuelle. Si vous souhaitez utiliser une carte réseau physique, connectez-vous et configurez-la à l'aide des outils standard du système d'exploitation. Si vous souhaitez utiliser une carte réseau virtuelle, créez-la à l'aide d'un logiciel tiers.

     Assurez-vous que les conditions suivantes sont remplies :

     - Les cartes réseau secondaires sont désactivées.

       Vous pouvez créer les adaptateurs réseau secondaires à l'état désactivé ou les désactiver après leur création.

     - Les adaptateurs réseau secondaires sur les deux nœuds présentent la même adresse IP.

   - Utilisez un répartiteur de charge tiers. Par exemple, vous pouvez utiliser un serveur nginx. Dans ce cas, procédez comme suit :

     a. Fournissez un appareil Linux dédié sur lequel un serveur nginx est installé.

     b. Configurez le répartiteur de charge. Définissez le nœud actif comme serveur principal et le nœud passif comme serveur de sauvegarde.

     c. Sur le serveur nginx, ouvrez tous les ports du Serveur d'administration : TCP 13000, UDP 13000, TCP 13299 et TCP 17000.

        Si vous souhaitez utiliser l'utilitaire klakaut pour l'automatisation, vous devez également ouvrir le port TCP 13291.

4. Redémarrez les deux nœuds ainsi que le serveur de fichiers.

5. Mappez, à chacun des nœuds, les deux dossiers partagés que vous avez créés lors de l'étape de préparation du serveur de fichiers. Vous devez mapper les dossiers partagés en tant que disques réseau. Lors du mappage des dossiers, vous pouvez sélectionner n'importe quelle lettre de disque vacante. Pour accéder aux dossiers partagés, utilisez les informations d'identification du compte utilisateur que vous avez créé lors de l'étape 1 du scénario.

Les nœuds sont préparés. Pour déployer le cluster de basculement Kaspersky Security Center, suivez les instructions supplémentaires du scénario.

Installation de Kaspersky Security Center sur les nœuds du cluster de basculement Kaspersky Security Center

Kaspersky Security Center est installé séparément sur les deux nœuds du cluster de basculement Kaspersky Security Center. Vous installez d'abord l'application sur le nœud actif, puis sur le nœud passif. Lors de l'installation, vous choisissez le nœud qui sera actif et celui qui sera passif.

Seul un utilisateur du groupe de domaine KLAdmins peut installer Kaspersky Security Center sur chaque nœud.

Pour installer Kaspersky Security Center sur le nœud actif du cluster de basculement Kaspersky Security Center, procédez comme suit :

1. Lancez le fichier exécutable sc_15.1_<build number>_full_<language>.exe.

   Une fenêtre s'ouvre et vous invite à sélectionner les applications Kaspersky à installer. Dans la fenêtre de sélection des applications, lancez l'Assistant d'installation du Serveur d'administration à l'aide du lien **Installer le Serveur d'administration de Kaspersky Security Center**. Suivez les instructions de l'assistant.

2. Lisez attentivement le Contrat de licence utilisateur final conclu entre vous et Kaspersky, ainsi que la Politique de confidentialité. Si vous acceptez toutes les dispositions du Contrat de licence utilisateur final et de la Politique de confidentialité, cochez les cases suivantes dans le groupe **Je confirme que j'ai lu, je comprends et j'accepte l'intégralité de ce qui suit** :

   - **Les termes et conditions de ce Contrat de licence utilisateur final**
   - **Politique de confidentialité décrivant le traitement des données**

   L'installation de l'application se poursuit après que vous avez coché les deux cases.

   Si vous n'êtes pas d'accord avec le Contrat de licence ou Politique de confidentialité, annulez l'installation en cliquant sur le bouton **Annuler**.

3. Sélectionnez **Nœud principal du cluster de basculement de Kaspersky Security Center** pour installer l'application sur le nœud actif.

4. Dans la fenêtre **Dossier partagé**, réalisez les opérations suivantes :

   - Dans les champs **Partage de l'état** et **Partage des données**, indiquez les chemins d'accès aux dossiers partagés que vous avez créés sur le serveur de fichiers lors de sa préparation.
   - Dans les champs **État de partage de données** et **Disque de partage de données**, sélectionnez les disques réseau auxquels vous avez mappé les dossiers partagés pendant la préparation des nœuds.
   - Sélectionnez le mode de connectivité du cluster : via un adaptateur réseau secondaire ou un répartiteur de charge tiers.

5. Effectuez les autres étapes de l'installation personnalisée, en commençant par l'étape 3.

   À l'étape 13, indiquez l'adresse IP d'un adaptateur réseau secondaire si vous avez créé un adaptateur lors de la préparation des nœuds du cluster. Dans le cas contraire, saisissez l'adresse IP du répartiteur de charge tiers que vous utilisez.

Kaspersky Security Center est installé sur le nœud actif.

Pour installer Kaspersky Security Center sur le nœud passif du cluster de basculement Kaspersky Security Center, procédez comme suit :

1. Lancez le fichier exécutable sc_15.1_<build number>_full_<language>.exe.

   Une fenêtre s'ouvre et vous invite à sélectionner les applications Kaspersky à installer. Dans la fenêtre de sélection des applications, lancez l'Assistant d'installation du Serveur d'administration à l'aide du lien **Installer le Serveur d'administration de Kaspersky Security Center**. Suivez les instructions de l'assistant.

2. Lisez attentivement le Contrat de licence utilisateur final conclu entre vous et Kaspersky, ainsi que la Politique de confidentialité. Si vous acceptez toutes les dispositions du Contrat de licence utilisateur final et de la Politique de confidentialité, cochez les cases suivantes dans le groupe **Je confirme que j'ai lu, je comprends et j'accepte l'intégralité de ce qui suit** :

   - **Les termes et conditions de ce Contrat de licence utilisateur final**
   - **Politique de confidentialité décrivant le traitement des données**

   L'installation de l'application se poursuit après que vous avez coché les deux cases.

   Si vous n'êtes pas d'accord avec le Contrat de licence ou Politique de confidentialité, annulez l'installation en cliquant sur le bouton **Annuler**.

3. Sélectionnez **Nœud secondaire du cluster de basculement de Kaspersky Security Center** pour installer l'application sur le nœud passif.

4. Dans la fenêtre **Dossier partagé**, dans le champ **Partage de l'état**, indiquez un chemin d'accès au dossier partagé avec des informations sur l'état du cluster que vous avez créé sur le serveur de fichiers au cours de sa préparation.

5. Cliquez sur le bouton **Installer**. Une fois l'installation terminée, cliquez sur le bouton **Terminer**.

Kaspersky Security Center est installé sur le nœud passif. Maintenant, vous pouvez tester le cluster de basculement Kaspersky Security Center pour vous assurer que vous l'avez correctement configuré et que le cluster fonctionne correctement.

Démarrage et arrêt manuels des nœuds de cluster

Vous devrez peut-être arrêter l'ensemble du cluster de basculement Kaspersky Security Center ou détacher temporairement l'un des nœuds du cluster à des fins de maintenance. Si tel est le cas, suivez les instructions de cette section. N'essayez pas de démarrer ni d'arrêter les services ou les processus liés au cluster de basculement d'une autre façon. Cette mesure pourrait entraîner une perte de données.

Démarrage et arrêt de l'ensemble du cluster de basculement à des fins de maintenance

Pour démarrer ou arrêter l'intégralité du cluster de basculement, procédez comme suit :

1. Sur le nœud actif, accédez à <Disque>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

2. Ouvrez la ligne de commande, puis exécutez l'une des commandes suivantes :

   - Pour arrêter le cluster, exécutez : `klfoc -stopcluster --stp klfoc`
   - Pour démarrer le cluster, exécutez : `klfoc -startcluster --stp klfoc`

Le cluster de basculement est démarré ou arrêté, selon la commande que vous exécutez.

Entretien de l'un des nœuds

Pour entretenir l'un des nœuds, procédez comme suit :

1. Sur le nœud actif, arrêtez le cluster de basculement à l'aide de la commande `klfoc -stopcluster --stp klfoc`.
2. Sur le nœud que vous souhaitez entretenir, accédez à <Disque>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.
3. Ouvrez la ligne de commande, puis détachez le nœud du cluster en exécutant la commande `detach_node.cmd`.
4. Sur le nœud actif, démarrez le cluster de basculement à l'aide de la commande `klfoc -startcluster --stp klfoc`.
5. Procédez à la maintenance.
6. Sur le nœud actif, arrêtez le cluster de basculement à l'aide de la commande `klfoc -stopcluster --stp klfoc`.
7. Sur le nœud qui a fait l'objet de la maintenance, accédez à <Disque>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.
8. Ouvrez la ligne de commande, puis attachez le nœud au cluster en exécutant la commande `attach_node.cmd`.
9. Sur le nœud actif, démarrez le cluster de basculement à l'aide de la commande `klfoc -startcluster --stp klfoc`.

Le nœud est entretenu et attaché au cluster de basculement.

Installation du Serveur d'administration sur un cluster de basculement Windows Server

La procédure d'installation du Serveur d'administration sur un cluster de basculement diffère de l'installation standard et de l'installation personnalisée sur un appareil autonome.

Suivez la procédure décrite dans cette section sur le nœud qui contient un stockage de données commun du cluster.

Pour installer le Serveur d'administration de Kaspersky Security Center sur un cluster :

Lancez le fichier exécutable ksc_<version number>.<build number>_full_<localization language>.exe.

La fenêtre de sélection des applications Kaspersky s'ouvre pour l'installation. Dans la fenêtre de sélection de l'application, cliquez sur le lien **Installer le Serveur d'administration de Kaspersky Security Center** pour lancer l'Assistant d'installation du Serveur d'administration. Suivez les instructions de l'assistant.

Étape 1. Lecture du Contrat de licence utilisateur final et de la Politique de confidentialité

Cette étape de l'Assistant d'installation requiert la prise de connaissance du Contrat de licence utilisateur final conclu entre vous et AO Kaspersky et Politique de confidentialité.

Vous pouvez être invités à prendre connaissance des Contrats de licence utilisateur final et des Politiques de confidentialité des plug-ins d'administration des applications, inclus dans la distribution de Kaspersky Security Center.

Lisez attentivement le Contrat de licence utilisateur final conclu entre vous et Kaspersky, ainsi que la Politique de confidentialité. Si vous acceptez tous les termes du Contrat de licence et de la Politique de confidentialité, confirmez-le en cochant les cases appropriées.

L'installation de l'application se poursuit après que vous avez coché les deux cases.

Si vous n'êtes pas d'accord avec le Contrat de licence ou Politique de confidentialité, annulez l'installation en cliquant sur le bouton **Annuler**.

Étape 2. Sélection du type d'installation sur le cluster

Sélectionnez le type d'installation sur le cluster :

- **Cluster (installer sur tous les nœuds du cluster)**

  Il s'agit de l'option recommandée. Si vous sélectionnez cette option, le Serveur d'administration sera installé sur tous les nœuds du cluster simultanément.

  > Lors de l'étape de sélection de la Console d'administration pour l'installation, il faut sélectionner la console qui sera installée sur le nœud du cluster actuel. Si vous installez une console uniquement sur le nœud du cluster, en cas de défaillance du nœud, vous perdrez l'accès au Serveur d'administration. Lors de cette étape, nous vous recommandons de sélectionner la Console d'administration basée sur MMC pour l'installation sur tous les nœuds du cluster. Après avoir installé le Serveur d'administration, installez Kaspersky Security Center Web Console sur un appareil distinct qui n'est pas un nœud de cluster. Cela vous permet d'administrer le Serveur d'administration à l'aide de Kaspersky Security Center Web Console en cas de défaillance du nœud du cluster.

- **Localement (installation uniquement sur l'appareil actuel)**

  Si vous sélectionnez cette option, le Serveur d'administration ne sera installé que sur le nœud actuel, comme sur un serveur autonome, et le Serveur d'administration ne fonctionnera pas comme une application prenant en charge les clusters. Par exemple, vous pouvez choisir cette option pour économiser de l'espace de stockage partagé, si la tolérance aux pannes n'est pas nécessaire pour le Serveur d'administration. En cas de défaillance du nœud actuel, vous devrez installer le Serveur d'administration sur un autre nœud et restaurer l'état du Serveur d'administration à partir d'une sauvegarde.

Les étapes suivantes sont les mêmes que lorsque vous utilisez la méthode d'installation standard ou personnalisée, à partir de l'étape de sélection de la méthode d'installation.

Étape 3. Spécification du nom du Serveur d'administration virtuel

Spécifiez le nom de réseau du nouveau Serveur d'administration virtuel. Vous pourrez utiliser ce nom pour connecter la Console d'administration ou Kaspersky Security Center Web Console au Serveur d'administration.

Le nom que vous indiquez doit être différent du nom du cluster.

Étape 4. Spécification des détails du réseau du Serveur d'administration virtuel

Pour spécifier les détails du réseau de la nouvelle instance de Serveur d'administration virtuel :

1. Dans **Réseau pour l'utilisation,** sélectionnez le réseau de domaine auquel le nœud de cluster actuel est connecté.

2. Réalisez une des opérations suivantes :

   - Si DHCP est utilisé dans le réseau sélectionné pour attribuer des adresses IP, sélectionnez l'option **Utiliser DHCP**.

   - Si DHCP n'est pas utilisé dans le réseau sélectionné, spécifiez l'adresse IP requise.

     L'adresse IP que vous indiquez doit être différente de l'adresse IP du cluster.

3. Cliquez sur **Ajouter** pour appliquer les paramètres spécifiés.

Vous pourrez utiliser l'adresse IP attribuée automatiquement ou l'adresse IP spécifiée pour connecter la Console d'administration ou Kaspersky Security Center Web Console au Serveur d'administration.

Étape 5. Spécification d'un groupe de clusters

Un groupe de clusters est un rôle de cluster de basculement spécial qui contient des ressources communes pour tous les nœuds. Vous avez deux options :

- Création d'un nouveau groupe de clusters.

  Cette option est recommandée dans la plupart des cas. Le nouveau groupe de clusters contiendra toutes les ressources communes liées à l'instance du Serveur d'administration.

- Sélection d'un groupe de clusters existant.

  Sélectionnez cette option si vous souhaitez utiliser une ressource commune déjà associée à un groupe de clusters existant. Par exemple, il peut être intéressant d'utiliser cette option si vous souhaitez utiliser un stockage associé à un groupe de clusters existant et s'il n'y a aucun autre stockage disponible pour un nouveau groupe de clusters.

Étape 6. Sélection d'un stockage de données de cluster

Pour sélectionner un stockage de données de cluster :

1. Dans **Stockages disponibles**, sélectionnez le stockage de données dans lequel les ressources communes de l'instance de Serveur d'administration virtuel seront installées.

2. Si le stockage de données sélectionné contient plusieurs volumes, sous **Sections disponibles sur le disque**, sélectionnez le volume requis.

3. Dans **Chemin d'installation**, saisissez le chemin du stockage de données commun dans lequel les ressources de l'instance de Serveur d'administration virtuel seront installées.

Le stockage des données est sélectionné.

Étape 7. Spécification d'un compte pour l'installation à distance

Spécifiez le nom d'utilisateur et le mot de passe qui seront utilisés pour l'installation à distance de l'instance de Serveur d'administration virtuel sur un nœud passif du cluster.

Le compte que vous spécifiez doit disposer de privilèges administratifs sur tous les nœuds du cluster.

Étape 8. Sélection des modules pour l'installation

Sélectionnez les modules du Serveur d'administration de Kaspersky Security Center que vous voulez installer :

- **Administration des appareils mobiles**. Cochez cette case s'il faut créer des paquets d'installation pour les appareils mobiles lors de l'exécution de l'Assistant d'installation de Kaspersky Security Center. Vous pouvez aussi créer des paquets d'installation pour les appareils mobiles manuellement à l'aide des outils de la Console d'administration, une fois le Serveur d'administration installé.

- **Agent SNMP**. Reçoit les statistiques pour le Serveur d'administration via le protocole SNMP. Le module est accessible lors de l'installation de l'application sur un appareil doté du module SNMP.

  Après avoir installé Kaspersky Security Center, les fichiers .mib, nécessaires à l'obtention des données statistiques, seront situés dans le dossier d'installation de l'application dans le sous-dossier SNMP.

Les modules Agent d'administration et Console d'administration ne s'affichent pas dans la liste des modules. Ces modules s'installent automatiquement, il est impossible d'annuler leur installation.

A cette étape de l'Assistant, il faut aussi indiquer le dossier pour installer les modules du Serveur d'administration. Par défaut, les modules s'installent dans le dossier <Disk>:\Program Files\Kaspersky Lab\Kaspersky Security Center. Si le dossier avec ce nom n'existe pas, il sera automatiquement créé pendant l'installation. Vous pouvez modifier le dossier de destination à l'aide du bouton **Parcourir**.

Étape 9. Sélection de la taille du réseau

Indiquez la taille du réseau à installer Kaspersky Security Center. En fonction du nombre d'appareils sur le réseau, l'Assistant configure les paramètres d'installation et l'affichage de l'interface de l'application pour qu'ils correspondent.

Le tableau ci-dessous énumère les paramètres d'installation de l'application et d'affichage de l'interface lors de la sélection des tailles différentes du réseau.

Dépendance des paramètres d'installation de la sélection des tailles du réseau

Paramètres	1–100 appareils administrés	101–1 000 appareils administrés	1 001–5 000 appareils administrés	Plus de 5 000 appareils administrés
Affichage avec l'entrée des Serveurs d'administration virtuels et secondaires et de tous les paramètres, liés avec les Serveurs virtuels et secondaires, dans l'arborescence de la console (uniquement disponible dans la Console d'administration basée sur MMC)	Absent	Absent	Présent	Présent
Affichage avec les sections **Sécurité** dans les fenêtres des propriétés du Serveur et des groupes d'administration (disponible uniquement dans la Console d'administration basée sur MMC)	Absent	Absent	Présent	Présent
Répartition aléatoire du lancement de la tâche de mise à jour sur les appareils client	Absent	Selon un intervalle de 5 minutes	Selon un intervalle de 10 minutes	Selon un intervalle de 10 minutes

Lors de la connexion du Serveur d'administration au serveur de la base de données MySQL 5.7 et SQL Express, il est déconseillé d'utiliser l'application pour administrer plus de 10 000 appareils. Pour le système de gestion de base de données MariaDB, le nombre maximal recommandé d'appareils administrés est de 20 000.

Étape 10. Sélection d'une base de données

À cette étape de l'Assistant, sélectionnez un des systèmes de gestion de base de données qui servira au stockage de la base de données du Serveur d'administration :

- **Microsoft SQL Server ou SQL Server Express**
- **MySQL ou MariaDB**
- **PostgreSQL ou Postgres Pro**

Il est recommandé d'installer le Serveur d'administration sur un serveur dédié au lieu d'un contrôleur de domaine. Toutefois, si vous installez Kaspersky Security Center sur un serveur qui joue le rôle du contrôleur de domaine en lecture seule (RODC), le serveur Microsoft SQL Server (SQL Express) ne doit pas être installé en local (sur le même appareil). Dans ce cas, nous vous recommandons d'installer Microsoft SQL Server (SQL Express) à distance (sur un autre appareil), ou, si vous devez installer le SGBD localement, d'utiliser MySQL, MariaDB ou PostgreSQL.

La structure de la base de données du Serveur d'administration est décrite dans le fichier klakdb.chm qui figure dans le dossier d'installation de l'application Kaspersky Security Center. Ce fichier est également disponible dans une archive sur le portail de Kaspersky : klakdb.zip.

Étape 11. Configuration des paramètres du serveur SQL

À cette étape de l'Assistant, définissez les paramètres de connexion suivants en fonction du système de gestion de base de données (SGBD) que vous avez sélectionné :

- Si vous avez sélectionné **Microsoft SQL Server ou SQL Server Express** à l'étape précédente :

  - Indiquez dans le champ **Nom de l'instance du serveur SQL** le nom du serveur SQL installé dans le réseau. Le bouton **Parcourir** permet d'ouvrir la liste de tous les serveurs SQL installés dans le réseau. Par défaut, le champ est vide.

    Si vous vous connectez au serveur SQL via un port personnalisé, indiquez avec le nom d'hôte du serveur SQL le numéro de port séparé par une virgule, par exemple :

    ```
    Serveur_SQL_nom_hôte,1433
    ```

    Si vous sécurisez la communication entre le Serveur d'administration et le serveur SQL à l'aide d'un certificat, indiquez dans le champ **Nom de l'instance du serveur SQL** le même nom d'hôte que celui utilisé lors de la génération du certificat. Si vous utilisez une instance nommée du serveur SQL, indiquez avec le nom d'hôte du serveur SQL le numéro de port séparé par une virgule, par exemple :

    ```
    Serveur_SQL_nom,1433
    ```

    Si vous utilisez plusieurs instances de serveurs SQL sur le même hôte, indiquez également le nom de l'instance séparé par une barre oblique arrière, par exemple :

    ```
    Serveur_SQL_nom\Serveur_SQL_nom_instance,1433
    ```

    Si un serveur SQL sur le réseau d'entreprise a la fonction Always On activée, spécifiez le nom de l'écouteur du groupe de disponibilité dans le champ **Nom de l'instance du serveur SQL**. Notez que le Serveur d'administration ne prend en charge que le mode de disponibilité de validation synchrone lorsque la fonction Always On est activée.

  - Indiquez dans le champ **Nom de la base de données** le nom de DBMS créé pour héberger les informations du Serveur d'administration. La valeur par défaut est égale à *KAV*.

  Si vous souhaitez installer à cette étape un serveur SQL sur l'appareil depuis lequel vous installez Kaspersky Security Center, il faut interrompre l'installation et la lancer à nouveau après l'installation du serveur SQL. Serveurs SQL pris en charge figurant dans les exigences du système.

  Si vous souhaitez installer le serveur SQL sur un appareil distant, il n'est pas nécessaire d'interrompre l'Assistant d'installation de Kaspersky Security Center. Installez le serveur SQL et reprenez l'installation de Kaspersky Security Center.

- Si vous avez sélectionné **MySQL ou MariaDB** à l'étape précédente :

  - Indiquez dans le champ **Nom de l'instance du serveur SQL** le nom de l'instance du SGBD. Par défaut, l'adresse IP utilisée est celle de l'appareil sur lequel Kaspersky Security Center est installé.

  - Indiquez dans le champ **Port** le port de connexion du Serveur d'administration au SGBD. Le numéro de port par défaut est 3306.

  - Indiquez dans le champ **Nom de la base de données** le nom de DBMS créé pour héberger les informations du Serveur d'administration. La valeur par défaut est égale à *KAV*.

- Si vous avez sélectionné **PostgreSQL ou Postgres Pro** à l'étape précédente :

  - Indiquez dans le champ **PostgreSQL ou Postgres Pro Server** le nom de l'instance du SGBD. Par défaut, l'adresse IP utilisée est celle de l'appareil sur lequel Kaspersky Security Center est installé.

- Indiquez dans le champ **Port** le port de connexion du Serveur d'administration au SGBD. Le numéro de port par défaut est 5432.

Indiquez dans le champ **Nom de la base de données** le nom de DBMS créé pour héberger les informations du Serveur d'administration. La valeur par défaut est égale à *KAV*.

Étape 12. Sélection de la méthode d'authentification

Définissez la méthode d'authentification à utiliser lors de la connexion du Serveur d'administration au système de gestion de base de données.

Selon le SGBD sélectionné, vous pouvez sélectionner parmi les modes d'authentification suivants :

- Pour SQL Express ou Microsoft SQL Server, sélectionnez une des options suivantes :

  - **Mode d'authentification Microsoft Windows**. Dans ce cas lors de la vérification des privilèges le compte utilisateur sera utilisé pour le lancement du Serveur d'administration.

  - **Mode d'authentification du serveur SQL**. Le compte utilisateur indiqué dans la fenêtre sera utilisé dans le cas de sélection de ce mode. Remplissez les champs **Compte utilisateur** et **Mot de passe**.

    Pour voir le mot de passe saisi, maintenez le bouton **Afficher** enfoncé.

  Dans les deux modes d'authentification, l'application vérifie si la base de données est disponible. Si la base de données n'est pas disponible, un message d'erreur s'affiche et vous devez saisir les identifiants corrects.

  Si la base de données du Serveur d'administration se trouve sur un autre appareil et le compte utilisateur du Serveur d'administration n'a pas l'accès au serveur de la base de données, il faut utiliser le mode d'authentification du serveur SQL lors de l'installation ou de la mise à jour du Serveur d'administration. Cela peut se produire lorsque l'appareil avec la base de données ne se trouve pas dans le domaine ou si le Serveur d'administration est installé sous le compte LocalSystem.

Pour MySQL, MariaDB, PostgreSQL ou Postgres Pro, indiquez le compte et le mot de passe.

Étape 13. Sélection du compte utilisateur pour lancer le Serveur d'administration

Choisissez le compte utilisateur sous lequel le Serveur d'administration va être lancé en tant que service.

- **Créer un compte utilisateur automatiquement**. Le programme crée le compte utilisateur local KL-AK-*, sous lequel le service du Serveur d'administration kladminserver sera exécuté.

  Vous pouvez sélectionner cette option, si vous envisagez de placer le dossier partagé et le SGBD sur le même appareil que le Serveur d'administration.

- **Sélectionner un compte utilisateur**. Le service du Serveur d'administration (kladminserver) sera lancé sous le compte utilisateur que vous avez sélectionné.

  Il vous faudra sélectionner un compte utilisateur de domaine si, par exemple, vous envisagez d'utiliser en tant que SGBD un serveur SQL, quelle que soit sa version, y compris SQL-express, situé sur un autre appareil, et / ou si vous envisagez de placer le dossier partagé sur un autre appareil.

  Kaspersky Security Center est compatible avec les comptes de service administrés (MSA) et les comptes de service administrés de groupe (gMSA). Si ces comptes utilisateurs sont utilisés dans votre domaine, vous pouvez en choisir un comme compte pour le service du Serveur d'administration.

  Avant de définir MSA ou gMSA, vous devez installer le compte sur le même appareil que celui sur lequel vous souhaitez installer le Serveur d'administration. Si le compte n'est pas encore installé, annulez l'installation du Serveur d'administration, installez le compte, puis redémarrez l'installation du Serveur d'administration. Pour plus de détails sur l'installation des comptes de services administrés sur un appareil local, consultez la documentation officielle de Microsoft.

  Pour définir MSA ou gMSA :

  1. Cliquez sur le bouton **Parcourir**.
  2. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Type d'objet**.
  3. Sélectionnez le type **Compte utilisateur pour les services**, puis cliquez sur **OK**.
  4. Sélectionnez le compte utilisateur nécessaire et cliquez sur le bouton **OK**.

Le compte utilisateur que vous avez sélectionné doit disposer de droits différents en fonction du SGBD que vous prévoyez d'utiliser.

Pour des raisons de sécurité, ne faites pas du compte utilisateur sous lequel est exécuté le Serveur d'administration un compte privilégié.

Le compte du Serveur d'administration ne peut pas être modifié ultérieurement. Vous devez réinstaller le cluster de basculement pour utiliser un autre compte de Serveur d'administration.

Étape 14. Sélection du compte utilisateur pour lancer les services de Kaspersky Security Center

Choisissez le compte utilisateur sous lequel les services de Kaspersky Security Center vont être lancés sur cet appareil :

- **Créer un compte utilisateur automatiquement**. Kaspersky Security Center crée le compte utilisateur local KlScSvc sur cet appareil dans le groupe kladmins. Les services du Kaspersky Security Center se lanceront sous le compte utilisateur créé.

- **Sélectionner un compte utilisateur**. Les services de Kaspersky Security Center se lanceront sous le compte utilisateur que vous avez sélectionné.

  Il vous faudra choisir un compte utilisateur de domaine si, par exemple, vous envisagez de conserver les rapports dans un dossier situé sur un autre appareil, ou si cela est exigé par la stratégie de sécurité de votre organisation. Il peut également être nécessaire de choisir le compte utilisateur de domaine lors de l'installation du Serveur d'administration sur un cluster haute disponibilité.

Pour des raisons de sécurité, ne faites pas du compte utilisateur sous lequel sont lancés les services un compte privilégié.

Le compte utilisateur sélectionné servira à lancer le service KSN proxy (ksnproxy), le service du serveur proxy d'activation de Kaspersky (klactprx) et le service du portail d'authentification de Kaspersky (klwebsrv).

Étape 15. Définition du dossier partagé

Définissez le placement et le nom du dossier public, qui sera utilisé pour :

- La sauvegarde des fichiers pour l'installation à distance des applications (les fichiers sont copiés sur le Serveur d'administration lors de la création des paquets d'installation).

- Le stockage des mises à jour téléchargées depuis la source des mises à jour sur le Serveur d'administration.

L'accès public pour la lecture pour tous les utilisateurs sera ouvert à cette ressource.

Choisissez l'une des deux options suivantes :

- **Créer un dossier partagé**. Création du nouveau dossier. Indiquez le chemin d'accès au dossier dans le champ ci-après.

- **Sélectionner un dossier partagé existant**. La sélection du dossier partagé parmi les dossiers déjà existants.

Le dossier partagé peut être local sur l'appareil d'où l'installation a été réalisée ou distant sur n'importe lequel des appareils clients qui appartiennent au réseau de la société. Vous pouvez indiquer le dossier partagé à l'aide du bouton **Parcourir**, aussi que manuellement, en saisissant le chemin UNC dans le champ correspondant (par exemple, \\server\Share).

Le sous-dossier local KLSHARE est créé par défaut dans le dossier de l'application contenant des modules de Kaspersky Security Center.

Vous pouvez définir un dossier partagé ultérieurement si nécessaire.

Étape 16. Configuration des paramètres de connexion au Serveur d'administration

Configurez les paramètres de connexion au Serveur d'administration :

- **Port**

  Numéro de port utilisé pour se connecter au Serveur d'administration.

  Le numéro de port par défaut est 14000.

- **Port SSL**

  Numéro du port SSL : Affiche le numéro de port SSL utilisé pour établir une connexion sécurisée avec le Serveur d'administration.

  Le numéro de port par défaut est 13000.

- **Longueur de la clé de chiffrement**

  Choisissez la longueur de la clé de chiffrement : 1 024 ou 2 048 bits.

  Une clé de chiffrement de 1024 bits exerce une charge moins importante sur le processeur mais est considérée dépassée et, d'après ses caractéristiques techniques, peut ne pas assurer un chiffrement sûr. Il se peut également que l'équipement disponible ne soit pas compatible avec des certificats SSL qui utilisent une clé de 1 024 bits.

  Une clé de chiffrement de 2 048 bits répond aux standards modernes de chiffrement. Toutefois, l'utilisation d'une clé de chiffrement de 2 048 bits peut augmenter la charge sur le processeur.

  Par défaut, l'option **2048 bits (meilleure sécurité)** est sélectionnée.

Vous pouvez également modifier les paramètres de connexion ultérieure au Serveur d'administration comme suit :

- Vous pouvez modifier les numéros de port et les numéros de port SSL dans la section **Ports de connexion** des propriétés du Serveur d'administration. Pour en savoir plus sur les ports de connexion du Serveur d'administration, consultez la section Ports utilisés par Kaspersky Security Center.

- Vous pouvez modifier la longueur de la clé de chiffrement lors du remplacement du certificat du Serveur d'administration avec l'utilitaire klsetsrvcert en utilisant le paramètre `-o RsaKeyLen:<key length>`.

Étape 17. Définition de l'adresse du Serveur d'administration

Indiquez l'adresse du Serveur d'administration. Vous avez le choix parmi les options suivantes :

- **Nom du domaine DNS**. Vous pouvez utiliser cette méthode si le réseau comprend un serveur DNS et que les appareils clients peuvent l'utiliser pour recevoir l'adresse du Serveur d'administration.
- **Nom NetBIOS**. Vous pouvez utiliser cette méthode si les appareils clients reçoivent l'adresse du Serveur d'administration via le protocole NetBIOS ou si un serveur WINS est disponible sur le réseau.
- **Adresse IP**. Vous pouvez utiliser cette méthode si le Serveur d'administration possède une adresse IP statique qui ne sera pas modifiée par la suite.

Étape 18. Adresse du Serveur d'administration pour la connexion des appareils mobiles

Cette étape de l'Assistant d'installation est disponible au cas où vous auriez sélectionné Administration des appareils mobiles à installer.

Dans la fenêtre **Adresse pour la connexion des appareils mobiles**, indiquez l'adresse externe du Serveur d'administration pour la connexion des appareils mobiles qui se trouvent en dehors du réseau local. Vous pouvez spécifier l'adresse IP ou le système de nom de domaine (DNS) du Serveur d'administration.

Étape 19. Décompression et installation des fichiers sur le disque dur

A la fin de la configuration des paramètres d'installation des modules de Kaspersky Security Center, vous pouvez lancer l'installation des fichiers sur le disque dur.

Si les applications supplémentaires sont nécessaires pour lancer l'installation, l'Assistant d'installation vous en notifiera avant l'installation de Kaspersky Security Center sur la page **Installation des modules nécessaires**. Les applications nécessaires seront automatiquement installées après avoir cliqué sur le bouton **Suivant**.

Sur la dernière page, vous pouvez sélectionner la console à démarrer pour utiliser Kaspersky Security Center :

- **Lancer la Console d'administration basée sur MMC**
- **Démarrer Kaspersky Security Center Web Console**

  Cette option est disponible uniquement si vous avez choisi d'installer Kaspersky Security Center Web Console à l'une des étapes précédentes.

Vous pouvez aussi cliquer sur **Terminer** pour quitter l'assistant sans commencer à utiliser Kaspersky Security Center. Vous pouvez commencer à travailler plus tard, à tout moment.

Vous pouvez réaliser la configuration initiale de l'application au premier lancement de la Console d'administration ou de Kaspersky Security Center Web Console.

Installation du Serveur d'administration en mode silencieux

Le Serveur d'administration peut être installé en mode silencieux, c'est-à-dire sans saisie interactive des paramètres d'installation.

Pour installer le Serveur d'administration sur un appareil local en mode silencieux :

1. Lisez le Contrat de licence utilisateur final. Utilisez la commande ci-dessous uniquement si vous comprenez et acceptez les conditions du Contrat de licence utilisateur final.

2. Lisez la politique de confidentialité. Utilisez la commande ci-dessous uniquement si vous comprenez et acceptez que vos données soient traitées et transmises (y compris à des pays tiers) comme décrit dans la Politique de confidentialité.

3. exécutez la commande

```
setup.exe /s /v"DONT_USE_ANSWER_FILE=1 EULA=1 PRIVACYPOLICY=1 <setup_parameters>"
```

où `setup_parameters` est une liste des paramètres et de leurs valeurs respectives, séparés l'un de l'autre par un espace (`PARAM1=PARAM1VAL PARAM2=PARAM2VAL`). Le fichier setup.exe se trouve dans le dossier Server à l'intérieur de la distribution de Kaspersky Security Center.

Les noms et les valeurs possibles des paramètres qui peuvent être utilisés lors de l'installation du Serveur d'administration en mode silencieux sont cités dans le tableau ci-dessous.

Paramètres d'installation du Serveur d'administration en mode silencieux

Nom du paramètre	Description du paramètre	Valeurs possibles
CLUF	Accord avec les conditions du Contrat de licence.	• 1 : j'ai entièrement lu, compris et accepté les conditions du Contrat de licence utilisateur final. • Une autre valeur ou non définie - Je refuse les conditions du Contrat de licence (l'installation n'aura pas lieu).
PRIVACYPOLICY	Acceptation des conditions de la Politique de confidentialité.	• 1 : je comprends et j'accepte que mes données peuvent être traitées et transmises (y compris vers des pays tiers) dans le respect de la Politique de confidentialité. Je confirme que j'ai entièrement lu et que je comprends la Politique de confidentialité. • Une autre valeur ou non définie - Je refuse les conditions de la Politique de confidentialité (l'installation n'aura pas lieu).
INSTALLATIONMODETYPE	Type d'installation du Serveur d'administration.	• Standard – installation standard. • Custom – installation personnalisée.
INSTALLDIR	Chemin d'accès au dossier du Serveur d'administration.	Valeur de chaîne.
ADDLOCAL	Liste des modules (via virgule) du Serveur d'administration pour l'installation.	CSAdminKitServer, NAgent, CSAdminKitConsole, NSAC, MobileSupport, KSNProxy, SNMPAgent, GdiPlusRedist, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86. Minimum suffisant pour l'installation correcte du Serveur d'administration dans la liste des modules : `ADDLOCAL=CSAdminKitServer, CSAdminKitConsole, KSNProxy, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86`.

Nom du paramètre	Description du paramètre	Valeurs possibles
NETRANGETYPE	Taille du réseau (nombre d'appareils dans le réseau).	• NRT_1_100 — de 1 à 100 appareils. • NRT_100_1000 : de 101 à 1000 appareils. • NRT_GREATER_1000 : plus de 1000 appareils.
SRV_ACCOUNT_TYPE	Mode de définition du compte utilisateur sous lequel le Serveur d'administration sera lancé en tant que service.	• SrvAccountDefault : le compte utilisateur est créé automatiquement. • SrvAccountUser – le compte est défini manuellement. Dans ce cas, il faut définir les valeurs des paramètres `SERVERACCOUNTNAME` et `SERVERACCOUNTPWD`.
SERVERACCOUNTNAME	Mode de définition du compte utilisateur sous lequel le Serveur d'administration sera lancé en tant que service La valeur du paramètre est définie si SRV_ACCOUNT_TYPE=SrvAccountUser.	Valeur de chaîne.
SERVERACCOUNTPWD	Mot de passe du compte utilisateur sous lequel le Serveur d'administration va être lancé en tant que service. La valeur du paramètre est définie si SRV_ACCOUNT_TYPE=SrvAccountUser.	Valeur de chaîne.
SERVERCER	Longueur de la clé pour le certificat de Serveur d'administration (en bits).	• 1 : la longueur de la clé pour le certificat du Serveur d'administration est de 2048 bits. • Valeur non définie : la longueur de la clé pour le certificat de Serveur d'administration est de 1 024 bits.
DBTYPE	Le type de la base de données qui sera utilisée pour placer la base de données d'informations du Serveur d'administration. Ce paramètre est requis.	• MySQL : une base de données MySQL ou MariaDB sera utilisée. Dans ce cas, vous devez attribuer des valeurs aux paramètres `MYSQLSERVERNAME`, `MYSQLSERVERPORT`, `MYSQLDBNAME`, `MYSQLACCOUNTNAME` et `MYSQLACCOUNTPWD`. • MSSQL : une base de données Microsoft SQL Server (SQL Express) sera utilisée. Dans ce cas, il faut définir les valeurs des paramètres `MSSQLSERVERNAME`, `MSSQLDBNAME` et `MSSQLAUTHTYPE`. • POSTGRES : une base de données PostgreSQL ou Postgres Pro sera utilisée. Dans ce cas, vous devez attribuer des valeurs aux paramètres `POSTGRESSERVERNAME`, `POSTGRESSERVERPORT`, `POSTGRESDBNAME`, `POSTGRESACCOUNTNAME` et `POSTGRESACCOUNTPWD`.
MYSQLSERVERNAME	Le nom complet de SQL Server. la valeur du paramètre est définie si DBTYPE=MySQL	Valeur de chaîne.
MYSQLSERVERPORT	Le numéro du port pour la connexion à SQL Server. la valeur du paramètre est définie si DBTYPE=MySQL	Valeur numérique.
MYSQLDBNAME	Le nom de la base de données qui sera créé pour l'emplacement des informations du Serveur d'administration la valeur du paramètre est définie si DBTYPE=MySQL	Valeur de chaîne.
MYSQLACCOUNTNAME	Le nom du compte utilisateur pour la connexion à la base la valeur du paramètre est définie si DBTYPE=MySQL	Valeur de chaîne.
MYSQLACCOUNTPWD	Le mot de passe du compte utilisateur pour la connexion à la base la valeur du paramètre est définie si DBTYPE=MySQL	Valeur de chaîne.
MSSQLSERVERNAME	Le nom complet de SQL Server. la valeur du paramètre est définie si DBTYPE=MSSQL.	Valeur de chaîne.
MSSQLDBNAME	Le nom de la base de données la valeur du paramètre est définie si DBTYPE=MSSQL.	Valeur de chaîne.

Nom du paramètre	Description du paramètre	Valeurs possibles
MSSQLAUTHTYPE	Le type d'autorisation lors de la connexion à SQL Server. la valeur du paramètre est définie si DBTYPE=MSSQL.	• Windows : mode d'authentification de Microsoft Windows. • SQLServer : mode d'authentification du serveur SQL. Dans ce cas, il faut définir les valeurs des paramètres `MSSQLACCOUNTNAME` et `MSSQLACCOUNTPWD`.
MSSQLACCOUNTNAME	Le nom du compte utilisateur pour la connexion à SQL Server. la valeur du paramètre est définie si MSSQLAUTHTYPE=SQLServer.	Valeur de chaîne.
MSSQLACCOUNTPWD	Le mot de passe du compte utilisateur pour la connexion à SQL Server. la valeur du paramètre est définie si MSSQLAUTHTYPE=SQLServer.	Valeur de chaîne.
CREATE_SHARE_TYPE	Mode de définition du dossier partagé.	• Create : créer un dossier partagé. dans ce cas, il faut définir les valeurs des paramètres `SHARELOCALPATH` et `SHAREFOLDERNAME`. • ChooseExisting : sélectionner le dossier existant. dans ce cas, il faut définir la valeur du paramètre `EXISTSHAREFOLDERNAME`.
SHARELOCALPATH	– le chemin d'accès au dossier local. la valeur du paramètre est définie si CREATE_SHARE_TYPE=Create	Valeur de chaîne.
SHAREFOLDERNAME	– le nom de réseau du dossier. La valeur du paramètre est définie si CREATE_SHARE_TYPE=Create.	Valeur de chaîne.
EXISTSHAREFOLDERNAME	Le chemin d'accès complet au dossier partagé existant La valeur du paramètre est définie si CREATE_SHARE_TYPE=ChooseExisting.	Valeur de chaîne.
SERVERPORT	Le numéro de port pour se connecter au Serveur d'administration.	Valeur numérique.
SERVERSSLPORT	Le numéro du port pour établir une connexion sécurisée avec le Serveur d'administration via le protocole SSL.	Valeur numérique.
SERVERADDRESS	Adresse du Serveur d'administration.	Valeur de chaîne.
MOBILESERVERADDRESS	Adresse du Serveur d'administration pour la connexion des appareils mobiles.	Valeur de chaîne.

Les paramètres d'installation du Serveur d'administration sont décrites en détails dans la section Installation personnalisée.

Installation de la Console d'administration sur le poste de travail de l'administrateur

Vous pouvez installer la Console d'administration séparément sur le poste de travail de l'administrateur et gérer le Serveur d'administration par le réseau à l'aide de cette Console.

Pour installer la Console d'administration sur le poste de travail de l'administrateur, procédez comme suit :

1. Lancez le fichier exécutable setup.exe.

   La fenêtre de sélection des applications Kaspersky s'ouvre pour l'installation.

2. Dans la fenêtre de sélection des applications, lancez l'Assistant d'installation de la Console d'administration à l'aide du lien **Installer uniquement la Console d'administration de Kaspersky Security Center**. Suivez les instructions de l'assistant.

3. Sélectionnez le dossier de destination. Par défaut c'est <Disk>:\Program Files\Kaspersky Lab\Kaspersky Security Center Console. Si ce dossier n'existe pas, alors il sera créé automatiquement pendant l'installation. Vous pouvez modifier le dossier de destination à l'aide du bouton **Parcourir**.

4. Dans la fenêtre finale de l'Assistant d'installation, cliquez sur le bouton **Démarrer** pour commencer le processus d'installation de la Console d'administration.

A la fin du fonctionnement de l'Assistant, la Console d'administration sera installée sur le poste de travail de l'administrateur.

Pour installer la Console d'administration sur le poste de travail de l'administrateur en mode silencieux, procédez comme suit :

1. Lisez le Contrat de licence utilisateur final. Utilisez la commande ci-dessous uniquement si vous comprenez et acceptez les conditions du Contrat de licence utilisateur final.

2. Dans le dossier `Distrib\Console` du kit de distribution de Kaspersky Security Center, exécutez le fichier setup.exe à l'aide de la commande suivante :

   ```
   setup.exe /s /v"EULA=1"
   ```

   Si vous souhaitez installer tous les plug-ins d'administration à partir du dossier `Distrib\Console\Plugins` avec la Console d'administration, exécutez la commande suivante :

   ```
   setup.exe /s /v"EULA=1" /pALL
   ```

   Si vous souhaitez définir les plug-ins d'administration à installer à partir du dossier `Distrib\Console\Plugins` avec la Console d'administration, indiquez les plug-ins après la clé « /p » et séparez-les par un point-virgule :

   ```
   setup.exe /s /v"EULA=1" /pP1;P2;P3
   ```

   où `P1`, `P2`, `P3` sont les noms des plug-ins qui correspondent aux noms de dossier de plug-ins dans le dossier `Distrib\Console\Plugins`. Par exemple :

   ```
   setup.exe /s /v"EULA=1" /pKES4Mac;KESS;MDM4IOS
   ```

La Console d'administration et les plug-ins d'administration (le cas échéant) seront installés sur le poste de travail de l'administrateur.

Après l'installation de la Console d'administration il est nécessaire de se connecter au Serveur d'administration. Pour cela, lancez la Console d'administration et dans la fenêtre qui s'ouvre, indiquez le nom ou l'adresse IP de l'appareil sur lequel le Serveur d'administration est installé, sans oublier les paramètres du compte utilisateur de connexion à celui-ci. Après l'établissement de la connexion avec le Serveur d'administration, il est possible d'administrer le système de protection antivirus à l'aide de cette Console d'administration.

Vous pouvez supprimer la Console d'administration à l'aide des moyens standards d'installation et de suppression des applications Microsoft Windows.

Modifications du système après l'installation de Kaspersky Security Center

--Icône de la Console d'administration

Une fois que la Console d'administration a été installée sur votre appareil, son icône apparaît, ce qui vous permet de lancer la Console d'administration. Vous pouvez trouver la Console d'administration dans le menu **Démarrer → Applications → Kaspersky Security Center**.

Services du Serveur d'administration et de l'Agent d'administration

Le Serveur d'administration et l'Agent d'administration sont installés sur l'appareil à titre de service avec les propriétés reprises dans le tableau ci-dessous. Le tableau reprend également les attributs d'autres services exécutés sur l'appareil après l'installation du Serveur d'administration

Propriétés des services de Kaspersky Security Center

Module	Nom de service	Nom de service affiché	Compte utilisateur
Serveur d'administration	kladminserver	Serveur d'administration de Kaspersky Security Center	Compte utilisateur de type KL-AK-* indiqué par l'utilisateur ou compte spécial non privilégié créé lors de l'installation
Agent d'administration	klnagent	Agent d'administration de Kaspersky Security Center	Système local
Serveur Web pour accéder à Kaspersky Security Center Web Console et administrer le portail interne de l'entreprise	klwebsrv	Serveur Web de Kaspersky	Compte utilisateur spécial non privilégié KlScSvc
Serveur proxy d'activation	klactprx	Serveur proxy d'activation de Kaspersky	Compte utilisateur spécial non privilégié KlScSvc
Serveur proxy KSN	ksnproxy	Serveur proxy Kaspersky Security Network	Compte utilisateur spécial non privilégié KlScSvc

Si vous installez Kaspersky Security Center sur les nœuds du cluster de basculement Kaspersky Security Center, le service klfocsvc_klfoc devient disponible. Les services klnagent_klfoc et klfocsvc_klfoc s'exécutent sous le compte système local. Le service kladminserver_klfoc doit être exécuté sous le compte 'ksc' et les autres services doivent être exécutés sous le compte "rightless". Les comptes 'ksc' et 'rightless' doivent être ajoutés dans le groupe KLAdmins avec les permissions de l'administrateur local. Pour assurer le fonctionnement correct de Kaspersky Security Center, seuls les comptes 'ksc' et 'rightless' doivent être utilisés pour le fonctionnement des services. Il est déconseillé d'utiliser d'autres comptes avec les mêmes droits. Le tableau ci-dessous contient les propriétés des services qui sont appliqués sur l'appareil après l'installation du Serveur d'administration sur le cluster de basculement Kaspersky Security Center.

Propriétés des services de Kaspersky Security Center installés dans le cluster de basculement Kaspersky Security Center

Module	Nom de service	Nom de service affiché	Compte utilisateur
Serveur d'administration	kladminserver_klfoc	Serveur d'administration de Kaspersky Security Center	ksc
Agent d'administration	klnagent_klfoc	Agent d'administration de Kaspersky Security Center	Système local
Serveur Web pour accéder à Kaspersky Security Center Web Console et administrer le portail interne de l'entreprise	klwebsrv_klfoc	Serveur Web de Kaspersky	rightless
Serveur proxy d'activation	klactprx_klfoc	Serveur proxy d'activation de Kaspersky	rightless
Serveur proxy KSN	ksnproxy_klfoc	Serveur proxy Kaspersky Security Network	rightless
Cluster de basculement Kaspersky Security Center	klfocsvc_klfoc	Cluster de basculement Kaspersky Security Center	Système local

Services de Kaspersky Security Center Web Console

Si vous installez Kaspersky Security Center Web Console sur l'appareil, les services suivants sont déployés (voir le tableau ci-dessous) :

Services de Kaspersky Security Center Web Console

Nom de service affiché	Compte utilisateur
Service Kaspersky Security Center Web Console	Service NT/KSCSvcWebConsole
Kaspersky Security Center Web Console	Service réseau
Serveur des plug-ins des produits de Kaspersky Security Center	Service NT/KSCWebConsolePlugin
Service d'administration de Kaspersky Security Center Web Console	Système local
File d'attente des messages de Kaspersky Security Center Web Console.	Service NT/KSCWebConsoleMessageQueue

Version serveur de l'Agent d'administration

Outre le Serveur d'administration, la version serveur de l'Agent d'administration est également installée sur l'appareil. Elle fait partie du Serveur d'administration, est installée et supprimée, et peut coopérer uniquement avec le Serveur d'administration installé localement. Il n'est pas nécessaire de configurer les paramètres de la connexion de l'Agent d'administration au Serveur d'administration : la configuration est programmée en fonction des modules installés sur un appareil. La version serveur de l'Agent d'administration s'installe avec les mêmes attributs et exécute les mêmes fonctions d'administration des applications que l'Agent d'administration standard. La stratégie du groupe d'administration qui reprend l'appareil client du Serveur d'administration agit sur cette version. Toutes les tâches, prévues pour l'Agent d'administration excepté la tâche de changement du Serveur d'administration, seront créées pour la version serveur de l'Agent d'administration.

L'installation distincte de l'Agent d'administration sur l'appareil disposant du Serveur d'administration est impossible.

Vous pouvez consulter les propriétés des services du Serveur d'administration et de l'Agent d'administration, ainsi que suivre leur fonctionnement à l'aide des moyens d'administration standards Microsoft Windows : Administration de l'ordinateur\Services. Les informations relatives au fonctionnement du service du Serveur d'administration sont enregistrées dans le journal système Microsoft Windows sur l'appareil où est installé le Serveur d'administration, dans une branche distincte du journal des événements Kaspersky.

Il est déconseillé de lancer ou de désactiver manuellement les services et de modifier les comptes utilisateurs dans les réglages des services. En cas de nécessité, vous pouvez échanger le compte utilisateur du service du Serveur d'administration à l'aide de l'utilitaire klsrvswch. Notez que vous devez lancer l'utilitaire klsrvswch sur l'appareil du Serveur d'administration sous le compte avec privilèges d'administrateur qui a été utilisé pour installer le Serveur d'administration.

Comptes utilisateurs et groupes de sécurité

Le programme d'installation du Serveur d'administration crée par défaut les comptes utilisateurs suivants :

- KL-AK-* : compte utilisateur du service du Serveur d'administration.
- KlScSvc : compte utilisateur pour les autres services compris dans le Serveur d'administration.
- KlPxeUser : compte utilisateur pour le déploiement des systèmes d'exploitation.

Si au moment de l'exécution du programme d'installation, vous avez sélectionné d'autres comptes utilisateurs pour le service du Serveur d'administration et d'autres services, les comptes utilisateurs que vous avez choisis seront utilisés.

Les groupes de sécurité locaux nommés KLAdmins et KLOperators et leur ensemble de droits respectifs sont également créés automatiquement sur l'appareil sur lequel le Serveur d'administration est installé.

Il n'est pas recommandé d'installer le Serveur d'administration sur un contrôleur de domaine. Cependant, si vous installez le Serveur d'administration sur le contrôleur de domaine, vous devez démarrer le programme d'installation avec les droits d'administrateur de domaine. Dans ce cas, le programme d'installation crée automatiquement des groupes de sécurité de domaine appelés KLAdmins et KLOperators. Si vous installez le Serveur d'administration sur un appareil qui n'est pas le contrôleur de domaine, vous devez démarrer le programme d'installation avec les droits d'administrateur local à la place. Dans ce cas, le programme d'installation crée automatiquement des groupes de sécurité locaux appelés KLAdmins et KLOperators.

Lors de la configuration des notifications par email, vous pouvez avoir besoin de créer un compte utilisateur sur le serveur de messagerie pour l'authentification ESMTP.

Suppression de l'application

Vous pouvez supprimer Kaspersky Security Center à l'aide des moyens standard d'installation et de suppression des applications Microsoft Windows. La suppression d'une application requiert le lancement d'un Assistant qui va supprimer tous les modules de l'application (y compris les plug-ins) de l'appareil. L'assistant fait en sorte que votre navigateur par défaut ouvre une page Web contenant un sondage vous permettant de nous expliquer pourquoi vous avez choisi d'arrêter d'utiliser Kaspersky Security Center. Si lors du fonctionnement de l'Assistant vous n'avez pas défini la suppression du dossier partagé (KLSHARE), alors après la fin de toutes les tâches liées, vous pouvez le supprimer manuellement.

Des fichiers peuvent rester dans le dossier temporaire après la suppression de l'application.

L'Assistant de création de la tâche de suppression de l'application vous proposera d'enregistrer la copie de sauvegarde du Serveur d'administration.

Lors de la suppression de l'application sous Microsoft Windows 7 et Microsoft Windows 2008, un arrêt anticipé de l'Assistant de création de la tâche de suppression de l'application peut se produire. Afin d'éviter ceci, désactivez le Contrôle de compte d'utilisateur (UAC) dans le système d'exploitation et redémarrez la suppression de l'application.

À propos de la mise à jour de Kaspersky Security Center

Cette section contient des informations sur la mise à jour de Kaspersky Security Center à partir d'une version antérieure. Vous pouvez mettre à jour Kaspersky Security Center de différentes manières, selon que Kaspersky Security Center a été installé localement ou sur les nœuds du cluster de basculement Kaspersky Security Center.

Lors de la mise à jour, l'utilisation simultanée du SGBD par le Serveur d'administration et une autre application est strictement interdite.

Veuillez noter que si vous mettez à niveau le Serveur d'administration vers la version 15.1, vous ne pourrez pas créer d'autres paquets d'installation de l'Agent d'administration de la version 15 ou toute version antérieure. Cependant, les paquets d'installation créés précédemment resteront disponibles.

Lors de la mise à jour de Kaspersky Security Center à partir d'une version précédente, tous les plug-ins installés des applications Kaspersky prises en charge sont conservés. Le plug-in du Serveur d'administration et le plug-in de l'Agent d'administration sont mis à niveau automatiquement (aussi bien pour la Console d'administration que pour Kaspersky Security Center Web Console).

Mise à jour de Kaspersky Security Center depuis une version antérieure

La rubrique suivante décrit les étapes de préparation recommandées pour la mise à niveau : Mise à jour de Kaspersky Security Center et des applications de sécurité administrées.

Vous pouvez installer le Serveur d'administration version 15.1 sur un appareil disposant d'une version antérieure du Serveur d'administration (à partir de la version 11 (11.0.0.1131b)). Lors de la mise à jour jusqu'à la version 15.1, tous les données et les paramètres de la version précédente du Serveur d'administration sont conservées.

En cas de problèmes lors de l'installation, vous pouvez restaurer la version précédente du Serveur d'administration, en utilisant la copie de sauvegarde des données du Serveur créée avant la mise à jour.

Si dans le réseau au moins un Serveur d'administration de nouvelle version est installé, vous pouvez mettre à niveau les autres Serveurs d'administration du réseau à l'aide de la tâche d'installation à distance qui utilise le paquet d'installation du Serveur d'administration.

> Si vous avez déployé le cluster de basculement Kaspersky Security Center, vous pouvez également mettre à jour Kaspersky Security Center sur ses nœuds.

Pour mettre à jour le Serveur d'administration de la version précédente à la version 15.1, procédez comme suit :

1. Lancez le fichier d'installation ksc_15.1_<numéro de version>_full_<language>.exe pour la version 15.1 (vous pouvez télécharger ce fichier à partir du site de Kaspersky).

2. Dans la fenêtre de sélection des applications, lancez l'Assistant d'installation du Serveur d'administration à l'aide du lien **Installer Kaspersky Security Center**. Suivez les instructions de l'assistant.

3. Lecture du Contrat de licence utilisateur final et de la Politique de confidentialité. Si vous acceptez toutes les dispositions du Contrat de licence utilisateur final et de la Politique de confidentialité, cochez les cases suivantes dans le groupe **Je confirme que j'ai lu, je comprends et j'accepte l'intégralité de ce qui suit** :

   - **Les termes et conditions de ce Contrat de licence utilisateur final**
   - **Politique de confidentialité décrivant le traitement des données**

   L'installation de l'application se poursuit après que vous avez coché les deux cases. L'Assistant d'installation vous invite à créer une sauvegarde des données du Serveur d'administration pour la version antérieure.

   Kaspersky Security Center prend en charge la récupération des données à partir d'une sauvegarde créée avec une ancienne version du Serveur d'administration.

4. Si vous souhaitez créer une sauvegarde des données du Serveur d'administration, indiquez-la dans la fenêtre **Sauvegarde des données du Serveur d'administration** qui s'ouvre.

   Une sauvegarde est créée par l'utilitaire klbackup. Cet utilitaire fait partie du kit de distribution de l'application et se trouve dans la racine du dossier d'installation de Kaspersky Security Center.

5. Installez le Serveur d'administration de version 15.1, en suivant l'Assistant d'installation.

   Si un message vous indique que le service de Kaspersky Security Center 14 Web Console est occupé, cliquez sur le bouton **Ignorer** dans la fenêtre de l'Assistant.

   Il est déconseillé d'interrompre l'exécution de l'Assistant d'installation. Si vous annulez la mise à jour à l'étape d'installation du Serveur d'administration, la version mise à jour de Kaspersky Security Center risque d'échouer.

6. Pour les appareils dotés d'un Agent d'administration de la version antérieure, créez et lancez une tâche d'installation à distance de la nouvelle version de l'Agent d'administration.

   Nous vous recommandons de mettre à jour l'Agent d'administration pour Linux vers la même version que Kaspersky Security Center.

   Une fois la tâche d'installation à distance terminée, la version de l'Agent d'administration est mise à jour.

   Exécutez les commandes suivantes sur les ressources basées sur Linux pour supprimer les dépendances devenues obsolètes :

   - Pour les ressources basées sur Debian, exécutez l'une des commandes suivantes :
     - `apt-get -y autoremove`
     - `apt -y autoremove`
   - Pour les ressources basées sur RPM, exécutez l'une des commandes suivantes :
     - `dnf autoremove`
     - `yum autoremove`

Mise à jour de Kaspersky Security Center sur les nœuds du cluster de basculement Kaspersky Security Center

Vous pouvez installer la version 15.1 du Serveur d'administration sur chaque nœud du cluster de basculement Kaspersky Security Center doté d'une version antérieure du Serveur d'administration (à partir de la version 13.2). Lors de la mise à jour jusqu'à la version 15.1, tous les données et les paramètres de la version précédente du Serveur d'administration sont conservées.

Si vous avez précédemment installé Kaspersky Security Center localement sur des appareils, vous pouvez également mettre à jour Kaspersky Security Center sur ces appareils.

Pour mettre à jour Kaspersky Security Center sur les nœuds du cluster de basculement Kaspersky Security Center :

1. Effectuez les actions suivantes sur le nœud actif du cluster :

   a. Lancez le fichier exécutable sc_15.1_<build number>_full_<language>.exe.

      Une fenêtre s'ouvre et vous invite à sélectionner les applications Kaspersky à mettre à jour. Lancez l'Assistant d'installation du Serveur d'administration en cliquant sur le lien **Installer le Serveur d'administration de Kaspersky Security Center**. Suivez les instructions de l'Assistant.

   b. Lecture du Contrat de licence utilisateur final et de la Politique de confidentialité. Si vous acceptez toutes les dispositions du Contrat de licence utilisateur final et de la Politique de confidentialité, cochez les cases suivantes dans le groupe **Je confirme que j'ai lu, je comprends et j'accepte l'intégralité de ce qui suit** :

      - **Les termes et conditions de ce Contrat de licence utilisateur final**
      - **Politique de confidentialité décrivant le traitement des données**

      Cochez les deux cases pour poursuivre l'installation.

      Si vous n'acceptez pas le Contrat de licence ou la Politique de confidentialité, cliquez sur le bouton **Annuler** pour annuler la mise à jour.

2. Exécutez les mêmes actions sur le nœud passif du cluster de basculement Kaspersky Security Center que sur le nœud actif.

3. Démarrer le cluster.

Par conséquent, vous avez installé la version la plus récente du Serveur d'administration sur les nœuds du cluster de basculement de Kaspersky Security Center.

Mise à jour de Kaspersky Security Center sur les nœuds du cluster de basculement Microsoft

Vous pouvez installer la version 15.1 du Serveur d'administration sur chaque nœud du cluster de basculement Microsoft doté d'une version antérieure du Serveur d'administration (à partir de la version 13.2). Lors de la mise à jour jusqu'à la version 15.1, tous les données et les paramètres de la version précédente du Serveur d'administration sont conservées.

Pour mettre à niveau Kaspersky Security Center sur les nœuds du cluster de basculement Microsoft, effectuez les actions suivantes sur n'importe quel nœud du cluster :

1. Lancez le fichier exécutable sc_15.1_<build number>_full_<language>.exe.

   Une fenêtre s'ouvre et vous invite à sélectionner les applications Kaspersky à mettre à jour. Lancez l'Assistant d'installation du Serveur d'administration en cliquant sur le lien **Installer le Serveur d'administration de Kaspersky Security Center**. Suivez les instructions de l'Assistant.

2. Lecture du Contrat de licence utilisateur final et de la Politique de confidentialité. Si vous acceptez toutes les dispositions du Contrat de licence utilisateur final et de la Politique de confidentialité, cochez les cases suivantes dans le groupe **Je confirme que j'ai lu, je comprends et j'accepte l'intégralité de ce qui suit** :

   - **Les termes et conditions de ce Contrat de licence utilisateur final**
   - **Politique de confidentialité décrivant le traitement des données**

   Cochez les deux cases pour poursuivre l'installation.

   Si vous n'acceptez pas le Contrat de licence ou la Politique de confidentialité, cliquez sur le bouton **Annuler** pour annuler la mise à jour.

3. Dans la fenêtre **Type d'installation sur le cluster**, sélectionnez le **Cluster (installer sur tous les nœuds du cluster)**.

   Ensuite, le programme d'installation configure et termine la mise à jour du Serveur d'administration sur tous les nœuds du cluster. Pendant la mise à niveau, il est impossible de modifier les paramètres du Serveur d'administration.

Par conséquent, vous avez installé la version la plus récente du Serveur d'administration sur les nœuds du cluster de basculement Microsoft.

Configuration initiale de Kaspersky Security Center

Cette section décrit les étapes à suivre absolument après l'installation de Kaspersky Security Center pour effectuer la configuration initiale.

Guide de sécurisation renforcée

Le guide de sécurisation renforcée est destiné aux experts chargés de l'installation et de l'administration de Kaspersky Security Center, et aux spécialistes un support technique au sein des organisations qui utilisent Kaspersky Security Center.

Le Guide de sécurisation renforcée décrit les recommandations et les fonctionnalités de configuration de Kaspersky Security Center et de ses modules, dans le but de réduire les risques de compromission.

Avant la configuration, créez une copie de sauvegarde du Serveur d'administration de Kaspersky Security Center à l'aide de la tâche Sauvegarde des données du Serveur d'administration ou utilitaire klbackup et enregistrez-la dans un endroit sûr.

Le Guide de sécurisation renforcée comprend les informations suivantes :

- Sélection de l'architecture du Serveur d'administration
- Configuration d'une connexion sécurisée au Serveur d'administration
- Configuration des comptes d'accès au Serveur d'administration
- Gestion de la protection du Serveur d'administration et des appareils clients
- Configuration de la protection des applications administrées
- Maintenance du Serveur d'administration
- Transfert d'informations vers des applications tierces

Avant de commencer à utiliser le Serveur d'administration, Kaspersky Security Center vous invite à lire la version abrégée du Guide de sécurisation renforcée des capacités.

Notez que vous ne pouvez pas utiliser le Serveur d'administration tant que vous n'avez pas confirmé avoir lu le Guide de sécurisation renforcée.

Pour lire le Guide de sécurisation renforcée :

1. Ouvrez la Console d'administration ou Kaspersky Security Center Web Console et connectez-vous à la console. La console vérifie si vous avez confirmé la lecture de la version actuelle du Guide de sécurisation renforcée.

   Si vous n'avez pas encore lu le Guide de sécurisation renforcée, une fenêtre s'ouvre et affiche une version succincte de celui-ci.

2. Exécutez une des actions suivantes :

   - Si vous souhaitez consulter la version abrégée du Guide de renforcement sous la forme d'un document texte, cliquez sur le lien **Ouvrir dans une nouvelle fenêtre**.
   - Si vous souhaitez consulter la version complète du Guide de renforcement, cliquez sur le lien **Ouvrir le guide de renforcement dans l'aide en ligne**.

3. Après avoir lu le Guide de renforcement, cochez la case **Je confirme que j'ai entièrement lu et que je comprends le guide de sécurisation renforcée**, puis cliquez sur le bouton **Accepter**.

Vous pouvez maintenant utiliser le Serveur d'administration.

Lorsqu'une nouvelle version du Guide de sécurisation renforcée de la sécurité apparaît, Kaspersky Security Center vous invite à la lire.

Assistant de configuration initiale du Serveur d'administration

Cette section reprend les informations sur le fonctionnement de l'Assistant de configuration initiale du Serveur d'administration.

À propos de l'Assistant de configuration initiale de l'application

Cette section reprend les informations sur le fonctionnement de l'Assistant de configuration initiale du Serveur d'administration.

L'Assistant de configuration initiale du Serveur d'administration vous permet de créer un minimum de tâches et de stratégies nécessaires, d'ajuster un minimum de paramètres, de télécharger et d'installer des plug-ins pour les applications Kaspersky administrées et de créer des paquets d'installation des applications Kaspersky administrées. Pendant le fonctionnement de l'Assistant, vous pouvez introduire les modifications suivantes dans l'application :

- Téléchargez et installez des plug-ins pour les applications administrées. Lorsque l'Assistant de configuration initiale de l'application a terminé, la liste des plug-ins d'administration installés s'affiche dans **Avancé** → **Informations sur les plug-ins d'administration des applications installés** de la fenêtre des propriétés du Serveur d'administration.

- Créez des paquets d'installation pour des applications de Kaspersky administrées. Une fois que l'Assistant de configuration initiale de l'application a terminé, des paquets d'installation pour l'Agent d'administration pour Windows et les applications administrées de Kaspersky s'affichent dans la liste **Serveur d'administration** → **Avancé** → **Installation à distance** → **Paquets d'installation**.

- Ajouter des fichiers de clés ou saisir des codes d'activation qui peuvent être diffusés automatiquement sur les appareils dans les groupes d'administration. Une fois l'Assistant de configuration initiale de l'application terminé, des informations sur les clés de licence s'affichent dans la liste de la fenêtre des propriétés du **Serveur d'administration** → **Licences pour les logiciels de Kaspersky** et dans la section **Clés de licence**.

- Configurer l'interaction avec Kaspersky Security Network (KSN).

- Configurer l'envoi de notifications par email des événements survenus pendant l'utilisation du Serveur d'administration et des applications administrées (afin qu'une notification passe avec succès, sur le Serveur d'administration et sur tous les appareils, le service Windows Messenger doit être lancé). Une fois que l'Assistant de configuration initiale de l'application a terminé, les paramètres des notifications par e-mail s'affichent dans la section **Notification** de la fenêtre des propriétés du Serveur d'administration.

- Configurer les paramètres des mises à jour et de correction des vulnérabilités des applications installées sur les appareils.

- Configurer la stratégie de protection des postes de travail et des serveurs, ainsi que les tâches de recherche de logiciels malveillants, de récupération des mises à jour et de sauvegarde des données pour le niveau supérieur de la stratégie des appareils administrés. Une fois que l'Assistant de configuration initiale de l'application a terminé, les tâches créées s'affichent dans la liste **Serveur d'administration** → **Tâches**, alors que les stratégies des plug-in des applications administrées sont affichées dans la liste du **Serveur d'administration** → **Stratégies**.

L'Assistant de configuration initiale de l'application crée des stratégies pour les applications administrées telles que Kaspersky Endpoint Security for Windows, à moins que ces stratégies ne soient créées pour le groupe d'**appareils administrés**. L'Assistant de configuration initiale de l'application crée des tâches si les tâches portant le même nom n'existent pas pour le groupe d'**appareils administrés**.

Dans la Console d'administration, Kaspersky Security Center vous invite automatiquement à exécuter l'Assistant de configuration initiale de l'application après l'avoir démarré pour la première fois. Vous pouvez aussi lancer l'Assistant de configuration initiale de l'application manuellement à tout moment.

Démarrage de l'Assistant de configuration initiale du Serveur d'administration

L'application vous invite automatiquement à lancer l'Assistant de configuration initiale de l'application après l'installation du Serveur d'administration, lors de la première connexion au Serveur d'administration. Vous pouvez aussi lancer l'Assistant de configuration initiale de l'application manuellement à tout moment.

Pour lancer manuellement l'Assistant de configuration initiale de l'application, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez l'entrée **Serveur d'administration**.
2. Dans le menu contextuel de l'entrée, sélectionnez l'option **Toutes les tâches → &Assistant de configuration initiale du Serveur d'administration**.

   L'Assistant propose de réaliser la configuration initiale du Serveur d'administration. Suivez les instructions de l'assistant.

Si vous redémarrez l'Assistant de configuration initiale de l'application, les tâches et stratégies créées lors de l'exécution précédente de l'Assistant ne peuvent pas être recréées.

Étape 1. Configuration des paramètres du serveur proxy

Indiquez les paramètres d'accès Internet du Serveur d'administration. Vous devez configurer l'accès Internet pour utiliser Kaspersky Security Network et télécharger les mises à jour des bases antivirus pour Kaspersky Security Center et les applications Kaspersky administrées.

Sélectionnez l'option **Utiliser un serveur proxy** si vous souhaitez utiliser un serveur proxy pour vous connecter à Internet. Si cette option est sélectionnée, les champs de saisie des paramètres sont accessibles. Configurez les paramètres suivants de connexion au serveur proxy :

- **Adresse**

  Adresse du serveur proxy pour la connexion de Kaspersky Security Center à Internet.

- **Numéro de port**

  Numéro du port via lequel la connexion proxy à Kaspersky Security Center sera établie.

- **Ne pas utiliser le serveur proxy pour les adresses locales**

  Le serveur proxy n'est pas utilisé lors de la connexion aux appareils dans le réseau local.

- **Authentification du serveur proxy**

  Si la case est cochée, les champs de saisie permettent d'indiquer les identifiants pour l'authentification sur le serveur proxy.

  Ce champ de saisie est accessible si la case **Utiliser un serveur proxy** est cochée.

- **Nom d'utilisateur**

  Compte utilisateur sous lequel la connexion au serveur proxy est établie (ce champ est disponible si la case **Authentification du serveur proxy** est cochée).

- **Mot de passe**

  Mot de passe défini par l'utilisateur sous le compte duquel la connexion au serveur proxy est établie (ce champ est disponible si la case **Authentification du serveur proxy** est cochée).

  Pour voir le mot de passe saisi, cliquez sur le bouton **Afficher** et maintenez-le enfoncé aussi longtemps que vous en avez besoin.

Vous pouvez aussi configurer l'accès à Internet plus tard, indépendamment de l'Assistant de démarrage rapide.

Étape 2. Sélection de la méthode d'activation de l'application

Choisissez une des options suivantes pour activer Kaspersky Security Center :

- **Veuillez saisir le code d'activation**

  Le *code d'activation* est une suite unique de 20 caractères alphanumériques. Vous le saisissez pour ajouter la clé activant le Kaspersky Security Center. Vous recevez le code d'activation à l'adresse email que vous avez indiquée après l'achat de Kaspersky Security Center.

  Pour activer l'application à l'aide du code d'activation, vous avez besoin d'un accès Internet pour vous connecter aux serveurs d'activation de Kaspersky.

  Si vous avez sélectionné cette option d'activation, vous pouvez activer l'option **Distribuer automatiquement la clé de licence sur les appareils administrés**.

  Si cette option est activée, la clé de licence sera déployée automatiquement sur les appareils administrés.

  Si cette option est désactivée, vous pouvez déployer la clé de licence sur les appareils administrés ultérieurement, dans le nœud **Licences pour les logiciels de Kaspersky** de l'arborescence de la Console d'administration.

  Si l'activation à l'aide du code d'activation a échoué pour une raison quelconque, vous pouvez activer l'application en utilisant un fichier clé.

- **Indiquez le fichier clé**

  Le *fichier clé* est un fichier doté d'une extension .key qui vous est fourni par Kaspersky. Il permet d'ajouter le fichier clé activant l'application.

  Les méthodes d'obtention du fichier clé sont décrites dans la section suivante : À propos du fichier clé.

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

  Si vous avez sélectionné cette option d'activation, vous pouvez activer l'option **Distribuer automatiquement la clé de licence sur les appareils administrés**.

  Si cette option est activée, la clé de licence sera déployée automatiquement sur les appareils administrés.

  Si cette option est désactivée, vous pouvez déployer la clé de licence sur les appareils administrés ultérieurement, dans le nœud **Licences pour les logiciels de Kaspersky** de l'arborescence de la Console d'administration.

- **Reportez l'activation de l'application**

  L'application fonctionne avec la fonctionnalité de base, sans l'Administration des appareils mobiles et sans la Gestion des vulnérabilités et des correctifs.

Si vous avez choisi l'activation reportée de l'application, vous pouvez ajouter une clé de licence plus tard à tout moment.

Étape 3. Sélection des zones de protection et des systèmes d'exploitation

Sélectionnez les zones de protection et les systèmes d'exploitation utilisés sur votre réseau. Lorsque vous sélectionnez ces options, vous spécifiez les filtres pour les plug-ins d'administration des applications et les paquets de distribution sur les serveurs Kaspersky que vous pouvez télécharger pour les installer sur les appareils clients de votre réseau. Sélectionnez les options :

- **Zone**

  Vous pouvez sélectionner les zones de protection suivantes :

  - **Postes de travail**. Sélectionnez cette option si vous souhaitez protéger les postes de travail de votre réseau. L'option Poste de travail est sélectionnée par défaut.
  - **Serveurs de fichiers et systèmes de stockage de données**. Sélectionnez cette option si vous souhaitez protéger les serveurs de fichiers de votre réseau.
  - **Appareils mobiles**. Sélectionnez cette option si vous souhaitez protéger les appareils mobiles appartenant à l'entreprise ou aux employés de l'entreprise. Si vous sélectionnez cette option mais que vous n'avez pas fourni de licence avec la Fonction Administration des appareils mobiles, un message s'affiche vous informant de la nécessité de fournir une licence avec la Fonction Administration des appareils mobiles. Si vous ne fournissez pas de licence, vous ne pouvez pas utiliser la fonction Appareil mobile.
  - **Environnements virtuels**. Sélectionnez cette option si vous souhaitez protéger les machines virtuelles de votre réseau.
  - **Anti-Spam Kaspersky**. Sélectionnez cette option si vous souhaitez protéger les serveurs email de votre organisation contre le spam, la fraude et la diffusion de logiciels malveillants.

- **Systèmes d'exploitation**

  Vous pouvez sélectionner les plateformes suivantes :

  - Microsoft Windows
  - Linux
  - macOS
  - Android
  - Autres

  Pour plus d'informations sur les systèmes d'exploitation pris en charge, reportez-vous à la section Configuration matérielle et logicielle requise.

Vous pouvez sélectionner les paquets de l'application Kaspersky dans la liste des paquets disponibles ultérieurement, indépendamment de l'Assistant de configuration initiale de l'application. Pour simplifier la recherche des paquets requis, vous pouvez filtrer la liste des paquets disponibles selon les critères suivants :

- Zone de protection
- Type de logiciel téléchargé (paquet de distribution, utilitaire, plug-in ou plug-in Internet)
- Version de l'application Kaspersky
- Langue de localisation de l'application Kaspersky

Étape 4. Installation des plug-ins pour les applications administrées

Sélectionnez les plug-ins pour les applications administrées à installer. Une liste des plug-ins situés sur les serveurs de Kaspersky s'affiche. La liste est filtrée selon les options sélectionnées à l'étape précédente de l'Assistant. Par défaut, une liste complète comprend des plug-ins dans toutes les langues. Pour afficher uniquement le plug-in d'une langue spécifique, sélectionnez la langue dans la liste déroulante **Afficher la langue de la Console d'administration ou**. La liste des plug-ins comprend les colonnes suivantes :

- **Nom de l'application**

  Les plug-ins en fonction des zones de protection et des plates-formes que vous avez sélectionnées à l'étape précédente sont sélectionnés.

- **Version de l'application**

  La liste comprend des plug-ins de toutes les versions placées sur les serveurs de Kaspersky. Par défaut, les plug-ins des dernières versions sont sélectionnés.

- **Langue de localisation**

  Par défaut, la langue de localisation d'un plug-in est définie par la langue Kaspersky Security Center que vous avez sélectionnée lors de l'installation. Vous pouvez spécifier d'autres langues dans la liste déroulante **Afficher la langue de la Console d'administration ou**.

Une fois les plug-ins sélectionnés, leur installation démarre automatiquement dans une fenêtre distincte. Pour installer certains plug-ins, vous devez accepter les conditions du CLUF. Lisez le texte du CLUF, sélectionnez l'option **J'accepte les termes du Contrat de licence utilisateur final** et cliquez sur le bouton **Installer**. Si vous n'acceptez pas les termes du CLUF, le plug-in n'est pas installé.

Une fois l'installation terminée, fermez la fenêtre d'installation.

Vous pouvez également sélectionner les plug-ins d'administration ultérieurement, indépendamment de l'Assistant de configuration initiale de l'application.

Étape 5. Téléchargement des paquets de distribution et création des paquets d'installation

Kaspersky Endpoint Security for Windows comprend un outil de chiffrement pour les informations stockées sur les appareils clients. Pour télécharger un paquet de distribution de Kaspersky Endpoint Security for Windows valable pour les besoins de votre organisation, consultez la législation du pays où se trouvent les appareils clients de votre organisation.

Dans la fenêtre **Type de chiffrement**, sélectionnez l'un des types de chiffrement suivants :

- Chiffrement fort (AES256). Ce type de chiffrement utilise une longueur de clé de 256 bits.
- Chiffrement simplifié (AES56). Ce type de chiffrement utilise une longueur de clé de 56 bits.

La fenêtre **Type de chiffrement** s'affiche uniquement si vous avez sélectionné **Postes de travail** en tant que zone de protection et **Microsoft Windows** en tant que plateforme.

Une fois que vous avez sélectionné un type de chiffrement, la liste des paquets de distribution des deux types de cryptage s'affiche. Un paquet de distribution avec le type de chiffrement choisi est sélectionné dans la liste. La langue du paquet de distribution correspond à la langue de Kaspersky Security Center. Si aucun paquet de distribution de Kaspersky Endpoint Security for Windows n'existe pour la langue de Kaspersky Security Center, le paquet de distribution anglais est sélectionné.

Dans la liste, vous pouvez sélectionner les langues du paquet de distribution au moyen la liste déroulante **Afficher la langue de la Console d'administration ou**.

Les distributifs des applications administrées peuvent nécessiter l'installation d'une version minimale spécifique de Kaspersky Security Center.

Dans la liste, vous pouvez sélectionner des paquets de distribution de tout type de chiffrement différent de celui que vous avez sélectionné dans la fenêtre **Type de chiffrement**. Une fois que vous avez sélectionné un paquet de distribution pour Kaspersky Endpoint Security for Windows, le téléchargement des paquets de distribution correspondant aux modules et platesformes démarre. Vous pouvez suivre la progression du téléchargement dans la colonne **État de téléchargement**. Une fois que l'Assistant de configuration initiale de l'application a terminé, des paquets d'installation pour l'Agent d'administration pour Windows et les applications administrées de Kaspersky s'affichent dans la liste **Serveur d'administration → Avancé → Installation à distance → Paquets d'installation**.

Pour terminer le téléchargement de certains paquets de distribution, vous devez accepter le CLUF. Lorsque vous cliquez sur le bouton **Accepter**, le texte du CLUF s'affiche. Pour passer à l'étape suivante de l'Assistant, vous devez accepter les termes et conditions du CLUF et les termes et conditions de la politique de confidentialité de Kaspersky. Sélectionnez les options relatives au CLUF et à la politique de confidentialité de Kaspersky, puis cliquez sur le bouton **Accepter tout**. Si vous n'acceptez pas les termes et conditions, le téléchargement du paquet est annulé.

Une fois que vous avez accepté les termes et conditions du CLUF et les termes et conditions de la politique de confidentialité de Kaspersky, le téléchargement des paquets de distribution se poursuit. Une fois le téléchargement terminé, l'état **Le paquet d'installation a été créé** est affiché. Par la suite, vous pouvez utiliser les paquets d'installation pour déployer des applications Kaspersky sur les appareils clients.

Vous pouvez créer des paquets d'installation manuellement, indépendamment de l'Assistant de configuration initiale de l'application. Dans l'arborescence de la Console d'administration, accédez au **Serveur d'administration** → **Avancé** → **Installation à distance** → **Paquets d'installation**.

Étape 6. Configuration de Kaspersky Security Network

Vous pouvez accéder aux bases de données de réputation de Kaspersky Security Network pour garantir une vitesse de réaction plus élevée des applications de Kaspersky face aux menaces, augmenter l'efficacité de fonctionnement de certains modules de protection, ainsi que diminuer le risque de faux positifs.

Lisez la Déclaration KSN affichée dans la fenêtre. Indiquer les paramètres du transfert des informations sur le fonctionnement de Kaspersky Security Center dans la base de connaissances de Kaspersky Security Network. Sélectionnez l'une des options ci-dessous :

- **J'&accepte les termes du Kaspersky Security Network**

  Kaspersky Security Center et les applications administrées installées sur les appareils client transfèrent automatiquement les détails de leurs opérations à Kaspersky Security Network. La coopération avec Kaspersky Security Network garantit une mise à jour plus rapide des bases de données sur les virus et les menaces, ce qui améliore la vitesse de réaction face aux menaces naissantes.

- **Je refuse les termes du Kaspersky Security Network**

  Kaspersky Security Center et les applications administrées ne fourniront aucune information à Kaspersky Security Network.

  Si vous sélectionnez cette option, l'utilisation de Kaspersky Security Network sera désactivée.

Si vous avez téléchargé le plug-in Kaspersky Endpoint Security for Windows, les deux déclarations KSN (la Déclaration KSN pour Kaspersky Security Center et la Déclaration KSN pour Kaspersky Endpoint Security for Windows) s'affichent. Les instructions KSN des autres applications Kaspersky administrées dont les plug-ins ont été téléchargés sont affichées dans des fenêtres distinctes et vous devez accepter (ou ne pas accepter) chacune des instructions séparément.

Vous pouvez également configurer l'accès du Serveur d'administration à Kaspersky Security Network (KSN) ultérieurement dans la fenêtre des propriétés du Serveur d'administration de la Console d'administration.

Étape 7. Configuration des notifications par email

Configurez l'envoi des notifications sur les événements enregistrés lors du travail avec les applications de Kaspersky sur les appareils administrés. Ces paramètres sont utilisés comme paramètres par défaut pour le Serveur d'administration.

Pour configurer la diffusion des notifications relatives aux événements qui surviennent dans les applications de Kaspersky, utilisez les paramètres suivants :

- **Destinataires (adresses email)**

  Les adresses email des utilisateurs auxquels l'application va envoyer les notifications. Vous pouvez entrer une ou plusieurs adresse(s). Si vous entrez plusieurs adresses, séparez-les par un point-virgule.

- **Serveurs SMTP**

  L'adresse ou les adresses des serveurs de messagerie de votre organisation.

  Si vous entrez plusieurs adresses, séparez-les par un point-virgule. Vous pouvez utiliser les valeurs suivantes du paramètre :

  - Adresse IPv4 ou IPv6
  - Nom de réseau Windows (nom NetBIOS) de l'appareil
  - Nom complet du serveur SMTP

- **Port du serveur SMTP**

  Numéro du port de communication du serveur SMTP. Si vous utilisez plusieurs serveurs SMTP, la connexion à ceux-ci est établie via le port de communication indiqué. Le numéro de port par défaut est 25.

- **Utiliser l'authentification &ESMTP**

  Activation de la prise en charge de l'authentification ESMTP. Après avoir coché la case, dans les champs **Nom d'utilisateur** et **Mot de passe**, vous pouvez définir les paramètres d'authentification ESMTP. Celle-ci est décochée par défaut.

- **Paramètres**

  Définissez les paramètres suivants :

  - **Objet** (objet d'un email)
  - **Adresse email de l'expéditeur**
  - **Paramètres TLS pour le serveur SMTP**

  Vous pouvez spécifier les paramètres TLS pour le serveur SMTP :

  Vous pouvez désactiver l'utilisation de TLS, utiliser TLS si le serveur SMTP prend en charge ce protocole ou vous pouvez forcer l'utilisation de TLS uniquement. Si vous choisissez d'utiliser uniquement TLS, spécifiez un certificat pour l'authentification du serveur SMTP et choisissez si vous souhaitez activer la communication via n'importe quelle version de TLS ou uniquement via TLS 1.2 ou les versions ultérieures. De plus, si vous choisissez d'utiliser uniquement TLS, vous pouvez spécifier un certificat pour l'authentification du client sur le serveur SMTP.

  - Recherchez un fichier de certificat de serveur SMTP :

  Vous pouvez recevoir un fichier avec la liste des certificats de l'autorité de certification de confiance et charger le fichier sur le Serveur d'administration. Kaspersky Security Center vérifie si le certificat d'un serveur SMTP est également signé par une autorité de certification de confiance ou non. Kaspersky Security Center ne peut pas se connecter à un serveur SMTP si le certificat du serveur SMTP ne provient pas d'une autorité de certification de confiance.

  - Recherchez un fichier de certificat client :

  Vous pouvez utiliser un certificat que vous avez reçu de n'importe quelle source, par exemple, de n'importe quelle autorité de certification de confiance. Vous devez spécifier le certificat et sa clé privée en utilisant l'un des types de certificats suivants :

  - Certificat X-509 :

  Spécifiez le fichier avec le certificat et le fichier avec la clé privée. Vous pouvez télécharger ces fichiers dans n'importe quel ordre. Lorsque les deux fichiers sont téléchargés, indiquez le mot de passe pour déchiffrer la clé privée. Le mot de passe peut présenter une valeur vide si la clé privée n'est pas chiffrée.

  - Conteneur pkcs12 :

  Vous devez charger un seul fichier contenant le certificat et sa clé privée. Lorsque le fichier est chargé, vous devez ensuite indiquer le mot de passe pour décoder la clé privée. Le mot de passe peut présenter une valeur vide si la clé privée n'est pas encodée.

Vous pouvez vérifier les paramètres définis pour l'envoi des notifications par email à l'aide du bouton **&Envoyer un message d'essai**.

Vous pouvez aussi configurer les notifications relatives aux événements, indépendamment de l'Assistant de démarrage rapide.

Étape 8. Configuration de la gestion des mises à jour

Configurez les paramètres d'utilisation des mises à jour des applications installées sur les appareils clients.

Vous ne pouvez configurer ces paramètres que si vous avez fourni une clé de licence dotée de l'option de gestion des vulnérabilités et des correctifs.

Dans le groupe de paramètres **Mode de recherche et d'installation des mises à jour**, vous pouvez sélectionner un mode de recherche et d'installation des mise à jour de Kaspersky Security Center :

- **Rechercher des mises à jour requises**

  La tâche *Recherche de vulnérabilités et de mises à jour requises* est créée automatiquement, si vous n'en avez pas.

  Par défaut, cette option est sélectionnée.

- **Rechercher et installer les mises à jour requises**

  Les tâches *Recherche de vulnérabilités et de mises à jour requises* et *Installation des mises à jour requises et correction des vulnérabilités* sont créées automatiquement, si vous n'en avez pas.

Dans le groupe de paramètres **Windows Server Update Services**, vous pouvez sélectionner la source de synchronisation des mises à jour :

- **Utiliser des sources de mise à jour définies dans la stratégie de domaine**

  Les appareils clients téléchargent les mises à jour de Windows Update en fonction des paramètres de stratégie de votre domaine. La stratégie d'Agent d'administration est créée automatiquement si vous n'en avez pas.

- **&Utiliser le Serveur d'administration comme serveur WSUS**

  Les appareils clients téléchargent les mises à jour Windows Update à partir du Serveur d'administration. La tâche *Synchronisation des mises à jour Windows Update* et la stratégie d'Agent d'administration sont créées automatiquement, si vous n'en avez pas.

Vous pouvez créer les tâches *Rechercher les vulnérabilités et les mises à jour requises* et *Installation des mises à jour requises et correction des vulnérabilités* séparément de l'Assistant de configuration initiale de l'application. Pour utiliser le Serveur d'administration comme serveur WSUS, créez la tâche *Synchronisation des mises à jour Windows Update* et puis sélectionner l'option **&Utiliser le Serveur d'administration comme serveur WSUS** dans la stratégie de l'Agent d'administration.

Étape 9. Création de la configuration initiale de la protection

La fenêtre **Création de la configuration initiale de la protection** affiche une liste des stratégies et tâches qui sont créées automatiquement. Les politiques et tâches suivantes sont créées :

- Stratégie de l'Agent d'administration de Kaspersky Security Center
- Stratégies pour les applications Kaspersky administrées dont les plug-ins d'administration ont été installés auparavant
- Tâche Maintenance du Serveur d'administration
- Sauvegarde des données du Serveur d'administration
- Téléchargement des mises à jour sur le stockage du Serveur d'administration
- Tâche Recherche de vulnérabilités et de mises à jour requises
- Installer la mise à jour

Avant de passer à l'étape suivante de l'Assistant, attendez la fin de la création des stratégies et des tâches.

Si vous avez téléchargé et installé le plug-in pour Kaspersky Endpoint Security for Windows 10 Service Pack 1 et versions ultérieures jusqu'à la v.11.0.1, lors de la création des stratégies et des tâches, une fenêtre s'ouvre pour la configuration initiale de la zone de confiance de Kaspersky Endpoint Security for Windows. L'application propose d'ajouter à la zone de confiance les éditeurs vérifiés par Kaspersky afin d'exclure leurs applications de l'analyse et d'éviter ainsi des blocages accidentels. Vous pouvez créer les exclusions recommandées à ce stade, ou créer une liste d'exclusions ultérieurement en effectuant la sélection suivante dans l'arborescence de la console : **Stratégies** → menu des propriétés de Kaspersky Endpoint Security → **Protection avancée** → **Zone de confiance** → **Paramètres** → **Ajouter**. La liste des exclusions de l'analyse peut être modifiée à tout moment pendant l'utilisation ultérieure de l'application.

La manipulation de la zone de confiance s'opère à l'aide des moyens de l'application Kaspersky Endpoint Security for Windows. Les instructions détaillées sur l'exécution des opérations et la description des particularités de fonctionnalité de chiffrement sont décrites dans l'Aide en ligne de Kaspersky Endpoint Security for Windows.

Pour terminer la configuration initiale de la zone de confiance et revenir à l'Assistant, cliquez sur **OK**.

Cliquez sur **Suivant**. Ce bouton est disponible après la configuration de toutes les stratégies et tâches indispensables.

Vous pouvez également créer les tâches et les stratégies requises ultérieurement, indépendamment de l'Assistant de configuration initiale de l'application.

Étape 10. Connexion pour les appareils mobiles

Si vous avez activé la zone de protection des **Mobile devices** dans les paramètres de l'Assistant au préalable, spécifiez les paramètres de connexion des appareils mobiles d'entreprise de l'organisation administrée. Si vous n'avez pas activé la zone de protection des **Appareils mobiles**, cette étape est ignorée.

À cette étape de l'Assistant, procédez comme suit :

- Configurer les ports de connexion des appareils mobiles
- Configurer le Serveur d'administration pour l'authentication
- Créer ou gérer les certificats
- Configurer l'émission, les mises à jour automatiques, et le chiffrement de certificats généraux
- Créer une règle de déplacement pour les appareils mobiles

Pour configurer les ports de configurer les ports de connexion des appareils mobiles, procédez comme suit :

1. Cliquez sur le bouton **Configurer** à droite du champ **Connexion des appareils mobiles**.
2. Dans la liste déroulante, sélectionnez **Configurer les ports**.
   La fenêtre des propriétés du Serveur d'administration s'ouvre à la section **Ports supplémentaires**.

3. La section **Ports supplémentaires** permet de spécifier les paramètres de connexion de l'appareil mobile :

- **Port SSL pour le serveur proxy d'activation**

  Numéro du port SSL pour connecter Kaspersky Endpoint Security for Windows aux serveurs d'activation de Kaspersky.

  Le numéro de port par défaut est 17000.

- **Ouvrir le port pour les appareils mobiles**

  Un port s'ouvre pour les appareils mobiles en vue de la connexion au serveur de licences. Vous pouvez définir le numéro du port et d'autres paramètres dans les champs plus bas.

  Cette option est activée par défaut.

- **Port pour la synchronisation des appareils mobiles**

  Numéro du port utilisé pour la connexion des appareils mobiles au Serveur d'administration et l'échange d'informations avec ceux-ci. Le numéro de port par défaut est 13292.

  Vous pouvez désigner un autre port, si le port 13292 est utilisé à d'autres fins.

- **Port pour l'activation des appareils mobiles**

  Port de connexion de Kaspersky Endpoint Security for Android aux serveurs d'activation de Kaspersky.

  Le numéro de port par défaut est 17100.

- **Ouvrir le port pour les appareils protégés au niveau UEFI et KasperskyOS**

  Les appareils protégés au niveau UEFI peuvent se connecter au Serveur d'administration.

- **Port pour les appareils protégés au niveau UEFI et KasperskyOS**

  Vous pouvez modifier le numéro de port si l'option **Ouvrir le port pour les appareils protégés au niveau UEFI et KasperskyOS** est activée. Le numéro de port par défaut est 13294.

- **Ouvrir les ports pour Prometheus**

  Le port pour les requêtes d'extraction Prometheus. Le numéro de port par défaut est 13296.

4. Cliquez sur le bouton **OK** pour enregistrer les modifications et revenir à l'Assistant de configuration initiale de l'application.

Il vous faudra configurer l'authentification du Serveur d'administration par les appareils mobiles et l'authentification des appareils mobiles par le Serveur d'administration. Si vous le désirez, vous pouvez également procéder à la configuration de l'authentification plus tard, indépendamment de l'Assistant de configuration initiale de l'application.

Pour configurer les paramètres d'authentification du Serveur d'administration par les appareils mobiles, procédez comme suit :

1. Cliquez sur le bouton **Configurer** à droite du champ **Connexion des appareils mobiles**.

2. Choisissez l'option **C&onfigurer l'authentification** dans la liste déroulante.

   La fenêtre des propriétés du Serveur d'administration s'ouvre à la section **Certificats**.

3. Sélectionnez l'option d'authentification pour les appareils mobiles dans le groupe de paramètres **Authentification du Serveur d'administration par les appareils mobiles** et sélectionnez l'option d'authentification pour les appareils protégé au niveau UEFI dans le groupe de paramètres **Authentification du Serveur d'administration par les appareils protégés au niveau UEFI**.

   Ce certificat sert à l'authentification du Serveur d'administration lors de l'échange d'informations avec les appareils clients.

   L'option choisie par défaut est celle de l'utilisation du certificat créé lors de l'installation du Serveur d'administration. Si vous le voulez, vous pouvez ajouter un nouveau certificat.

Pour ajouter un nouveau certificat (facultatif) :

1. Sélectionnez **Autre certificat**.

   Le bouton **Parcourir** apparaît.

2. Cliquez sur le bouton **Parcourir**.

3. Configurez les paramètres du certificat dans la fenêtre qui s'ouvre :

- Type de certificat

  La liste déroulante permet de sélectionner le type de certificat :

  - **Certificat X.509**. Si cette option est sélectionnée, vous devez préciser la clé privée d'un certificat et un certificat ouvert :
    - **Clé privée (.prk, .pem)**. Dans ce champ, cliquez sur le bouton **Parcourir** pour préciser la clé privée d'un certificat au format PKCS #8 (*.prk).
    - **Clé publique (.cer)**. Dans ce champ, cliquez sur le bouton **Parcourir** pour préciser une clé publique au format PEM (*.cer).
  - **Conteneur PKCS#12**. Si vous sélectionnez cette option, vous pouvez indiquer un fichier de certificat au format P12 ou PFX en cliquant sur le bouton **Parcourir** et en remplissant le champ **Fichier du certificat**.

- Délai d'activation :
  - Immédiatement

    Le certificat actuel est remplacé par le nouveau certificat directement après que vous avez cliqué sur **OK**.

    Les appareils mobiles déjà connectés ne pourront plus se connecter au Serveur d'administration.

  - Dans le délai indiqué (jours)

    Si vous choisissez cette option, un certificat de réserve est généré. Le certificat actuel est remplacé par le nouveau à l'issue du nombre de jours indiqué. La date à partir de laquelle le certificat de réserve entre en vigueur s'affiche dans la section **Certificats**.

    Il est recommandé de planifier la réémission au préalable. Le certificat de réserve doit être téléchargé sur les appareils mobiles avant l'expiration de la période spécifiée. Une fois que le certificat actuel a été remplacé par le nouveau certificat, les appareils mobiles déjà connectés qui ne disposent pas du certificat de réserve ne pourront plus se connecter au Serveur d'administration.

4. Cliquez sur le bouton **Propriétés** pour afficher les paramètres du certificat de Serveur d'administration sélectionné.

Pour réémettre un certificat émis via le Serveur d'administration :

1. Sélectionnez **Le certificat a été émis via le Serveur d'administration**.
2. Cliquez sur le bouton **Réémettre**.
3. Dans la fenêtre qui s'ouvre, configurez les paramètres suivants :
   - Adresse de connexion :
     - Conserver l'adresse de connexion antérieure

L'adresse du Serveur d'administration auquel les appareils mobiles vont être connectés reste identique.

Par défaut, cette option est sélectionnée.

- **Modifier l'adresse de connexion sur**

  S'il est nécessaire que les appareils mobiles se connectent à une autre adresse, indiquez-la dans le champ.

  En cas de modification de l'adresse de connexion des appareils mobiles, il faut émettre un nouveau certificat. L'ancien certificat ne sera pas valide sur les appareils mobiles connectés. Les appareils déjà connectés ne pourront plus se connecter au Serveur d'administration et ne seront plus administrés.

- Délai d'activation :

  - **Immédiatement**

    Le certificat actuel est remplacé par le nouveau certificat directement après que vous avez cliqué sur **OK**.

    Les appareils mobiles déjà connectés ne pourront plus se connecter au Serveur d'administration.

  - **Dans le délai indiqué (jours)**

    Si vous choisissez cette option, un certificat de réserve est généré. Le certificat actuel est remplacé par le nouveau à l'issue du nombre de jours indiqué. La date à partir de laquelle le certificat de réserve entre en vigueur s'affiche dans la section **Certificats**.

    Il est recommandé de planifier la réémission au préalable. Le certificat de réserve doit être téléchargé sur les appareils mobiles avant l'expiration de la période spécifiée. Une fois que le certificat actuel a été remplacé par le nouveau certificat, les appareils mobiles déjà connectés qui ne disposent pas du certificat de réserve ne pourront plus se connecter au Serveur d'administration.

4. Cliquez sur le bouton **OK** pour enregistrer les modifications et revenir à la fenêtre **Certificats**.

5. Cliquez sur le bouton **OK** pour enregistrer les modifications et revenir à l'Assistant de configuration initiale de l'application.

Pour personnaliser l'émission, la mise à jour automatique et le chiffrement des certificats de type général pour l'identification des appareils mobiles par le Serveur d'administration, procédez comme suit :

1. Cliquez sur le bouton **Configurer** à droite du champ **Authentification de l'appareil mobile**.

   La fenêtre **Règles d'émission des certificats** s'ouvre, sur la section **Émission des certificats de messagerie**.

2. Le cas échéant, configurez les paramètres suivants dans la section **Paramètres d'émission** :

   - **Durée de validité du certificat, jours**

     Durée de validité du certificat en jours. Par défaut, la durée de validité du certificat est de 365 jours. À l'expiration de ce délai, l'appareil mobile ne peut plus se connecter au Serveur d'administration.

   - **Source du certificat**

     Sélection de la source du certificat de type général pour les appareils mobiles : les certificats sont émis par le Serveur d'administration ou définis manuellement.

     Vous pouvez modifier le modèle de certificat si l'intégration à l'infrastructure à clés publiques a été configurée dans la section **Intégration avec PKI**. Dans ce cas, vous pouvez sélectionner les champs suivants de sélection du modèle :

   - **Modèle par défaut**

     Utilisation du certificat émis par une source des certificats externe (centre de certification) selon le modèle défini par défaut.

     Cette option est sélectionnée par défaut.

   - **Autre modèle**

     Choix du modèle sur la base duquel les certificats vont être émis. Les modèles de certificat peuvent être définis dans le domaine. Le bouton **Actualiser la liste** permet d'actualiser la liste des modèles de certificat.

3. Le cas échéant, définissez les paramètres suivants d'émission automatique des certificats dans la section **Paramètres des mises à jour automatiques** :

   - **Mettre à jour lorsqu'il reste le nombre de jours suivant avant la fin de la durée de validité du certificat (jours)**

     Nombre de jours séparant le moment où le Serveur d'administration doit émettre un nouveau certificat et la fin de la durée de validité du certificat actuel. Par exemple, si la valeur 4 est indiquée dans le champ, le Serveur d'administration émet un nouveau certificat quatre jours avant la fin de la durée de validité du certificat actuel. La valeur par défaut est égale à 7.

   - **Réémettre automatiquement le certificat si possible**

     Sélectionnez cette option pour réémettre automatiquement un certificat pour le nombre de jours spécifié dans le champ **Mettre à jour lorsqu'il reste le nombre de jours suivant avant la fin de la durée de validité du certificat (jours)**. Si un certificat a été défini manuellement, il ne peut pas être renouvelé automatiquement et l'option activée ne fonctionnera pas.

     Cette option est Inactif par défaut.

   Les certificats sont mis à jour automatiquement par le centre de certification.

4. Le cas échéant, dans la section des paramètres, **Protection par mot de passe**, spécifiez les paramètres de déchiffrement des certificats pendant l'installation.

   Sélectionnez l'option **Demander le mot de passe lors de l'installation du certificat** afin que l'utilisateur soit invité à saisir le mot de passe lors de l'installation du certificat sur un appareil mobile. Le mot de passe est utilisé seulement une fois, lors de l'installation du certificat sur l'appareil mobile.

   Le mot de passe est créé automatiquement par les outils du Serveur d'administration et envoyé à l'adresse email que vous avez définie. Vous pouvez indiquer l'adresse email de l'utilisateur ou la vôtre, si vous souhaitez transmettre le mot de passe à l'utilisateur par la suite via une autre méthode.

   Vous pouvez définir le nombre de caractères du mot de passe de déchiffrement du certificat à l'aide du curseur.

   La fonction de saisie du mot de passe est requise, par exemple, pour protéger un certificat général dans le paquet d'installation autonome de Kaspersky Endpoint Security for Android. La protection par le mot de passe empêche l'accès d'un individu malintentionné au certificat général en cas de vol du paquet d'installation autonome sur le Serveur Web de Kaspersky Security Center.

   Si cette option est désactivée, le déchiffrement du certificat lors de l'installation se produit automatiquement et l'utilisateur n'est pas invité à saisir le mot de passe. Cette option est Inactif par défaut.

5. Cliquez sur le bouton **OK** pour enregistrer les modifications et revenir à la fenêtre de l'Assistant de configuration initiale de l'application.

   Cliquez sur le bouton **Annuler** pour revenir à l'Assistant de configuration initiale de l'application sans enregistrer les modifications effectuées.

Pour activer la fonction de déplacement des appareils mobiles dans le groupe d'administration qui vous intéresse,

Dans le champ **Déplacement automatique des appareils mobiles**, sélectionnez l'option **Créer une règle de déplacement des appareils mobiles**.

Si l'option **Créer une règle de déplacement des appareils mobiles** est sélectionnée, l'application crée automatiquement une règle de déplacement qui déplace les appareils exécutant Android et iOS dans le groupe **Appareils administrés** :

- Appareils Android dotés de Kaspersky Endpoint Security for Android et d'un certificat de messagerie
- Avec les systèmes d'exploitation sur lesquels le profil MDM iOS avec un certificat partagé est installé

Si une telle règle existe déjà, l'application ne crée pas la règle.

Cette option est Inactif par défaut.

Kaspersky ne prend plus en charge Kaspersky Safe Browser.

Étape 11. Téléchargement des mises à jour

Les mises à jour des bases antivirus pour Kaspersky Security Center et les applications administrées de Kaspersky sont téléchargées automatiquement. Les mises à jour requises sont automatiquement téléchargées depuis des Serveurs Kaspersky.

Pour télécharger les mises à jour séparément de l'Assistant de configuration initiale de l'application, créez et configurez la tâche *Télécharger les mises à jour dans le stockage du Serveur d'Administration*.

Étape 12. Recherche d'appareils

La fenêtre **Sondage du réseau** affiche les informations sur l'état du sondage du réseau exécuté par le Serveur d'administration.

Vous pouvez consulter les appareils détectés sur le réseau par le Serveur d'administration et obtenir une aide sur l'utilisation de la fenêtre **Recherche d'appareils** en cliquant dans la partie inférieure de la fenêtre.

Vous pouvez interroger votre réseau ultérieurement, indépendamment de l'Assistant de configuration initiale de l'application. Utilisez la Console d'administration pour configurer le sondage des domaines Windows, Active Directory, des plages IP et des réseaux IPv6.

Étape 13. Fin de l'Assistant de configuration initiale de l'application

Dans la fenêtre de fin de l'Assistant de configuration initiale de l'application, sélectionnez l'option **Exécuter l'Assistant de l'installation à distance** si vous voulez lancer l'installation automatique des applications antivirus et/ou de l'Agent d'administration sur les appareils de votre réseau.

Cliquez sur **Terminer** pour terminer le travail de l'Assistant.

Configuration de la connexion de la Console d'administration au Serveur d'administration

La Console d'administration est connectée au Serveur d'administration via le port SSL TCP 13291. Le même port peut être utilisé par les objets d'automatisation de l'utilitaire klakaut.

Le port TCP 14000 peut être utilisé pour connecter la Console d'administration, les points de distribution, les Serveurs d'administration secondaires et les objets d'automatisation de l'utilitaire klakaut, ainsi que pour recevoir des données depuis les appareils clients.

En général, le port SSL TCP 13000 peut être utilisé uniquement par l'Agent d'administration, un Serveur d'administration secondaire et le Serveur d'administration principal installé en zone démilitarisée. Dans certains cas, la connexion de la Console d'administration devra être établie via le port SSL 13000 :

- Si un port SSL unique doit être utilisé aussi bien pour la Console d'administration que pour les autres activités (la réception des données depuis les appareils clients, la connexion des points de distribution, la connexion des Serveurs d'administration secondaires).
- Si un objet d'automatisation de l'utilitaire klakaut n'est pas connecté au Serveur d'administration directement, mais par le point de distribution situé en zone démilitarisée.

Pour permettre la connexion de la Console d'administration via le port 13000, procédez comme suit :

1. Ouvrez le registre système de l'appareil sur lequel le Serveur d'administration est installé, par exemple, à l'aide de la commande regedit dans le menu **Démarrer** → **Exécuter**.
2. Rendez-vous dans la section :
   - Pour les systèmes 32 bits :

     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\.core\.independent\KLLIM
   - Pour les systèmes 64 bits :

     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\.core\.independent\
3. Pour la clé LP_ConsoleMustUsePort13291 (DWORD), sélectionnez la valeur 00000000.

   Par défaut, la valeur 1 est indiquée pour cette clé.
4. Relancez le service du Serveur d'administration.

La Console d'administration pourra ainsi se connecter au Serveur d'administration via le port 13000.

Configuration des paramètres d'accès Internet du Serveur d'administration.

Vous devez configurer l'accès à Internet pour utiliser Kaspersky Security Network et télécharger les mises à jour des bases antivirus pour Kaspersky Security Center et les applications Kaspersky administrées.

Pour indiquer les paramètres d'accès Internet du Serveur d'administration :

1. Dans l'arborescence de la console, sélectionnez l'entrée **Serveur d'administration %s**.
2. Dans le menu contextuel Serveur d'administration, sélectionnez l'option **Propriétés**.
3. Dans la fenêtre des propriétés du Serveur d'administration, accédez à **Avancé → Paramètres d'accès au réseau Internet**
4. Sélectionnez l'option **Utiliser un serveur proxy** si vous souhaitez utiliser un serveur proxy pour vous connecter à Internet. Si cette option est sélectionnée, les champs de saisie des paramètres sont accessibles. Configurez les paramètres suivants de connexion au serveur proxy :

   - **Adresse**

     Adresse du serveur proxy pour la connexion de Kaspersky Security Center à Internet.

   - **Numéro de port**

     Numéro du port via lequel la connexion proxy à Kaspersky Security Center sera établie.

   - **Ne pas utiliser le serveur proxy pour les adresses locales**

     Le serveur proxy n'est pas utilisé lors de la connexion aux appareils dans le réseau local.

   - **Authentification du serveur proxy**

     Si la case est cochée, les champs de saisie permettent d'indiquer les identifiants pour l'authentification sur le serveur proxy.

     Ce champ de saisie est accessible si la case **Utiliser un serveur proxy** est cochée.

   - **Nom d'utilisateur**

     Compte utilisateur sous lequel la connexion au serveur proxy est établie (ce champ est disponible si la case **Authentification du serveur proxy** est cochée).

   - **Mot de passe**

     Mot de passe défini par l'utilisateur sous le compte duquel la connexion au serveur proxy est établie (ce champ est disponible si la case **Authentification du serveur proxy** est cochée).

     Pour voir le mot de passe saisi, cliquez sur le bouton **Afficher** et maintenez-le enfoncé aussi longtemps que vous en avez besoin.

Vous pouvez également configurer l'accès à Internet à l'aide de l'Assistant de configuration initiale de l'application.

Connexion d'appareils itinérants

Cette section décrit comment connecter au Serveur d'administration des appareils itinérants (c'est-à-dire des appareils administrés situés en dehors du réseau principal).

Scénario : connexion d'appareils itinérants via une passerelle de connexion

Ce scénario décrit comment connecter au Serveur d'administration des appareils administrés situés en dehors du réseau principal.

Prérequis

Le scénario prévoit les conditions préalables suivantes :

- Une zone démilitarisée (DMZ) est organisée dans le réseau de votre organisation.
- Le Serveur d'administration de Kaspersky Security Center Administration est déployé sur le réseau de l'organisation.

Étapes

Ce scénario se déroule par étapes :

1. **Sélection d'un appareil client dans la DMZ**

   Cet appareil sera utilisé comme passerelle de connexion L'appareil que vous sélectionnez doit répondre aux exigences en matière de passerelles de connexion.

2. **Installation de l'Agent d'administration dans le rôle de passerelle de connexion**

   Nous vous recommandons d'utiliser une installation locale pour installer l'Agent d'administration sur l'appareil sélectionné.

   Par défaut, le fichier d'installation se trouve à l'adresse suivante : \\<nom du serveur>\KLSHARE\PkgInst\NetAgent_<numéro de la version>

   Dans la fenêtre **Passerelle de connexion** de l'Assistant d'installation de l'Agent d'administration, sélectionnez l'option **Utiliser l'Agent d'administration en tant que passerelle de connexion en DMZ**. Ce mode active simultanément le rôle de passerelle de connexion et indique à l'Agent d'administration d'attendre les connexions du Serveur d'administration plutôt que d'établir des connexions avec le Serveur d'administration.

   Vous pouvez également installer l'Agent d'administration sur un appareil Linux et le configurer pour qu'il fonctionne en tant que passerelle de connexion, mais faites attention à la liste des limitations de l'Agent d'administration s'exécutant sur les appareils Linux.

3. **Autorisation de connexions dans les pare-feux sur la passerelle de connexion**

   Pour vous assurer que le Serveur d'administration peut réellement se connecter à la passerelle de connexion dans la DMZ, autorisez les connexions au port TCP 13000 dans tous les pare-feux entre le Serveur d'administration et la passerelle de connexion.

   Si la passerelle de connexion ne dispose d'aucune adresse IP réelle sur Internet, mais se trouve plutôt derrière une Traduction d'adresses réseau (NAT), configurez une règle pour transférer les connexions via la NAT.

4 Création d'un groupe d'administration pour les appareils externes

Créez un nouveau groupe sous le groupe **Appareils administrés**. Ce nouveau groupe contiendra des appareils externes administrés.

5 Connexion de la passerelle de connexion au Serveur d'administration

La passerelle de connexion que vous avez configurée attend une connexion à partir du Serveur d'administration. Cependant, le Serveur d'administration n'énumère pas l'appareil avec la passerelle de connexion parmi les appareils administrés. Cela est dû au fait que la passerelle de connexion n'a pas tenté d'établir une connexion avec le Serveur d'administration. Par conséquent, vous avez besoin d'une procédure spéciale pour vous assurer que le Serveur d'administration amorce une connexion à la passerelle de connexion.

Procédez comme suit :

1. Ajoutez la passerelle de connexion en tant que point de distribution.
2. Déplacez la passerelle de connexion du groupe **Appareils non définis** vers le groupe que vous avez créé pour les appareils externes.

La passerelle de connexion est connectée et configurée.

6 Connexion d'appareils de bureau externes au Serveur d'administration

En règle générale, les appareils de bureau externes ne sont pas déplacés à l'intérieur du périmètre. Par conséquent, vous devez les configurer pour vous connecter au Serveur d'administration via la passerelle lors de l'installation de l'Agent d'administration.

7 Configuration des mises à jour pour les appareils de bureau externes

Si les mises à jour des applications de sécurité sont configurées de manière à être téléchargées à partir du Serveur d'administration, les appareils externes téléchargent les mises à jour via la passerelle de connexion. Ceci présente deux inconvénients :

- Il s'agit d'un trafic inutile, qui occupe la bande passante du canal de communication via Internet de l'entreprise.
- Il ne s'agit pas nécessairement du moyen le plus rapide d'obtenir des mises à jour. Il est très probable qu'il serait moins coûteux et plus rapide pour les appareils externes de recevoir les mises à jour à partir des serveurs de mise à jour de Kaspersky.

Procédez comme suit :

1. Déplacez tous les appareils externes vers le groupe d'administration distinct que vous avez créé précédemment.
2. Excluez le groupe contenant les appareils externes de la tâche de mise à jour.
3. Créez une tâche de mise à jour distincte pour le groupe contenant les appareils externes.

8 Connexion d'ordinateurs portables itinérants au Serveur d'administration

Les ordinateurs portables itinérants se trouvent parfois au sein du réseau, et parfois en dehors de celui-ci. Pour assurer une gestion efficace, vous avez besoin qu'ils se connectent au Serveur d'administration différemment en fonction de leur position. Pour utiliser le trafic de manière efficace, ils doivent également recevoir des mises à jour de différentes sources en fonction de leur position.

Vous devez configurer des règles pour les utilisateurs itinérants : profils de connexion et descriptions d'emplacement réseau. Chaque règle définit l'instance de Serveur d'administration à laquelle les ordinateurs portables itinérants doivent se connecter en fonction de leur position et l'instance de Serveur d'administration à partir de laquelle ils doivent recevoir les mises à jour.

Scénario : Connexion d'appareils itinérants via un Serveur d'administration secondaire dans la DMZ

Si vous souhaitez connecter au Serveur d'administration des appareils administrés situés en dehors du réseau principal, vous pouvez le faire à l'aide d'un Serveur d'administration secondaire situé dans la zone démilitarisée (DMZ).

Prérequis

Avant de démarrer, assurez-vous que vous avez :

- Une zone démilitarisée (DMZ) est organisée dans le réseau de votre organisation.
- Le serveur d'administration de Kaspersky Security Center est déployé sur le réseau interne de l'organisation.

Étapes

Ce scénario se déroule par étapes :

1. **Sélection d'un appareil client dans la DMZ**

   Dans le DMZ, sélectionnez un appareil client qui va servir de Serveur d'administration secondaire.

2. **Installation du Serveur d'administration de Kaspersky Security Center**

   Installer le Serveur d'administration de Kaspersky Security Center sur cet appareil client.

3. **Création d'une hiérarchie des Serveurs d'administration**

   Si vous placez un Serveur d'administration secondaire dans la DMZ, le Serveur d'administration secondaire doit recevoir une connexion du Serveur d'administration primaire. Pour ce faire, ajoutez un nouveau Serveur d'administration à titre de Serveur secondaire de telle sorte que le Serveur d'administration primaire se connecte au Serveur d'administration secondaire via le port 13000. Lorsque vous combinez deux Serveurs d'administration dans une hiérarchie, assurez-vous que le port 13291 est accessible sur les deux Serveurs d'administration. La connexion de la Console d'administration au Serveur d'administration s'opère via le port 13291.

4. **Connexion des appareils administrés hors du bureau au Serveur d'administration secondaire**

   Vous pouvez connecter des appareils itinérants au Serveur d'administration dans la DMZ de la même manière qu'une connexion s'opère entre le Serveur d'administration et les appareils administrés dans le réseau principal. Les appareils administrés itinérants initient la connexion via le port 13000.

À propos de la connexion d'appareils itinérants

Certains appareils administrés se trouvent toujours en dehors du réseau principal (par exemple, les appareils dans les succursales régionales d'une entreprise ; les kiosques, les distributeurs de billets et les terminaux installés dans différents points de vente ; les appareils dans les bureaux à domicile des employés). Certains appareils sortent du périmètre de temps en temps (par exemple, les ordinateurs portables des utilisateurs qui visitent les succursales régionales ou le bureau d'un client).

Vous devez toujours surveiller et administrer la protection des appareils itinérants : recevoir des informations réelles sur leur état de la protection et maintenir leurs applications de sécurité à jour. Cela est nécessaire, car, par exemple, si un tel appareil est compromis alors qu'il est éloigné du réseau principal, il pourrait devenir une plateforme de propagation de menaces dès qu'il se connecte au réseau principal. Pour connecter des appareils itinérants au Serveur d'administration, vous pouvez utiliser deux méthodes :

- Passerelle de connexion dans la zone démilitarisée (DMZ)

  Voir le schéma de trafic de données : Serveur d'administration sur LAN, appareils administrés sur Internet, passerelle de connexion utilisée

- Serveur d'Administration dans la zone démilitarisée

  Voir le schéma de trafic de données : Serveur d'administration dans la DMZ, appareils administrés sur Internet.

Une passerelle de connexion dans la DMZ

Une méthode recommandée pour connecter des appareils itinérants au Serveur d'administration consiste à organiser une DMZ dans le réseau de l'organisation et à installer une passerelle de connexion dans la DMZ. Les appareils externes se connecteront à la passerelle de connexion, et le Serveur d'administration à l'intérieur du réseau amorcera la connexion aux appareils via la passerelle de connexion.

Par rapport à l'autre méthode, celle-ci est plus sécurisée :

- Il n'est pas nécessaire d'ouvrir l'accès au Serveur d'administration depuis l'extérieur du réseau.
- Une passerelle de connexion compromise ne présente pas un risque élevé pour la sécurité des appareils du réseau. Une passerelle de connexion ne gère rien elle-même et n'établit aucune connexion.

En outre, une passerelle de connexion ne nécessite pas de nombreuses ressources matérielles.

Cependant, cette méthode comporte un processus de configuration plus compliqué :

- Pour qu'un appareil serve de passerelle de connexion dans la DMZ, vous devez installer l'Agent d'administration et le connecter au Serveur d'administration d'une manière très spécifique.
- Vous ne pourrez pas utiliser la même adresse pour vous connecter au Serveur d'administration dans toutes les situations. De l'extérieur du périmètre, vous devrez utiliser non seulement une adresse différente (adresse de passerelle de connexion), mais également un mode de connexion différent : via une passerelle de connexion.
- Vous devez également définir différents paramètres de connexion pour les ordinateurs portables situés à différents endroits.

Pour ajouter une passerelle de connexion à un réseau précédemment configuré, procédez comme suit :

1. Installer l'Agent d'administration en mode passerelle de connexion.
2. Réinstallez l'Agent d'administration sur les appareils que vous souhaitez connecter à la passerelle de connexion récemment ajoutée.

Serveur d'administration dans la DMZ

Une autre méthode consiste à installer un seul Serveur d'administration dans la DMZ.

Cette configuration est moins sécurisée que l'autre méthode. Pour gérer les ordinateurs portables externes dans ce cas, le Serveur d'administration doit accepter les connexions de n'importe quelle adresse sur Internet. Il gérera toujours tous les ordinateurs du réseau interne, mais à partir de la DMZ. Par conséquent, un serveur compromis pourrait causer d'énormes dégâts, malgré la faible probabilité d'un tel événement.

Le risque diminue considérablement si le Serveur d'administration de la DMZ ne gère pas les appareils du réseau interne. Une telle configuration peut être utilisée, par exemple, par un fournisseur de services pour gérer les appareils des clients.

Cette méthode peut être intéressante dans les cas suivants :

- Si vous connaissez bien l'installation et la configuration du Serveur d'administration et que vous ne souhaitez pas effectuer une autre procédure pour installer et configurer une passerelle de connexion.
- Si vous avez besoin de gérer plus d'appareils. La capacité maximale du Serveur d'administration est de 100 000 appareils, tandis qu'une passerelle de connexion peut prendre en charge jusqu'à 10 000 appareils.

Cette solution présente également des difficultés possibles :

- Le Serveur d'administration nécessite plus de ressources matérielles et une base de données supplémentaire.
- Les informations sur les ordinateurs seront stockées dans deux bases de données indépendantes (pour le Serveur d'administration à l'intérieur du réseau et une autre dans la DMZ), ce qui complique la surveillance.
- Pour gérer tous les appareils, le Serveur d'administration doit être intégré dans une hiérarchie, ce qui complique non seulement la surveillance, mais également la gestion. Une instance de Serveur d'administration secondaire impose des limitations sur les structures possibles des groupes d'administration. Vous devez décider quelles tâches et stratégies distribuer à une instance de Serveur d'administration secondaire et la manière de le faire.
- La configuration des appareils externes pour utiliser le Serveur d'administration dans la DMZ depuis l'extérieur et pour utiliser le Serveur d'administration principal depuis l'intérieur n'est pas plus simple que la configuration pour utiliser une connexion conditionnelle via une passerelle.
- Risques de sécurité élevés. Une instance de Serveur d'administration compromise facilite la compromission de ses ordinateurs portables administrés. Si cela se produit, il suffit aux pirates informatiques d'attendre que l'un des ordinateurs portables revienne sur le réseau de l'entreprise afin de pouvoir continuer leur attaque sur le réseau local.

Connexion d'appareils de bureau externes au Serveur d'administration

Les appareils de bureau qui sont toujours en dehors du réseau principal (par exemple, les appareils dans les succursales régionales de l'entreprise ; les kiosques, les distributeurs de billets et les terminaux installés dans différents points de vente ; les appareils dans les bureaux à domicile des employés) ne peuvent pas être connectés directement au Serveur d'administration. Ils doivent être connectés au Serveur d'administration via une passerelle de connexion installée dans une zone démilitarisée (DMZ). Cette configuration est effectuée lors de l'installation de l'Agent d'administration sur ces appareils.

Pour connecter des appareils de bureau externes au Serveur d'administration, procédez comme suit :

1. Créez un paquet d'installation pour l'Agent d'administration.
2. Ouvrez les propriétés du paquet d'installation créé et accédez à la section **Avancé**, puis sélectionnez l'option **Se connecter au Serveur d'administration au moyen d'une passerelle de connexion**.

   Le paramètre **Se connecter au Serveur d'administration au moyen d'une passerelle de connexion** est incompatible avec le paramètre **Utiliser l'Agent d'administration en tant que passerelle de connexion en DMZ**. Vous ne pouvez pas activer ces deux paramètres en même temps.

3. Dans **Adresse de la passerelle de connexion**, indiquez l'adresse publique de la passerelle de connexion.

   Si la passerelle de connexion se trouve derrière une Traduction d'adresses réseau (NAT) et ne dispose pas de sa propre adresse publique, configurez une règle de passerelle NAT pour transférer les connexions de l'adresse publique à l'adresse interne de la passerelle de connexion.

4. Créez un paquet d'installation autonome fondé sur le paquet d'installation créé.
5. Fournissez le paquet d'installation autonome aux appareils cibles par voie électronique ou au moyen d'un disque amovible.
6. Installez l'Agent d'administration à partir du paquet autonome.

Les appareils de bureau externes sont connectés au Serveur d'administration.

À propos des profils de connexion pour les utilisateurs itinérants

Le travail des utilisateurs itinérants avec des ordinateurs portables (ci-après, les " appareils ") peut imposer une modification du mode de connexion au Serveur d'administration ou la permutation entre les Serveurs d'administration en fonction de la situation actuelle de l'appareil sur le réseau.

Les profils des connexions ne sont pris en charge que pour les appareils fonctionnant sous Windows et macOS.

Utilisation de différentes adresses du même Serveur d'administration

Les appareils dotés de l'Agent d'administration peuvent, à différents moments, se connecter au Serveur d'administration depuis le réseau interne de l'entreprise ou depuis Internet. Dans ce cas, il peut être nécessaire que l'Agent d'administration utilise différentes adresses pour la connexion au Serveur d'administration : l'adresse externe du Serveur pour la connexion depuis Internet et l'adresse interne du Serveur pour la connexion depuis le réseau interne.

Pour cela, vous devez ajouter un profil (pour la connexion au Serveur d'administration via Internet) à la stratégie de l'Agent d'administration. Ajoutez le profil dans les propriétés de la stratégie (section **Connectivité**, sous-section **Connexion**). Dans la fenêtre de création de profil, vous devez désactiver l'option **Utiliser uniquement pour récupérer les mises à jour** et sélectionner l'option **&Synchroniser les paramètres de connexion aux paramètres du Serveur d'administration indiqués dans ce profil**. Si l'accès au Serveur d'administration s'opère via une passerelle de connexion (cf. la configuration de Kaspersky Security Center de type Accès depuis Internet : Agent d'administration en tant que passerelle de connexion dans la zone démilitarisée), il faut indiquer l'adresse de la passerelle dans le champ correspondant.

Permutation entre les Serveurs d'administration en fonction du réseau actuel

Si la société compte plusieurs bureaux avec différents Serveurs d'administration et qu'une partie des appareils dotés de l'Agent d'administration se déplace entre ceux-ci, il faut que l'Agent d'administration puisse se connecter au Serveur d'administration du réseau local du bureau dans lequel l'appareil se trouve.

Dans ce cas, il faut créer un profil de connexion au Serveur d'administration pour chaque bureau dans les propriétés de la stratégie de l'Agent d'administration, à l'exception du bureau domestique où se trouve le Serveur d'administration domestique d'origine. Vous devez indiquer les adresses des Serveurs d'administration correspondants dans les profils de connexion et activer ou désactiver l'option **Utiliser uniquement pour récupérer les mises à jour** :

- Sélectionnez cette option si vous souhaitez que l'Agent d'administration soit synchronisé avec le Serveur d'administration domestique, tout en utilisant le Serveur local pour télécharger les mises à jour uniquement.
- Désactivez cette option si l'Agent d'administration doit être entièrement administré par le Serveur d'administration local.

Ensuite, il faut configurer les conditions de permutation vers les profils créés : pas moins d'une condition pour chacun des bureaux, à l'exclusion du "bureau domestique". L'idée de cette condition est de détecter dans l'environnement réseau des détails propres à un des bureaux. Si la condition se vérifie, le profil correspondant s'active. Si aucune des conditions ne se vérifie, l'Agent d'administration passe au Serveur d'administration domestique.

Création d'un profil de connexion pour les utilisateurs itinérants

Un profil de connexion au Serveur d'administration est disponible uniquement sur les appareils exécutés sous Windows et macOS.

Pour créer le profil de connexion de l'Agent d'administration au Serveur d'administration pour les utilisateurs itinérants, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le groupe d'administration pour les appareils dont il faut créer le profil de connexion de l'Agent d'administration au Serveur d'administration.
2. Exécutez une des actions suivantes :
   - Si vous voulez créer un profil de connexion pour tous les appareils du groupe, dans l'espace de travail du groupe, sous l'onglet **Stratégies**, sélectionnez une stratégie d'Agent d'administration. Ouvrez la fenêtre de la stratégie sélectionnée.
   - Si vous voulez créer le profil de connexion pour l'appareil sélectionné dans le groupe, dans l'espace de travail du groupe sous l'onglet **Appareils**, sélectionnez l'appareil et procédez comme suit :
     a. Ouvrez la fenêtre des propriétés de l'appareil sélectionné.
     b. Dans la section **Applications** de la fenêtre des propriétés de l'appareil, sélectionnez Agent d'administration.
     c. Ouvrez la fenêtre des propriétés de l'Agent d'administration.
3. Dans la fenêtre des propriétés, dans la section **Connectivité**, sélectionnez la sous-section **Profils de connexion**.

4. Dans le groupe de paramètres **Profils de connexion au Serveur d'administration**, cliquez sur le bouton **Ajouter**.

   Par défaut, la liste des profils de connexion contient les profils <Offline mode> et <Home Administration Server>. Les profils ne peuvent être modifiés ou supprimés.

   Le profil <Offline mode> ne définit aucun serveur pour la connexion. Par conséquent, l'Agent d'administration, une fois transféré vers ce profil, ne tente aucune connexion à un Serveur d'administration quelconque tant que les applications installées sur les appareils clients utilisent les stratégies pour les utilisateurs itinérants. Le profil <Offline mode> est invoqué quand les appareils sont déconnectés du réseau.

   Le profil <Home Administration Server> spécifie la connexion pour le Serveur d'administration qui a été sélectionnée lors de l'installation de l'Agent d'administration. Le profil <Home Administration Server> est invoqué quand un appareil qui fonctionnait dans un autre réseau se connecte à nouveau au Serveur d'administration domestique.

5. Dans la fenêtre **Nouveau profil** qui s'ouvre, configurez les paramètres du profil de connexion :

- **Nom du profil**

  Le champ de saisie permet de consulter ou de modifier le nom du profil de connexion.

- **Serveur d'administration**

  Adresse du Serveur d'administration auquel l'appareil client doit se connecter lors de l'activation du profil.

- **Port**

  Numéro du port utilisé pour la connexion.

- **Port SSL**

  Numéro de port utilisé pour la connexion par protocole SSL.

- **Utiliser SSL**

  Si l'option est activée, la connexion aura lieu via un port sécurisé à l'aide du protocole SSL.

  Cette option est activée par défaut. Nous vous recommandons de ne pas désactiver cette option afin que votre connexion reste sécurisée.

- Cliquez sur le lien **Configurer la connexion via le serveur proxy** pour configurer la connexion via un serveur proxy. Sélectionnez l'option **Utiliser un serveur proxy** si vous souhaitez utiliser un serveur proxy pour vous connecter à Internet. Si cette option est sélectionnée, les champs sont disponibles pour saisir les paramètres. Configurez les paramètres suivants de connexion au serveur proxy :

  - **Adresse du serveur proxy**

    Adresse du serveur proxy pour la connexion de Kaspersky Security Center à Internet.

  - **Numéro de port**

    Numéro du port via lequel la connexion proxy à Kaspersky Security Center sera établie.

  - **Authentification du serveur proxy**

    Si la case est cochée, les champs de saisie permettent d'indiquer les identifiants pour l'authentification sur le serveur proxy.

    Ce champ de saisie est accessible si la case **Utiliser un serveur proxy** est cochée.

  - **Nom d'utilisateur** (ce champ est disponible lorsque l'option **Authentification du serveur proxy** est sélectionnée)

Compte utilisateur sous lequel la connexion au serveur proxy est établie (ce champ est disponible si la case **Authentification du serveur proxy** est cochée).

- Mot de passe (ce champ est disponible lorsque l'option **Authentification du serveur proxy** est sélectionnée)

  Mot de passe défini par l'utilisateur sous le compte duquel la connexion au serveur proxy est établie (ce champ est disponible si la case **Authentification du serveur proxy** est cochée).

  Pour voir le mot de passe saisi, cliquez sur le bouton **Afficher** et maintenez-le enfoncé aussi longtemps que vous en avez besoin.

- Paramètres de la passerelle des connexions

  Adresse de la passerelle via laquelle la connexion entre les appareils clients et le Serveur d'administration s'opère.

- Activer le mode de l'utilisateur autonome

  Si l'option est activée, en cas de connexion via ce profil, les applications installées sur l'appareil client vont utiliser les profils de stratégie pour les appareils qui se trouvent en mode de l'utilisateur autonome et les stratégies pour utilisateurs autonomes. Si aucune stratégie pour les utilisateurs autonomes n'est définie pour l'application, c'est la stratégie active qui sera utilisée.

  Si l'option est activée, les applications utiliseront les stratégies actives.

  Cette option est Inactif par défaut.

- Utiliser uniquement pour récupérer les mises à jour

  Si l'option est désactivée, le profil sera utilisé uniquement lors du téléchargement des mises à jour par les applications installées sur l'appareil client. Pour les autres opérations, la connexion au Serveur d'administration sera réalisée selon les paramètres de connexion d'origine définis lors de l'installation de l'Agent d'administration.

  Cette option est activée par défaut.

- &Synchroniser les paramètres de connexion aux paramètres du Serveur d'administration indiqués dans ce profil

  Si l'option est activée, l'Agent d'administration se connecte au Serveur d'administration en utilisant les paramètres utilisés dans les propriétés du profil.

  Si l'option est désactivée, l'Agent d'administration se connecte au Serveur d'administration en utilisant les paramètres d'origine définis lors de l'installation.

  Cette option n'est accessible que si l'option **Utiliser uniquement pour récupérer les mises à jour** est désactivée.

  Cette option est Inactif par défaut.

6. Sélectionnez l'option **Activer le mode de l'utilisateur autonome quand le Serveur d'administration n'est pas disponible** afin que lors de la connexion, les applications installées sur un appareil client utilisent les profils de stratégie pour les appareils en mode de l'utilisateur autonome et les stratégies pour les utilisateurs itinérants si

le Serveur d'administration est inaccessible. Si aucune stratégie pour les utilisateurs autonomes n'est définie pour l'application, c'est la stratégie active qui sera utilisée.

Finalement, le profil de connexion de l'Agent d'administration au Serveur d'administration pour les utilisateurs itinérants sera créé. Lors de la connexion de l'Agent d'administration au Serveur d'administration via ce profil de l'application, les applications installées sur l'appareil client utiliseront les stratégies pour les appareils en mode de l'utilisateur autonome et les stratégies pour les utilisateurs autonomes.

À propos du transfert de l'Agent d'administration à d'autres Serveurs d'administration

Paramètres de connexion d'origine de l'Agent d'administration au Serveur d'administration lors de l'installation de l'Agent d'administration. Pour basculer l'Agent d'administration sur d'autres Serveurs d'administration, vous pouvez utiliser les règles de basculement. Cette fonctionnalité est prise en charge uniquement pour les Agents d'administration installés sur des appareils fonctionnant sous Windows ou macOS.

Les règles de commutation peuvent se déclencher en cas de modification des paramètres réseau suivants :

- Adresse de la passerelle par défaut.
- Adresse IP du serveur DHCP (Dynamic Host Configuration Protocol).
- Suffixe DNS du sous-réseau.
- Adresse IP du serveur DNS du réseau.
- Accessibilité du domaine Windows. Ce paramètre est disponible uniquement pour les appareils exécutant Windows.
- Adresse et masque de sous-réseau.
- Adresse IP du serveur WINS du réseau. Ce paramètre est disponible uniquement pour les appareils exécutant Windows.
- Nom DNS ou NetBIOS de l'appareil client.
- Accessibilité de l'adresse de connexion SSL.

Si des règles de permutation de l'Agent d'administration sur d'autres Serveurs d'administration sont rédigées, l'Agent d'administration réagit aux modifications des paramètres du réseau de la manière suivante :

- Si les caractéristiques du réseau correspondent à une des règles formées, l'Agent d'administration se connecte au Serveur d'administration indiqué dans cette règle. Si la règle le prévoit, les applications installées sur les appareils clients adopteront les stratégies pour les utilisateurs autonomes.
- Si une des règles n'est pas exécutée, l'Agent d'administration revient aux paramètres d'origine de connexion au Serveur d'administration définis lors de l'installation. Les applications installées sur les appareils clients reviennent aux stratégies actives.
- Si le Serveur d'administration est inaccessible, l'Agent d'administration utilise les stratégies pour les utilisateurs autonomes.

L'Agent d'administration bascule vers la stratégie pour les utilisateurs autonomes uniquement si l'option **Activer le mode de l'utilisateur autonome quand le Serveur d'administration n'est pas disponible** est activée dans les paramètres de la stratégie de l'Agent d'administration.

Les paramètres de connexion de l'Agent d'administration au Serveur d'administration sont préservés dans le profil de connexion. Le profil de connexion permet de créer des règles de permutation des appareils clients vers les stratégies pour les utilisateurs autonomes, ainsi que de configurer le profil de sorte qu'il soit uniquement utilisé pour le téléchargement des mises à jour.

Création d'une règle de permutation de l'Agent d'administration selon l'emplacement réseau

La permutation de l'Agent d'administration selon emplacement réseau est disponible uniquement sur les appareils tournant sous Windows ou macOS.

Afin de créer la règle de permutation de l'Agent d'administration d'un Serveur d'administration sur un autre, lors de la modification des caractéristiques du réseau, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le groupe d'administration dont les appareils requièrent la création de la règle de permutation de l'Agent d'administration selon la description de l'emplacement réseau.
2. Exécutez une des actions suivantes :
   - Si vous voulez créer une règle pour tous les appareils du groupe, dans l'espace de travail du groupe sous l'onglet **Stratégies**, sélectionnez une stratégie d'Agent d'administration. Ouvrez la fenêtre de la stratégie sélectionnée.
   - Si vous voulez créer une règle pour l'appareil sélectionné dans un groupe, dans l'espace de travail du groupe, sous l'onglet **Appareils**, sélectionnez l'appareil et procédez comme suit :
     a. Ouvrez la fenêtre des propriétés de l'appareil sélectionné.
     b. Dans la section **Applications** de la fenêtre des propriétés de l'appareil, sélectionnez Agent d'administration.
     c. Ouvrez la fenêtre des propriétés de l'Agent d'administration.

3. Dans la fenêtre **Propriétés** qui s'ouvre, dans la section **Connectivité**, sélectionnez la sous-section **Profils de connexion**.

4. Dans le groupe **Paramètres d'emplacement réseau**, cliquez sur le bouton **Ajouter**.

5. Dans la fenêtre **Nouvelle description** qui s'ouvre, configurez la description de l'emplacement réseau et la règle de permutation. Configurez les paramètres suivants de la description de l'emplacement de réseau :

   - Nom de la description de l'emplacement réseau

     Le nom de la descriptions de l'emplacement réseau ne peut pas contenir plus de 255 caractères, ni contenir les caractères spéciaux ("*<>?\/:|).

   - Utiliser le profil de connexion

     La liste déroulante permet de sélectionner le profil de connexion de l'Agent d'administration au Serveur d'administration. Le profil est utilisé quand les conditions de la description de l'emplacement réseau sont remplies. Le profil de connexion contient les paramètres de connexion de l'Agent d'administration au Serveur d'administration et définit le transfert des appareils clients aux stratégies pour les utilisateurs itinérants. Le profil est utilisé uniquement pour télécharger les mises à jour.

6. Dans la section **Conditions de permutation**, cliquez sur le bouton **Ajouter** afin de créer une liste des conditions de description de l'emplacement réseau.

   Les conditions dans une règle sont réunies via l'opérateur logique "ET". Pour que la règle de permutation selon la description de l'emplacement de réseau fonctionne, toutes les conditions de permutation de la règle doivent être remplies.

7. Sélectionnez dans la liste déroulante la valeur correspondant à la modification d'une caractéristique du réseau auquel l'appareil client est connecté :

   - **Adresse de la passerelle de connexion par défaut** : L'adresse de la passerelle principale du réseau a changé.
   - **Adresse du serveur DHCP** : modification de l'adresse IP du serveur DHCP (Dynamic Host Configuration Protocol) dans le réseau.
   - **Domaine DNS** : Le suffixe DNS du sous-réseau a été modifié.
   - **Adresse du serveur DNS** : l'adresse IP du serveur DNS dans le réseau a été modifiée.
   - **Accessibilité du domaine Windows (Windows uniquement)** : Change l'état du domaine Windows auquel l'appareil client est connecté. Utilisez ce paramètre uniquement pour les appareils exécutant Windows.
   - **Sous-réseau** : modifie l'adresse et le masque du sous-réseau.
   - **Adresse du serveur WINS (Windows uniquement)** : modification de l'adresse IP du serveur WINS dans le réseau. Utilisez ce paramètre uniquement pour les appareils exécutant Windows.
   - **Résolvabilité des noms** : le nom DNS ou NetBIOS de l'appareil client a changé.
   - **Accessibilité de l'adresse de la connexion SSL** : l'appareil client peut ou ne peut pas (selon l'option sélectionnée) établir une connexion SSL avec un serveur défini (nom:port). Pour chaque serveur, vous pouvez également définir un certificat SSL. Dans ce cas, l'Agent d'administration vérifie le certificat du serveur en plus de vérifier la capacité d'une connexion SSL. Si le certificat ne correspond pas, la connexion échoue. La fréquence de connexion est de une fois par minute.

8. Définissez dans la fenêtre qui s'ouvre la valeur de la condition de permutation de l'Agent d'administration sur un autre Serveur d'administration. Le nom de la fenêtre dépend de la valeur sélectionnée à l'étape précédente. Configurez les paramètres suivants de la condition de permutation :

   - Valeur

     Le champ permet d'ajouter une ou plusieurs valeurs pour la condition créée.

   - Correspond à au moins une valeur de la liste

     Si cette option a été sélectionnée, la condition sera exécutée avec n'importe quelle valeur indiquée dans la liste **Valeur**.

     Cette option est sélectionnée par défaut.

   - Ne correspond à aucune des valeurs de la liste

     Si cette option a été sélectionnée, la condition sera exécutée si sa valeur est absente dans la liste **Valeur**.

9. Dans la fenêtre **Nouvelle description**, sélectionnez l'option **La description est active** pour activer l'utilisation de la nouvelle description de l'emplacement réseau.

Ceci débouche sur la création d'une règle de permutation selon la description de l'emplacement réseau que l'Agent d'administration va utiliser, quand les conditions sont remplies, pour établir la connexion au Serveur d'administration renseigné dans la description du profil de connexion.

La vérification de la correspondance entre la description de l'emplacement réseau et les caractéristiques du réseau s'opère dans l'ordre de présentation dans la liste. Si les caractéristiques du réseau correspondent à plusieurs descriptions, c'est la première d'entre elles qui sera appliquée. Vous pouvez modifier l'ordre de suivi des règles dans la liste à l'aide des boutons **Haut** (↓) et **Bas** (↑).

Notifications sur les événements

Cette section explique comment choisir le mode de notification de l'administrateur au sujet des événements survenus sur les appareils clients. Elle aborde également la configuration des paramètres des notifications sur les événements.

Elle décrit aussi comment vérifier la diffusion des notifications relatives aux événements à l'aide du " virus " d'essai Eicar.

Configuration des paramètres de notification sur les événements

Kaspersky Security Center permet de sélectionner le mode de notification de l'administrateur sur les événements survenus sur les appareils client et de configurer les paramètres de ces notifications :

- Email. Quand un événement se produit, l'application envoie une notification à l'adresse email indiquée. Vous pouvez configurer le texte de la notification.
- SMS. Quand un événement se produit, l'application envoie la notification aux numéros de téléphone indiqués. Vous pouvez configurer l'envoi des notifications SMS via la passerelle de messagerie.
- Fichier exécutable. Quand un événement se produit sur l'appareil, le fichier exécutable est lancé sur le poste de travail de l'administrateur. Le fichier exécutable permet à l'administrateur d'obtenir les paramètres de l'événement survenu.

Pour configurer les notifications sur les événements survenus sur les appareils clients, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez l'entrée portant le nom du Serveur d'administration requis.
2. Dans l'espace de travail de l'entrée, sélectionnez l'onglet **Événements**.
3. Cliquez sur le lien **Configurer les paramètres des notifications et d'exportation des événements**, puis dans la liste déroulante, sélectionnez la valeur **Configurer les notifications**.

   Cela permet d'ouvrir la fenêtre **Propriétés : Événements**.

4. Dans la section **Notification**, sélectionnez le mode de notification (email, SMS, fichier exécutable à lancer) et configurez les paramètres des notifications.

   - **Email**

L'onglet **Email** vous permet de configurer les notifications d'événement par email.

Dans le champ **Destinataires (adresses email)**, indiquez les adresses e-mail auxquelles l'application enverra des notifications. Vous pouvez spécifier plusieurs adresses dans ce champ, en les séparant par un point-virgule.

Dans le champ **Serveurs SMTP**, spécifiez les adresses du serveur de messagerie, en les séparant par un point-virgule. Vous pouvez utiliser les valeurs suivantes du paramètre :

- Adresse IPv4 ou IPv6
- Nom de réseau Windows (nom NetBIOS) de l'appareil
- Nom complet du serveur SMTP

Dans le champ **Port du serveur SMTP**, spécifiez le numéro d'un port de communication du serveur SMTP. Le numéro de port par défaut est 25.

Si vous activez l'option **Utiliser la recherche MX de DNS**, vous pouvez utiliser plusieurs enregistrements MX des adresses IP pour le même nom DNS du serveur SMTP. Le même nom DNS peut avoir plusieurs enregistrements MX avec des priorités différentes pour la réception des emails. Le Serveur d'administration tente d'envoyer des notifications par email au serveur SMTP par ordre croissant de priorité des enregistrements MX. Cette option est Inactif par défaut.

Si vous activez l'option **Utiliser la recherche MX de DNS** et n'activez pas l'utilisation des paramètres TLS, nous vous recommandons d'utiliser les paramètres DNSSEC sur votre appareil serveur comme mesure supplémentaire de protection pour l'envoi des notifications par email.

Cliquez sur le lien **Paramètres** pour définir des paramètres de notification supplémentaires :

- Nom de l'objet (nom de l'objet d'un message électronique)
- Adresse email de l'expéditeur
- Paramètres d'authentification ESMTP

Vous devez indiquer un compte pour l'authentification sur un serveur SMTP si l'option d'authentification ESMTP est activée pour un serveur SMTP.

- Paramètres TLS pour le serveur SMTP :
  - **Ne pas utiliser TLS**

    Vous pouvez choisir cette option si vous désactivez le chiffrement des emails.
  - **Utiliser TLS si pris en charge par le serveur SMTP**

    Vous pouvez choisir cette option si vous voulez utiliser une connexion TLS pour un serveur SMTP. Si le serveur SMTP n'est pas compatible avec TLS, le Serveur d'administration connecte le serveur SMTP sans utiliser TLS.
  - **Toujours utiliser TLS, vérifier la validité du certificat de serveur**

    Vous pouvez choisir cette option si vous voulez utiliser les paramètres d'authentification TLS. Si le serveur SMTP n'est pas compatible avec TLS, le Serveur d'administration ne peut pas connecter le serveur SMTP.

Nous vous recommandons d'utiliser cette option pour améliorer la protection de la connexion avec un serveur SMTP. Si vous choisissez cette option, vous pouvez définir les paramètres d'authentification pour une connexion TLS.

Si vous choisissez la valeur **Toujours utiliser TLS, vérifier la validité du certificat de serveur**, vous pouvez spécifier un certificat pour l'authentification du serveur SMTP et choisir si vous souhaitez activer la communication via n'importe quelle version de TLS ou uniquement via TLS 1.2 ou les versions ultérieures. Vous pouvez également spécifier un certificat pour l'authentification du client sur le serveur SMTP.

Vous pouvez spécifier les paramètres TLS pour le serveur SMTP :

- Recherchez un fichier de certificat de serveur SMTP :

Vous pouvez recevoir un fichier avec la liste des certificats de l'autorité de certification de confiance et charger le fichier sur le Serveur d'administration. Kaspersky Security Center vérifie si le certificat d'un serveur SMTP est également signé par une autorité de certification de confiance ou non. Kaspersky Security Center ne peut pas se connecter à un serveur SMTP si le certificat du serveur SMTP ne provient pas d'une autorité de certification de confiance.

- Recherchez un fichier de certificat client :

Vous pouvez utiliser un certificat que vous avez reçu de n'importe quelle source, par exemple, de n'importe quelle autorité de certification de confiance. Vous devez spécifier le certificat et sa clé privée en utilisant l'un des types de certificats suivants :

- Certificat X-509 :

Vous devez spécifier un fichier avec le certificat et un fichier avec la clé privée. Les deux fichiers ne dépendent pas l'un de l'autre, et l'ordre de chargement des fichiers est sans importance. Lorsque les deux fichiers sont chargés, vous devez spécifier le mot de passe pour décoder la clé privée. Le mot de passe peut présenter une valeur vide si la clé privée n'est pas encodée.

- Conteneur pkcs12 :

Vous devez charger un seul fichier contenant le certificat et sa clé privée. Lorsque le fichier est chargé, vous devez ensuite indiquer le mot de passe pour décoder la clé privée. Le mot de passe peut présenter une valeur vide si la clé privée n'est pas encodée.

Le champ **Message de notification** contient du texte standard avec des informations sur l'événement que l'application envoie lors d'un événement. Ce texte inclut des paramètres de remplacement, comme le nom de l'événement, le nom de l'appareil et le nom de domaine. Vous pouvez modifier le texte du message en ajoutant d'autres paramètres de remplacement avec des détails plus pertinents de l'événement. La liste des paramètres de remplacement est disponible en cliquant sur le bouton à droite du champ.

Si le texte de notification contient un caractère en pourcentage (%), vous devez l'indiquer deux fois de suite pour autoriser l'envoi du message. Par exemple, « La charge du processeur est de 100 %% ».

Cliquez sur le lien **Configurer la limite du nombre de notifications** pour indiquer le nombre maximum de notifications que l'application peut envoyer pendant l'intervalle de temps spécifié.

Cliquez sur le bouton **&Envoyer un message d'essai** pour vérifier si vous avez correctement configuré les notifications. L'application envoie une notification de test aux adresses email que vous avez indiquées.

- SMS

L'onglet **SMS** vous permet de configurer la transmission de notifications par SMS des divers événements à un téléphone portable. Les messages SMS sont envoyés via une passerelle de messagerie.

Dans le champ **Destinataires (adresses email)**, indiquez les adresses email auxquelles l'application enverra des notifications. Vous pouvez spécifier plusieurs adresses dans ce champ, en les séparant par un point-virgule. Les notifications seront envoyées aux numéros de téléphone associés aux adresses email spécifiées.

Dans le champ **Serveurs SMTP**, spécifiez les adresses du serveur de messagerie, en les séparant par un point-virgule. Vous pouvez utiliser les valeurs suivantes du paramètre :

- Adresse IPv4 ou IPv6
- Nom de réseau Windows (nom NetBIOS) de l'appareil
- Nom complet du serveur SMTP

Dans le champ **Port du serveur SMTP**, spécifiez le numéro d'un port de communication du serveur SMTP. Le numéro de port par défaut est 25.

Cliquez sur le lien **Paramètres** pour définir des paramètres de notification supplémentaires :

- Nom de l'objet (nom de l'objet d'un message électronique)
- Adresse email de l'expéditeur
- Paramètres d'authentification ESMTP

Au besoin, vous pouvez spécifier un compte pour l'authentification sur un serveur SMTP si l'option d'authentification ESMTP est activée pour un serveur SMTP.

- Paramètres TLS pour le serveur SMTP

Vous pouvez désactiver l'utilisation de TLS, utiliser TLS si le serveur SMTP prend en charge ce protocole ou vous pouvez forcer l'utilisation de TLS uniquement. Si vous choisissez d'utiliser uniquement TLS, vous pouvez spécifier un certificat pour l'authentification du serveur SMTP et choisir si vous souhaitez activer la communication via n'importe quelle version de TLS ou uniquement via TLS 1.2 ou les versions ultérieures. De plus, si vous choisissez d'utiliser uniquement TLS, vous pouvez spécifier un certificat pour l'authentification du client sur le serveur SMTP.

- Rechercher un fichier de certificat de serveur SMTP

Vous pouvez recevoir un fichier avec la liste des certificats des autorités de certification de confiance et charger le fichier dans Kaspersky Security Center. Kaspersky Security Center vérifie si le certificat du serveur SMTP est également signé par une autorité de certification de confiance ou non. Kaspersky Security Center ne peut pas se connecter au serveur SMTP si le certificat du serveur SMTP ne provient pas d'une autorité de certification de confiance.

Vous devez charger un seul fichier contenant le certificat et sa clé privée. Lorsque le fichier est chargé, vous devez ensuite indiquer le mot de passe pour décoder la clé privée. Le mot de passe peut être vide si la clé privée n'est pas encodée. Le champ **Message de notification** contient un texte standard avec des informations sur l'événement que l'application envoie lorsqu'un événement se produit. Ce texte inclut des paramètres de remplacement, comme le nom de l'événement, le nom de l'appareil et le nom de domaine. Vous pouvez modifier le texte du message en ajoutant d'autres paramètres de remplacement avec des détails plus pertinents de l'événement. La liste des paramètres de remplacement est disponible en cliquant sur le bouton à droite du champ.

Si le texte de notification contient un caractère en pourcentage (%), vous devez l'indiquer deux fois de suite pour autoriser l'envoi du message. Par exemple, « La charge du processeur est de 100 %% ».

Cliquez sur le lien **Configurer la limite de notification numérique** pour indiquer le nombre maximum de notifications que l'application peut envoyer au cours de l'intervalle de temps spécifié.

Cliquez sur le bouton **Envoyer un message d'essai** pour vérifier si vous avez bien configuré les notifications. L'application envoie une notification de test au destinataire que vous avez indiqué.

- **Fichier exécutable à exécuter**

  Si cette méthode de notification est sélectionnée, dans le champ de saisie, vous pouvez indiquer quelle application démarre selon l'événement qui se produit.

  Cliquez sur le lien **Configurer la limite du nombre de notifications** pour indiquer le nombre maximum de notifications que l'application peut envoyer sur l'intervalle de temps spécifié.

  Cliquez sur le bouton **Envoyer un message d'essai** pour vérifier si vous avez bien configuré les notifications : l'application envoie une notification d'essai aux adresses électroniques que vous avez indiquées.

5. Dans le champ **Message de notification**, saisissez le texte que l'application enverra lorsqu'un événement se produira.

   Dans la liste déroulante située à droite du champ de texte, choisissez les paramètres prédéfinis avec les détails de l'événement à ajouter au texte (par exemple, la description de l'événement, l'heure à laquelle il s'est produit, etc.).

   Si le texte de la notification contient le caractère %, il faut le saisir deux fois pour que le message puisse être envoyé. Par exemple, « La charge du processeur est de 100 %% ».

6. Cliquez sur le bouton **&Envoyer un message d'essai** pour vérifier si la notification a été correctement configurée.

   L'application envoie la notification au destinataire indiqué.

7. Cliquez sur le bouton **OK** afin d'enregistrer les modifications.

Les paramètres configurés de notification sont diffusés sur tous les événements survenus sur les appareils clients.

Vous pouvez remplacer les paramètres de notification de certains événements dans la section **Configuration de l'événement** des Paramètres du Serveur d'administration, des paramètres d'une stratégie, ou des paramètres d'une application.

Vérification de déploiement des notifications

Pour vérifier la diffusion des notifications relatives aux événements, vous pouvez compter sur la notification de la détection du « virus » d'essai Eicar sur les appareils client.

Pour vérifier la diffusion des notifications sur les événements, procédez comme suit :

1. Arrêtez la tâche de protection en temps réel du système de fichiers sur l'appareil client et copiez le « virus » d'essai Eicar sur celui-ci. Activez à nouveau la tâche de protection en temps réel du système de fichiers.

2. Lancez la tâche d'analyse des appareils client pour le groupe d'administration ou pour l'ensemble d'appareils contenant l'appareil client « infecté » par le virus Eicar.

   Si la tâche d'analyse est configurée correctement, le « virus » d'essai est détecté lors de l'exécution de l'analyse. Si les paramètres de notifications sont configurés correctement, vous recevrez la notification relative à la détection du virus.

   Dans l'espace de travail de l'entrée **Serveur d'administration**, sous l'onglet **Événements**, la sélection de **Derniers événements** permet d'afficher un enregistrement relatif à la détection du « virus ».

Le « virus » d'essai EICAR ne contient aucun code qui peut nuire à votre appareil. Ceci étant dit, la majorité des logiciels de protection des éditeurs le détecte comme un virus. Vous pouvez télécharger le « virus » d'essai depuis le site Internet officiel de l'organisation EICAR.

Notification relative aux événements via un fichier exécutable

Kaspersky Security Center permet de lancer un fichier exécutable afin de signaler à l'administrateur les événements survenus sur les appareils clients. Le fichier exécutable doit contenir un autre fichier exécutable avec les paramètres variables à envoyer à l'administrateur (voir le tableau ci-dessous).

Paramètres variables de description de l'événement

Variable	Description du paramètre secondaire
%SEVERITY%	Importance de l'événement. Valeurs possibles : • **Information** • **Avertissement** • **Erreur** • **Critique**
%COMPUTER%	Nom de l'appareil où l'événement s'est produit. La longueur maximale du nom de l'appareil est de 256 caractères.
%DOMAIN%	Nom de domaine de l'appareil où l'événement s'est produit.
%EVENT%	Nom du type d'événement. La longueur maximale du nom du type d'événement est de 50 caractères.
%DESCR%	Description de l'événement. La longueur maximale de la description est de 1 000 caractères.
%RISE_TIME%	Heure de création de l'événement.
%KLCSAK_EVENT_TASK_DISPLAY_NAME%	Nom de la tâche. La longueur maximale du nom de la tâche est de 100 caractères.
%KL_PRODUCT%	Nom de l'application.
%KL_VERSION%	Numéro de version de l'application.
%KLCSAK_EVENT_SEVERITY_NUM%	Numéro d'importance de l'événement. Valeurs possibles : • 1—**Information** • 2—**Avertissement** • 3—**Erreur** • 4—**Critique**

Variable	Description du paramètre secondaire
%HOST_IP%	Adresse IP de l'appareil où l'événement s'est produit.
%HOST_CONN_IP%	Adresse IP de connexion de l'appareil où l'événement s'est produit.

Exemple :
La notification de l'événement s'opère via un fichier exécutable (par exemple, script1.bat) au sein duquel un autre fichier exécutable (par exemple, script2.bat) contenant la variable %COMPUTER% est lancé. Quand l'événement se produit, le fichier script1.bat est lancé sur l'appareil de l'administrateur. Ce fichier lance à son tour le fichier script2.bat avec la variable %COMPUTER%. L'administrateur reçoit le nom de l'appareil sur lequel l'événement s'est produit.

Chiffrer la communication selon TLS

Afin d'éliminer les vulnérabilités sur votre réseau d'entreprise, vous pouvez activer le chiffrement du trafic, en utilisant le protocole TLS. Vous pouvez activer les protocoles de chiffrement TLS et les suites de chiffrement prises en charge sur le Serveur d'administration et le serveur MDM iOS. Kaspersky Security Center prend en charge les versions 1.0, 1.1, 1.2 et 1.3 du protocole TLS. Vous pouvez sélectionner le protocole de chiffrement et les suites de chiffrement requis.

Kaspersky Security Center utilise des certificats auto-signés. Il n'est pas nécessaire de réaliser une configuration complémentaire des appareils iOS. Vous pouvez également utiliser vos propres certificats. Les experts de Kaspersky recommande d'utiliser des certificats émis par des autorités de certification de confiance.

Serveur d'administration

Pour configurer les protocoles de chiffrement et les suites cryptographiques sur le Serveur d'administration :

1. Exécutez l'invite de commande Windows en utilisant les droits d'administrateur, puis remplacez votre répertoire actuel par celui contenant l'utilitaire klscflag. L'utilitaire klsclag se trouve dans le dossier dans lequel le Serveur d'administration est installé. Chemin d'installation par défaut est <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

2. Utilisez l'indicateur SrvUseStrictSslSettings pour configurer les protocoles de chiffrement et les suites de chiffrement autorisés sur le Serveur d'administration. Saisissez la commande suivante :

   ```
   klscflag -fset -pv ".core/.independent" -s Transport -n SrvUseStrictSslSettings -v <valeur> -t d
   ```

   Spécifiez le paramètre <value> de l'indicateur SrvUseStrictSslSettings :

   - `4` : Seuls les protocoles TLS 1.2 et TLS 1.3 sont activés. Les suites de chiffrement avec LS_RSA_WITH_AES_256_GCM_SHA384 sont également activées (ces suites de chiffrement sont nécessaires pour une compatibilité descendante avec les versions précédentes de Kaspersky Security Center). Il s'agit de la valeur par défaut.

     Suites de chiffrement prises en charge pour le protocole TLS 1.2 :

     - ECDHE-RSA-AES256-GCM-SHA384
     - ECDHE-RSA-AES256-SHA384
     - ECDHE-RSA-CHACHA20-POLY1305
     - AES256-GCM-SHA384 (suite de chiffrement avec TLS_RSA_WITH_AES_256_GCM_SHA384)
     - ECDHE-RSA-AES128-GCM-SHA256
     - ECDHE-RSA-AES128-SHA256

     Suites de chiffrement prises en charge pour le protocole TLS 1.3 :

     - TLS_AES_256_GCM_SHA384
     - TLS_CHACHA20_POLY1305_SHA256
     - TLS_AES_128_GCM_SHA256
     - TLS_AES_128_CCM_SHA256

   - `5` : Seuls les protocoles TLS 1.2 et TLS 1.3 sont activés. Pour les protocoles TLS 1.2 et TLS 1.3, les suites de chiffrement spécifiques répertoriées ci-dessous sont prises en charge.

     Suites de chiffrement prises en charge pour le protocole TLS 1.2 :

     - ECDHE-RSA-AES256-GCM-SHA384
     - ECDHE-RSA-AES256-SHA384
     - ECDHE-RSA-CHACHA20-POLY1305
     - ECDHE-RSA-AES128-GCM-SHA256

- ECDHE-RSA-AES128-SHA256

Suites de chiffrement prises en charge pour le protocole TLS 1.3 :

- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_GCM_SHA256
- TLS_AES_128_CCM_SHA256

Il est déconseillé d'utiliser 0, 1, 2 ou 3 comme valeur de paramètre de l'indicateur SrvUseStrictSslSettings. Les valeurs de ces paramètres correspondent aux versions non sécurisées du protocole TLS (les protocoles TLS 1.0 et TLS 1.1) et aux suites de chiffrement non sécurisées et sont utilisées uniquement à des fins de compatibilité avec les versions antérieures de Kaspersky Security Center.

3. Redémarrez les services Kaspersky Security Center 15.1 suivants :

- Serveur d'administration
- Serveur Web
- Proxy d'activation

Le chiffrement du trafic à l'aide du protocole TLS est activé.

Vous pouvez utiliser les indicateurs KLTR_TLS12_ENABLED et KLTR_TLS13_ENABLED pour activer la prise en charge des protocoles TLS 1.2 et TLS 1.3, respectivement. Ces indicateurs sont activés par défaut.

Pour activer ou désactiver la prise en charge des protocoles TLS 1.2 et TLS 1.3 :

1. Exécutez l'utilitaire klscflag.

   Exécutez l'invite de commande Windows en utilisant les droits d'administrateur, puis remplacez votre répertoire actuel par celui contenant l'utilitaire klscflag. L'utilitaire klsclag se trouve dans le dossier dans lequel le Serveur d'administration est installé. Chemin d'installation par défaut est <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

2. Saisissez l'une des commandes suivantes à l'invite de commande Windows, en utilisant les droits d'administrateur :

   - Utilisez cette commande pour activer ou désactiver la prise en charge du protocole TLS 1.2 :

     ```
     klscflag -fset -pv ".core/.independent" -s Transport -n KLTR_TLS12_ENABLED -v <valeur> -t d
     ```

   - Utilisez cette commande pour activer ou désactiver la prise en charge du protocole TLS 1.3 :

     ```
     klscflag -fset -pv ".core/.independent" -s Transport -n KLTR_TLS13_ENABLED -v <valeur> -t d
     ```

   Spécifiez le paramètre `<valeur>` de l'indicateur :

   - `1` : Pour activer la prise en charge du protocole TLS.
   - `0` : Pour désactiver la prise en charge du protocole TLS.

Serveur MDM iOS

La connexion entre les appareils iOS et le Serveur MDM iOS est chiffrée par défaut.

Pour configurer les protocoles de chiffrement et les suites cryptographiques sur le Serveur MDM iOS :

1. Ouvrez le registre système de l'appareil client sur lequel le Serveur MDM iOS est installé, par exemple, à l'aide de la commande regedit dans le menu **Démarrer** → **Exécuter**.
2. Rendez-vous dans la section :
   - Pour les systèmes 32 bits :
     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\Connectors\KLIOSMDM\1.0.0.0\Cor
   - Pour les systèmes 64 bits :
     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\Connectors\KLIOSI
3. Créez une clé appelée `StrictSslSettings`.
4. Définissez le type de clé `DWORD`.
5. Attribuez une valeur à la clé :
   - `2` : les protocoles TLS 1.0, TLS 1.1 et TLS 1.2 sont activés.
   - `3` : seul le protocole TLS 1.2 est activé (valeur par défaut).
6. Redémarrez le service Serveur MDM iOS Kaspersky Security Center.

Configuration de l'interface

Vous pouvez configurer l'interface de Kaspersky Security Center :

- Affichez et masquez des objets dans l'arborescence de la console, l'espace de travail et les fenêtres de propriétés des objets (dossiers, sections), en fonction des fonctionnalités utilisées.
- Affichez et masquez les éléments de la fenêtre principale (par exemple, l'arborescence de la console ou les menus standard tels que **Actions** et **Affichage**).

Pour configurer l'interface de Kaspersky Security Center conformément à l'ensemble de fonctionnalités actuellement utilisé, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez l'entrée **Serveur d'administration**.
2. Dans la barre de menus de la fenêtre principale de l'application, sélectionnez **Affichage** → **Configurer l'interface**.

3. Dans la fenêtre **Configurer l'interface** qui s'ouvre, configurez l'affichage des éléments d'interface à l'aide des cases à cocher suivantes :

- Afficher la gestion des vulnérabilités et des correctifs

  Si cette option est activée, le dossier d'**installation à distance** affiche le sous-dossier de **Déploiement des images des appareils** et le dossier **Stockages** affiche le sous-dossier **Matériel**.

  Cette option est désactivée par défaut si l'Assistant de configuration initiale de l'application n'a pas terminé ses opérations. Cette option est activée par défaut après la fin des opérations de l'Assistant de configuration initiale de l'application.

  Si cette option est désactivée, les éléments de menu **Créer une session RDP** et **Partage du bureau Windows** ne seront pas disponibles, même si vous avez une licence d'administration système.

- Afficher le chiffrement et la protection des données

  Si cette option est activée, l'arborescence de la console affiche le dossier **Chiffrement et protection des données**.

  Cette option est activée par défaut.

- Afficher les paramètres Endpoint Control

  Si cette option est activée, les sous-sections suivantes sont affichées dans la section **Contrôles de sécurité** de la fenêtre des propriétés de la stratégie de Kaspersky Endpoint Security for Windows :

  - **Contrôle des applications**
  - **Contrôle des appareils**
  - **Contrôle Internet**
  - **Contrôle évolutif des anomalies**

  Si cette option est désactivée, ces sous-sections ne sont pas affichées dans la section **Contrôles de sécurité**.

  Cette option est activée par défaut.

- Afficher l'Administration des appareils mobiles

  Si cette option est activée, la fonctionnalité **Administration des appareils mobiles** est disponible. Une fois que vous avez redémarré l'application, l'arborescence de la console affiche le dossier **Appareils mobiles**.

  Cette option est activée par défaut.

- Afficher les Serveurs d'administration secondaires

Si la case est cochée, l'arborescence de la console affiche les nœuds des Serveurs d'administration secondaires et virtuels au sein des groupes d'administration. Les fonctionnalités connectées aux Serveurs d'administration secondaires et virtuels, par exemple, la création de tâches pour l'installation à distance d'applications sur les Serveurs d'administration secondaires, sont disponibles à ce niveau.

Celle-ci est décochée par défaut.

- Afficher les sections des paramètres de sécurité

  Si cette option est activée, la section **Sécurité** s'affiche dans la fenêtre des propriétés du Serveur d'administration, des groupes d'administration et d'autres objets. Cette option vous permet d'accorder aux utilisateurs et aux groupes d'utilisateurs des autorisations personnalisées pour utiliser des objets.

  Cette option est Inactif par défaut.

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

Pour appliquer certaines des modifications, vous devez fermer la fenêtre principale de l'application, puis l'ouvrir de nouveau.

Pour configurer l'affichage des éléments dans la fenêtre principale de l'application, procédez comme suit :

1. Dans la barre de menus de la fenêtre principale de l'application, sélectionnez **Affichage** → **Configurer**.
2. Dans la fenêtre **Configurer l'affichage** qui s'ouvre, configurez l'affichage des éléments de la fenêtre principale à l'aide des cases à cocher.
3. Cliquez sur le bouton **OK**.

Recherche d'appareils en réseau

Cette section décrit les étapes à suivre absolument après l'installation de Kaspersky Security Center.

Scénario de recherche d'appareils en réseau

Vous devez effectuer la recherche d'appareils avant l'installation des applications de sécurité. Le Serveur d'administration reçoit les informations sur les appareils détectés et vous permet d'administrer les appareils à l'aide de stratégies. Des sondages réguliers du réseau sont nécessaires pour mettre à jour la liste des appareils disponibles dans le réseau.

Avant de lancer le sondage du réseau, assurez-vous que le protocole SMB est activé. Sinon, Kaspersky Security Center ne peut pas détecter les appareils dans le réseau interrogé. Pour activer le protocole SMB, suivez les instructions correspondant à votre système d'exploitation.

La recherche d'appareils en réseau se déroule selon les étapes suivantes :

1. **Découvrir les appareils**

   L'Assistant de configuration initiale de l'application vous guide tout au long de la recherche initiale d'appareils et vous aide à rechercher des appareils connectés en réseau comme des ordinateurs, des tablettes et des téléphones mobiles. Vous pouvez aussi commencer la recherche d'appareils manuellement.

2. **Configurer les sondages programmés**

   Décidez quel(s) type(s) de sondage vous voulez utiliser régulièrement. Activez les types souhaités et configurez la programmation du sondage. Vous pouvez consulter les recommandations relatives à la fréquence des sondages du réseau.

3. **Configurer des règles pour ajouter des appareils découverts aux groupes d'administration (facultatif)**

   Si de nouveaux appareils apparaissent sur votre réseau, ils sont détectés à l'occasion de sondages réguliers et sont automatiquement inclus dans le groupe **Appareils non définis**. Vous pouvez configurer des règles de déplacement des appareils pour automatiser l'attribution des appareils au groupe **Appareils administrés**. Vous pouvez aussi configurer des règles de conservation.

   Si vous ignorez l'étape 3, les appareils nouvellement détectés sont affectés au groupe **Appareils non définis**. Vous pouvez déplacer ces appareils vers le groupe **Appareils administrés** manuellement. Si vous déplacez les appareils vers le groupe **Appareils administrés** manuellement, vous pouvez analyser les informations sur chaque appareil et décider si vous voulez le déplacer vers un groupe d'administration, et si oui, quel groupe exact.

Résultats

La réalisation du scénario donne les résultats suivants :

- Le Serveur d'administration de Kaspersky Security Center a trouvé des appareils présents sur le réseau et vous donne des informations à leur sujet.
- Les prochains sondages sont configurés et se déroulent selon le calendrier indiqué.
- Les appareils découverts sont classés selon les règles configurées. (Ou, en l'absence de règles, ils restent dans le groupe **Appareils non définis**).

Appareils non définis

Cette section reprend les informations sur l'utilisation des appareils du réseau de l'entreprise, non inclus dans un groupe d'administration.

Recherche d'appareils

Cette section décrit les types de recherche d'appareils disponibles dans le Kaspersky Security Center et explique l'utilisation de chaque type.

Le Serveur d'administration reçoit des informations sur la structure du réseau et des appareils sur ce réseau par des sondages régulières. Les informations sont enregistrées dans la base de données du Serveur d'administration. Le Serveur d'administration peut réaliser les types de sondage suivants :

- **Sondage du réseau Windows**. Le Serveur d'administration peut effectuer deux types de sondage du réseau Windows : rapide et complet. Lors du sondage rapide, le Serveur d'administration ne reçoit que les informations relatives à la liste des noms NetBIOS des appareils de tous les domaines et des groupes de travail du réseau. Pendant le sondage entier, d'autres informations sont demandées de chaque appareil client comme le nom du système d'exploitation, l'adresse IP, le nom DNS et le nom NetBIOS. Par défaut, les interrogations rapides et complètes sont activées. Le sondage du réseau Windows peut échouer, par exemple, si les ports UDP 137, UDP 138, TCP 139 sont fermés sur le routeur ou par le pare-feu.

- **Sondage Active Directory**. Le Serveur d'administration récupère les informations relatives à la structure de l'unité Active Directory, et les noms DNS des appareils des groupes Active Directory. Par défaut, ce type de sondage est activé. Nous vous recommandons d'utiliser le sondage Active Directory si vous utilisez Active Directory ; sinon, le Serveur d'administration ne trouve aucun appareil. Si vous utilisez Active Directory mais que certains appareils en réseau ne sont pas répertoriés comme membres, ces appareils ne peuvent pas être découverts par un sondage d'Active Directory.

- **Sondage des plages IP**. Le Serveur d'administration sonde les intervalles IP créés à l'aide de paquets ICMP ou le protocole NBNS et reçoit toutes les informations sur les appareils appartenant aux plages IP. Par défaut, ce type de sondage est désactivé. Il n'est pas recommandé d'utiliser ce type de sondage si vous utilisez le sondage réseau et/ou le sondage Active Directory.

- **Sondage Zeroconf**. Un point de distribution qui sonde le réseau IPv6 en utilisant la mise en réseau sans configuration (également appelé *Zeroconf*). Par défaut, ce type de sondage est désactivé. Vous pouvez utiliser le sondage Zeroconf si le point de distribution exécute Linux.

Si vous configurez et activez les règles de déplacement de l'appareil, les appareils détectés sont automatiquement inclus dans le groupe **Appareils administrés**. Si aucune règle de déplacement n'est activée, les nouveaux appareils détectés sont automatiquement inclus dans le groupe **Appareils non définis**.

Vous pouvez modifier les paramètres de recherche d'appareils pour chaque type. Par exemple, il se peut que vous souhaitiez modifier la programmation du sondage ou décider de sonder l'ensemble de la forêt de domaines ou uniquement un domaine en particulier.

Avant de lancer le sondage du réseau, assurez-vous que le protocole SMB est activé. Sinon, Kaspersky Security Center ne peut pas détecter les appareils dans le réseau interrogé. Pour activer le protocole SMB, suivez les instructions correspondant à votre système d'exploitation.

Sondage du réseau Windows

À propos du sondage du réseau Windows

Lors du sondage rapide, le Serveur d'administration ne reçoit que les informations relatives à la liste des noms NetBIOS des appareils de tous les domaines et des groupes de travail du réseau. Au cours d'un sondage complet, les informations suivantes sont demandées à chaque appareil client :

- Nom du système d'exploitation

- Adresse IP

- Nom DNS
- Nom NetBIOS

Les sondages rapides et complets nécessitent les éléments suivants :

- Les ports UDP 137/138, TCP 139, UDP 445 et TCP 445 doivent être disponibles sur le réseau.
- Le protocole SMB est activé.
- Le service Microsoft Computer Browser doit être utilisé et l'ordinateur du navigateur principal doit être activé sur le Serveur d'administration.
- Le service Microsoft Computer Browser doit être utilisé et l'ordinateur du navigateur principal doit être activé sur les appareils clients :
  - Sur au moins un appareil, si le nombre d'appareils en réseau ne dépasse pas 32.
  - Sur au moins un appareil pour 32 appareils en réseau.

Le sondage complet ne peut s'exécuter que si le sondage rapide a été exécuté au moins une fois.

Affichage et modification des paramètres de sondage du réseau Windows

Pour modifier les paramètres du sondage du réseau Windows, procédez comme suit :

1. Dans l'arborescence de la console dans le dossier **Recherche d'appareils**, sélectionnez le sous-dossier **Domaines**.

   Vous pouvez passer au dossier **Appareils non définis** depuis le dossier **Recherche d'appareils** en cliquant sur le bouton **Analyser maintenant**.

   Dans l'espace de travail du sous-dossier **Domaines**, la liste des appareils s'affiche.

2. Cliquez sur **Sonder maintenant**.

   La fenêtre des propriétés du domaine s'ouvre. Vous pouvez modifier les paramètres du sondage du réseau Windows :

   - **Autoriser le sondage du réseau Windows**

     Par défaut, cette option est sélectionnée. Si vous ne souhaitez pas sonder le réseau Windows (par exemple, si vous pensez que le sondage dans Active Directory est suffisant), décochez cette option.

   - **Planifier le sondage rapide**

La période par défaut est de 15 minutes.

Lors du sondage rapide, le Serveur d'administration ne reçoit que les informations relatives à la liste des noms NetBIOS des appareils de tous les domaines et des groupes de travail du réseau.

Les données obtenues à l'issue d'un sondage remplacent complètement les anciennes données.

Les options de programmation du sondage sont disponibles :

- **Tous les N jours**

  Le sondage s'exécute régulièrement, selon l'intervalle défini en jours, à partir de la date et heure définis.

  Le sondage s'exécute par défaut chaque jour, à partir de la date et de l'heure actuelle du système.

- **Toutes les N minutes**

  Le sondage s'exécute régulièrement, selon l'intervalle défini en minutes, à partir de l'heure définie.

  Le sondage s'exécute par défaut toutes les cinq minutes, à partir de l'heure actuelle du système.

- **Par jours de la semaine**

  Le sondage s'exécute régulièrement les jours définis de la semaine, à l'heure indiquée.

  Par défaut, le sondage s'exécute chaque vendredi à 18h00.

- **Chaque mois, les jours indiqués des semaines sélectionnées**

  Le sondage s'exécute régulièrement les jours définis de chaque mois, à l'heure indiquée.

  Par défaut, aucun jour du mois n'est sélectionné. L'heure de lancement par défaut est 18h00.

- **Lancer les tâches non exécutées**

  Si le Serveur d'administration est éteint ou s'il n'est pas disponible au moment auquel le sondage a été programmé, le Serveur d'administrateur peut soit lancer le sondage immédiatement après que le Serveur d'administration a été allumé ou attendre la prochaine programmation du sondage.

  Si cette option est activée, le Serveur d'administration lance le sondage directement après qu'il a été allumé.

  Si cette option est désactivée, le Serveur d'administration attend la prochaine programmation du sondage.

  Cette option est activée par défaut.

- **Planifier le sondage complet**

La période par défaut est une heure. Les données obtenues à l'issue d'un sondage remplacent complètement les anciennes données.

Les options de programmation du sondage sont disponibles :

- **Tous les N jours**

  Le sondage s'exécute régulièrement, selon l'intervalle défini en jours, à partir de la date et heure définis.

  Le sondage s'exécute par défaut chaque jour, à partir de la date et de l'heure actuelle du système.

- **Toutes les N minutes**

  Le sondage s'exécute régulièrement, selon l'intervalle défini en minutes, à partir de l'heure définie.

  Le sondage s'exécute par défaut toutes les cinq minutes, à partir de l'heure actuelle du système.

- **Par jours de la semaine**

  Le sondage s'exécute régulièrement les jours définis de la semaine, à l'heure indiquée.

  Par défaut, le sondage s'exécute chaque vendredi à 18h00.

- **Chaque mois, les jours indiqués des semaines sélectionnées**

  Le sondage s'exécute régulièrement les jours définis de chaque mois, à l'heure indiquée.

  Par défaut, aucun jour du mois n'est sélectionné. L'heure de lancement par défaut est 18h00.

- **Lancer les tâches non exécutées**

  Si le Serveur d'administration est éteint ou s'il n'est pas disponible au moment auquel le sondage a été programmé, le Serveur d'administrateur peut soit lancer le sondage immédiatement après que le Serveur d'administration a été allumé ou attendre la prochaine programmation du sondage.

  Si cette option est activée, le Serveur d'administration lance le sondage directement après qu'il a été allumé.

  Si cette option est désactivée, le Serveur d'administration attend la prochaine programmation du sondage.

  Cette option est activée par défaut.

Si vous souhaitez effectuer le sondage immédiatement, cliquez sur **Sonder maintenant**. Les deux types de sondages commencent.

Sur le Serveur d'administration virtuel, l'affichage et la modification des paramètres du sondage du réseau Windows sont effectués dans la fenêtre des propriétés du point de distribution, dans la section **Recherche d'appareils**.

Sondage Active Directory

Utilisez le sondage Active Directory si vous utilisez Active Directory ; sinon, il est recommandé d'utiliser d'autres types de sondages. Si vous utilisez Active Directory mais que certains appareils en réseau ne sont pas répertoriés comme membres, ces appareils ne peuvent pas être découverts par un sondage d'Active Directory.

Les résultats du sondage d'Active Directory sont conservés pendant 30 jours sur le Serveur d'administration, quels que soient les résultats des sondages suivants.

Avant de lancer le sondage du réseau, assurez-vous que le protocole SMB est activé. Sinon, Kaspersky Security Center ne peut pas détecter les appareils dans le réseau interrogé. Pour activer le protocole SMB, suivez les instructions correspondant à votre système d'exploitation.

Voir et modifier les paramètres de sondage d'Active Directory

Pour voir et modifier les paramètres de sondage des groupes Active Directory, procédez comme suit :

1. Dans l'arborescence de la console, dans le dossier **Recherche d'appareils**, sélectionnez le sous-dossier **Active Directory**.

   Sinon, vous pouvez passer du dossier **Appareils non définis** au dossier **Recherche d'appareils** en cliquant sur le bouton **Sonder maintenant**.

2. Cliquez sur **Configurer les paramètres du sondage**.

   La fenêtre des propriétés d'Active Directory s'ouvre. Vous pouvez modifier les paramètres de sondage du groupe Active Directory :

   - Autoriser le sondage d'Ac&tive Directory

     Par défaut, cette option est sélectionnée. Cependant, si vous n'utilisez pas Active Directory, le sondage ne récupère aucun résultat. Dans ce cas, décochez cette option.

   - Planifier le sondage

La période par défaut est une heure.

Les options de programmation du sondage sont disponibles :

- **Tous les N jours**

  Le sondage s'exécute régulièrement, selon l'intervalle défini en jours, à partir de la date et heure définis.

  Le sondage s'exécute par défaut chaque jour, à partir de la date et de l'heure actuelle du système.

- **Toutes les N minutes**

  Le sondage s'exécute régulièrement, selon l'intervalle défini en minutes, à partir de l'heure définie.

  Le sondage s'exécute par défaut toutes les cinq minutes, à partir de l'heure actuelle du système.

- **Par jours de la semaine**

  Le sondage s'exécute régulièrement les jours définis de la semaine, à l'heure indiquée.

  Par défaut, le sondage s'exécute chaque vendredi à 18h00.

- **Chaque mois, les jours indiqués des semaines sélectionnées**

  Le sondage s'exécute régulièrement les jours définis de chaque mois, à l'heure indiquée.

  Par défaut, aucun jour du mois n'est sélectionné. L'heure de lancement par défaut est 18h00.

- **Lancer les tâches non exécutées**

  Si le Serveur d'administration est éteint ou s'il n'est pas disponible au moment auquel le sondage a été programmé, le Serveur d'administrateur peut soit lancer le sondage immédiatement après que le Serveur d'administration a été allumé ou attendre la prochaine programmation du sondage.

  Si cette option est activée, le Serveur d'administration lance le sondage directement après qu'il a été allumé.

  Si cette option est désactivée, le Serveur d'administration attend la prochaine programmation du sondage.

  Cette option est activée par défaut.

- **Avancé**

Vous pouvez sélectionner les domaines Active Directory à sonder :

- Le domaine Active Directory auquel appartient Kaspersky Security Center.
- La forêt de domaines à laquelle Kaspersky Security Center appartient.
- La liste désignée des domaines Active Directory.

  Si vous décochez cette option, vous pouvez ajouter des domaines à la zone d'action du sondage :

  - Cliquez sur le bouton **Ajouter**.
  - Dans les champs correspondants, indiquez l'adresse du contrôleur de domaine, ainsi que le nom et le mot de passe du compte pour y accéder.
  - Cliquez sur **OK** pour enregistrer les modifications.

  Vous pouvez sélectionner l'adresse du contrôleur de domaine dans la liste et cliquer sur les boutons **Modifier** ou **Éliminer** pour le modifier ou le supprimer.
- Cliquez sur **OK** pour enregistrer les modifications.

Si vous souhaitez effectuer le sondage immédiatement, cliquez sur le bouton **Sonder maintenant**.

Sur le Serveur d'administration virtuel, il est possible de voir et de modifier les paramètres de sondage des groupes Active Directory dans la fenêtre des propriétés du point de distribution, dans la section **Recherche d'appareils**.

Sondage des plages IP

Le Serveur d'administration sonde les intervalles IP créés à l'aide de paquets ICMP ou le protocole NBNS et reçoit toutes les informations sur les appareils appartenant aux plages IP. Par défaut, ce type de sondage est désactivé.

Pour tous les hôtes Linux au sein d'un contrôleur de domaine Microsoft Active Directory ou Samba, spécifiez les paramètres `netbios name` et `workgroup` dans le fichier `/etc/samba/smb.conf`. Dans le cas contraire, les résultats du sondage peuvent contenir des hôtes en double.

Avant de lancer le sondage du réseau, assurez-vous que le protocole SMB est activé. Sinon, Kaspersky Security Center ne peut pas détecter les appareils dans le réseau interrogé. Pour activer le protocole SMB, suivez les instructions correspondant à votre système d'exploitation.

Affichage et modification des paramètres de sondage des plages IP

Pour voir et modifier les paramètres de sondage des groupes de plage IP, procédez comme suit :

1. Dans l'arborescence de la console, dans le dossier **Recherche d'appareils**, sélectionnez le sous-dossier **Plages IP**.

   Vous pouvez passer du dossier **Appareils non définis** au dossier **Recherche d'appareils** en cliquant sur **Sonder maintenant**.

2. Si vous le souhaitez, dans le sous-dossier **Plages IP**, cliquez sur **Ajouter un sous-réseau** pour Ajouter une plage d'adresses IP pour le sondage, puis cliquez sur **OK**.

3. Cliquez sur **Configurer les paramètres du sondage**.

   La fenêtre des propriétés des plages IP s'ouvre. Vous pouvez modifier les paramètres du sondage de la plage d'adresses IP :

   - **Autoriser le sondage de la plage IP**

     Par défaut, cette option n'est pas sélectionnée. Il n'est pas recommandé d'utiliser ce type de sondage si vous utilisez le sondage réseau et/ou le sondage Active Directory.

   - **Planifier le sondage**

La période par défaut est de 420 minutes. Les données obtenues à l'issue d'un sondage remplacent complètement les anciennes données.

Les options de programmation du sondage sont disponibles :

- **Tous les N jours**

  Le sondage s'exécute régulièrement, selon l'intervalle défini en jours, à partir de la date et heure définis.

  Le sondage s'exécute par défaut chaque jour, à partir de la date et de l'heure actuelle du système.

- **Toutes les N minutes**

  Le sondage s'exécute régulièrement, selon l'intervalle défini en minutes, à partir de l'heure définie.

  Le sondage s'exécute par défaut toutes les cinq minutes, à partir de l'heure actuelle du système.

- **Par jours de la semaine**

  Le sondage s'exécute régulièrement les jours définis de la semaine, à l'heure indiquée.

  Par défaut, le sondage s'exécute chaque vendredi à 18h00.

- **Chaque mois, les jours indiqués des semaines sélectionnées**

  Le sondage s'exécute régulièrement les jours définis de chaque mois, à l'heure indiquée.

  Par défaut, aucun jour du mois n'est sélectionné. L'heure de lancement par défaut est 18h00.

- **Lancer les tâches non exécutées**

  Si le Serveur d'administration est éteint ou s'il n'est pas disponible au moment auquel le sondage a été programmé, le Serveur d'administrateur peut soit lancer le sondage immédiatement après que le Serveur d'administration a été allumé ou attendre la prochaine programmation du sondage.

  Si cette option est activée, le Serveur d'administration lance le sondage directement après qu'il a été allumé.

  Si cette option est désactivée, le Serveur d'administration attend la prochaine programmation du sondage.

  Cette option est activée par défaut.

Si vous souhaitez effectuer le sondage immédiatement, cliquez sur **Sonder maintenant**. Ce bouton n'est disponible que si vous avez sélectionné **Autoriser le sondage de la plage IP**.

Sur le Serveur d'administration virtuel, il est possible de consulter et de modifier les paramètres du sondage des plages IP dans la fenêtre des propriétés du point de distribution, dans la section **Recherche d'appareils**. Les appareils clients détectés suite au sondage des plages IP s'affichent dans le dossier **Domaines** du Serveur d'administration virtuel.

Sondage Zeroconf

Ce type de sondage est pris en charge uniquement pour les points de distribution basés sur Linux.

Un point de distribution peut sonder les réseaux qui ont des appareils avec des adresses IPv6. Dans ce cas, les plages IP ne sont pas spécifiées et le point de distribution sonde l'ensemble du réseau en utilisant la mise en réseau sans configuration (également appelée *Zeroconf*). Pour commencer à utiliser Zeroconf, vous devez installer l'utilitaire avahi-browse sur le point de distribution.

Pour activer le sondage Zeroconf :

1. Dans l'arborescence de la console, dans le dossier **Recherche d'appareils**, sélectionnez le sous-dossier **Plages IP**.

   Vous pouvez passer du dossier **Appareils non définis** au dossier **Recherche d'appareils** en cliquant sur **Sonder maintenant**.

2. Cliquez sur **Configurer les paramètres du sondage**.

3. Dans la fenêtre de propriétés des plages IP qui s'ouvre, sélectionnez **Activer le sondage avec la technologie Zeroconf**.

Après cela, le point de distribution commence à sonder votre réseau. Dans ce cas, les plages IP spécifiées sont ignorées.

Travail avec les domaines Windows. Affichage et modification des paramètres du domaine

Pour modifier les paramètres du domaine, procédez comme suit :

1. Dans l'arborescence de la console dans le dossier **Recherche d'appareils**, sélectionnez le sous-dossier **Domaines**.

2. Sélectionnez le domaine et ouvrez la fenêtre de ses propriétés à l'aide d'un des moyens suivants :

   - Dans le menu contextuel du domaine, sélectionnez l'option **Propriétés**.

   - En cliquant sur le lien **Afficher les propriétés du groupe**.

   Finalement, la fenêtre **Propriétés : <Domain name>** s'ouvre qui permet de configurer les paramètres du domaine sélectionnée.

Configuration des règles de rétention pour les appareils non définis

Une fois le sondage du réseau Windows terminé, les appareils trouvés sont placés dans des sous-groupes du groupe d'administration Appareils non définis. Ce groupe d'administration se trouve dans **Avancé** → **Recherche d'appareils** → **Domaines**. Le dossier **Domaines** est le groupe parent. Il contient les groupes enfants nommés après que les domaines et les groupes de travail correspondant ont été trouvés lors du sondages du réseau. Le groupe parent peut également contenir le groupe d'administration des appareils mobiles. Vous pouvez configurer les règles de rétention des appareils non définis pour le groupe parent et pour chacun des groupes enfant. Les règles de rétention ne dépendent pas des paramètres du sondage du réseau et fonctionnent même si le sondage du réseau est désactivé.

Pour configurer les règles de rétention pour les appareils non définis :

1. Dans l'arborescence de la console, dans le dossier **Recherche d'appareils**, effectuez une des opérations suivantes :

   - Pour configurer les paramètres du groupe parent, cliquez-droit sur le sous-dossier **Domaines**, puis sélectionnez **Propriétés**.

     La fenêtre des propriétés du groupe parent s'ouvre.

   - Pour configurer les paramètres d'un groupe enfant, cliquez-droit sur son nom, puis sélectionnez **Propriétés**.

     La fenêtre des propriétés du groupe enfant s'ouvre.

2. Dans la section **Appareils**, définissez les paramètres suivants :

   - **Supprimer l'appareil du groupe après une inactivité de plus de (jours)**

     Quand cette option est activée, vous pouvez définir la période à l'issue de laquelle un appareil est supprimé automatiquement du groupe. Cette option est également distribuée par défaut aux groupes enfants. Par défaut, la valeur de cet intervalle est de 7 jours.

     Cette option est activée par défaut.

   - **Hériter du groupe parent**

     Si cette option est activée, la période de conservation pour les appareils dans le groupe actif est héritée du groupe parent et ne peut être modifiée.

     Cette option est disponible uniquement pour les groupes enfant.

     Cette option est activée par défaut.

   - **Forcer l'héritage des groupes enfants**

     Les valeurs des paramètres sont diffusées dans les groupes enfants mais ces paramètres sont verrouillés dans les propriétés des groupes enfants.

     Cette option est Inactif par défaut.

Vos modifications sont enregistrées et appliquées.

Travail avec les plages IP

Vous pouvez configurer les paramètres des plages IP existantes, ainsi que créer les nouvelles plages IP.

Création de la plage IP

Pour créer une plage IP, procédez comme suit :

1. Dans l'arborescence de la console, dans le dossier **Recherche d'appareils**, sélectionnez le sous-dossier **Plages IP**.
2. Dans le menu contextuel du dossier, sélectionnez l'option **Nouveau → Plage IP**.
3. Dans la fenêtre **Nouvelle plage IP** qui s'ouvre, configurez les nouveaux paramètres de la plage IP créée.

La plage IP créée apparaît dans le dossier **Plages IP**.

Affichage et modification des paramètres de plage IP

Pour modifier les paramètres de la plage IP, procédez comme suit :

1. Dans l'arborescence de la console, dans le dossier **Recherche d'appareils**, sélectionnez le sous-dossier **Plages IP**.
2. Sélectionnez la plage IP et ouvrez la fenêtre de ses propriétés à l'aide d'un des moyens suivants :
   - Dans le menu contextuel de la plage IP, sélectionnez l'option **Propriétés**.
   - En cliquant sur le lien **Afficher les propriétés du groupe**.

Finalement, la fenêtre **Propriétés : <Nom de plage IP>** s'ouvre qui permet de configurer les paramètres de la plage IP sélectionnée.

Travail avec les groupes Active Directory. Affichage et modification des paramètres du groupe

Pour modifier les paramètres du groupe Active Directory, procédez comme suit :

1. Dans l'arborescence de la console, dans le dossier **Recherche d'appareils**, sélectionnez le sous-dossier **Active Directory**.
2. Sélectionnez le groupe Active Directory et ouvrez la fenêtre de ses propriétés à l'aide d'un des moyens suivants :
   - Dans le menu contextuel de la plage IP, sélectionnez l'option **Propriétés**.
   - En cliquant sur le lien **Afficher les propriétés du groupe**.

   Finalement, la fenêtre **Propriétés : <Nom du groupe Active Directory>** s'ouvre qui permet de configurer les paramètres du groupe Active Directory sélectionné.

Création des règles de déplacement automatique des appareils dans un groupe d'administration

Vous pouvez configurer le déplacement automatique des appareils, détectés lors du sondage du réseau de l'entreprise, dans les groupes d'administration.

Pour configurer la règle de déplacement automatique des appareils dans les groupes d'administration, procédez comme suit :

1. Dans l'arborescence de la console sélectionnez le dossier **Appareils non définis**.
2. Dans l'espace de travail de ce dossier, cliquez sur **Configurer les règles**.

   Cela permet d'ouvrir la fenêtre **Propriétés : Appareils non définis**. Dans la section **Déplacer les appareils**, configurez la règle de déplacement automatique des appareils dans les groupes d'administration.

La première règle applicable de la liste (du haut vers le bas de la liste) sera appliquée à un appareil.

Utilisation du mode dynamique VDI sur les appareils clients

Le réseau de l'entreprise peut contenir une infrastructure virtuelle sur la base de machines virtuelles temporaires. Kaspersky Security Center détecte les machines virtuelles temporaires et ajoute les données qui les concernent à la base de données du Serveur d'administration. Une fois que l'utilisateur a terminé de travailler avec la machine virtuelle temporaire, celle-ci est supprimée de l'infrastructure virtuelle Toutefois, l'entrée relative à la machine virtuelle supprimée peut être conservée dans la base de données du Serveur d'administration. De plus, les machines virtuelles inexistantes peuvent apparaître dans la Console d'administration.

Pour éviter de conserver des données relatives à des machines virtuelles qui n'existent pas, Kaspersky Security Center prend en charge le mode dynamique pour Virtual Desktop Infrastructure (VDI). L'administrateur peut activer la prise en charge du mode dynamique pour VDI dans les propriétés du paquet d'installation de l'Agent d'administration qui sera installé sur la machine virtuelle temporaire.

Lors de l'arrêt de la machine virtuelle temporaire, l'Agent d'administration informe le Serveur d'administration de l'arrêt. Si la machine virtuelle a bien été arrêtée, elle est supprimée de la liste des appareils connectés au Serveur d'administration. Si l'arrêt de la machine virtuelle n'est pas réalisé comme il se doit et que l'Agent d'administration n'a pas notifié le Serveur d'administration de l'arrêt, c'est le scénario de réserve qui est suivi. D'après ce scénario, la machine virtuelle est supprimée de la liste des appareils connectés au Serveur d'administration après trois tentatives échouées de synchronisation avec le Serveur.

Activation du mode dynamique VDI dans les propriétés du paquet d'installation de l'Agent d'administration

Pour activer le mode dynamique VDI, procédez comme suit :

1. Dans l'arborescence de la console, dans le dossier **Installation à distance**, sélectionnez le sous-dossier **Paquets d'installation**.
2. Dans le menu contextuel du paquet d'installation de l'Agent d'administration, sélectionnez l'option **Propriétés**.

   La fenêtre **Paramètres : Agent d'administration de Kaspersky Security Center** s'ouvre.
3. Dans la fenêtre **Propriétés : Agent d'administration de Kaspersky Security Center**, sélectionnez la section **Avancé**.
4. Dans la section **Avancé**, sélectionnez l'option **Activer le mode dynamique pour VDI**.

L'appareil sur lequel l'Agent d'administration s'installe sera membre d'une VDI.

Recherche d'appareils qui font partie de VDI

Pour rechercher les appareils non définis qui font partie de VDI, procédez comme suit :

1. Sélectionnez **Recherche** dans le menu contextuel du dossier **Appareils non définis**.

   Pour consulter la liste de tous les appareils qui font partie de Virtual Desktop Infrastructure, sélectionnez l'option **Recherche** dans le menu contextuel du dossier du **Serveur d'administration**.
2. Dans l'onglet **Recherche** de la fenêtre **Machines virtuelles**, sélectionnez l'option **Oui** dans le groupe de paramètres **Membre d'une Virtual Desktop Infrastructure**.
3. Cliquez sur le bouton **Rechercher**.

La liste des appareils non définis qui font partie de Virtual Desktop Infrastructure s'affiche.

Déplacement dans le groupe d'administration des appareils qui font partie de VDI

Pour déplacer les appareils qui font partie de VDI dans le groupe d'administration, procédez comme suit :

1. Dans l'espace de travail du dossier, **Appareils non définis**, cliquez sur **Configurer les règles**.

   Finalement, la fenêtre des propriétés du dossier **Appareils non définis** s'ouvre.

2. Dans la fenêtre des propriétés du dossier **Appareils non définis**, dans la section **Déplacer les appareils**, cliquez sur le bouton **Ajouter**.

   La fenêtre **Nouvelle règle** s'ouvre.

3. Dans la fenêtre **Nouvelle règle**, sélectionnez la section **Machines virtuelles**.

4. Dans la liste déroulante **Est une machine virtuelle**, sélectionnez **Oui**.

La règle de déplacement des appareils dans le groupe d'administration sera créée.

Inventaire du matériel

La liste du matériel (**Stockages** → **Matériel**) que vous utilisez pour faire l'inventaire du matériel est alimentée de deux façons : automatiquement et manuellement. Après chaque sondage du réseau, tous les appareils détectés sont automatiquement ajoutés à la liste. Cependant, vous pouvez également ajouter des appareils manuellement si vous ne souhaitez pas sonder le réseau. Vous pouvez ajouter manuellement d'autres appareils à la liste, par exemple des routeurs, des imprimantes ou du matériel informatique.

Il est possible de consulter et de modifier les informations détaillées sur les appareils dans les propriétés de l'appareil.

La liste du matériel détecté peut contenir les types suivants des appareils :

- Ordinateurs
- Appareils mobiles
- Appareils réseau
- Appareils virtuels
- Modules d'ordinateur
- Périphérie d'ordinateur
- Appareils connectés
- Téléphonie VoIP
- Stockages réseau

L'administrateur peut attribuer l'indice *Matériel corporatif* aux appareils détectés. Cet indice peut être manuellement attribué dans les propriétés de l'appareil ou définir les critères pour son attribution automatique. Dans ce cas, l'indice *Matériel corporatif* est attribué selon le type d'appareil.

Kaspersky Security Center permet d'exécuter l'amortissement du matériel. Pour cela, sélectionnez l'option **L'a&ppareil est radié** dans les propriétés d'un appareil. Un tel appareil ne s'affiche pas dans la liste du matériel.

L'administrateur peut manipuler la liste des contrôleurs logiques programmables (PLC) dans le dossier **Matériel**. Les informations détaillées sur la manipulation des listes de contrôleurs logiques programmables figurent dans le *Manuel de l'utilisateur de Kaspersky Industrial CyberSecurity for Nodes*.

Ajout d'informations sur les nouveaux appareils

Pour ajouter les informations sur les nouveaux appareils dans le réseau, procédez comme suit :

1. Dans l'arborescence de la console **Stockages**, sélectionnez le sous-dossier **Matériel**.
2. Dans l'espace de travail du dossier **Matériel** à l'aide du bouton **Ajouter un appareil**, ouvrez la fenêtre **Nouvel appareil**.

   La fenêtre **Nouvel appareil** s'ouvre.
3. Dans la fenêtre **Nouvel appareil**, dans la liste déroulante **Type**, sélectionnez le type d'appareil que vous souhaitez ajouter.
4. Cliquez sur le bouton **OK**.

   La fenêtre des propriétés de l'appareil s'ouvre sur la section **Général**.
5. Dans la section **Général**, remplissez les champs de saisie avec les données sur l'appareil. La section **Général** répertorie les paramètres suivants :

   - **&Appareil d'entreprise**. Cochez la case si vous voulez attribuer l'indice *Corporatif* à l'appareil. Avec cet attribut, il est possible de rechercher des appareils dans le dossier **Matériel**.
   - **L'a&ppareil est radié**. Cochez la case si vous ne voulez pas afficher l'appareil dans la liste des appareils dans le dossier **Matériel**.
6. Cliquez sur le bouton **Appliquer**.

Le nouvel appareil s'affiche dans l'espace de travail du dossier **Matériel**.

Configuration des critères de définition des appareils d'entreprise

Pour configurer les critères de définition des appareils d'entreprise, procédez comme suit :

1. Dans l'arborescence de la console **Stockages**, sélectionnez le sous-dossier **Matériel**.
2. Dans l'espace de travail du dossier **Matériel**, cliquez sur le bouton **Actions supplémentaires**, et, dans la liste déroulante, sélectionnez **Configurer la règle pour les appareils d'entreprise**.

   La fenêtre de propriétés du matériel s'affiche.

3. Dans la fenêtre des propriétés du matériel, dans la section **Appareils d'entreprise**, sélectionnez une méthode pour attribuer l'indice *Entreprise* à l'appareil :

   - **Établir &manuellement l'Attribut Appareil d'entreprise pour l'appareil**. L'indice *Matériel d'entreprise* est attribué à l'appareil manuellement dans la fenêtre des propriétés de l'appareil, dans la section **Général**.
   - **Établir &automatiquement l'Attribut Appareil d'entreprise pour l'appareil**. Dans le groupe de paramètres **Selon le type d'appareil**, définissez les types des appareils auxquels l'application va automatiquement attribuer l'indice *Entreprise*.

     Cette option affecte uniquement les appareils qui ont été ajoutés via l'interrogation du réseau. Pour les appareils ajoutés manuellement, définissez l'indice *Entreprise* manuellement.

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

Les critères de détection des appareils d'entreprise sont configurés.

Configuration des champs personnalisés

Pour configurer les champs personnalisés d'appareils, procédez comme suit :

1. Dans l'arborescence de la console **Stockages**, sélectionnez le sous-dossier **Matériel**.
2. Dans l'espace de travail du dossier **Matériel**, cliquez sur le bouton **Actions supplémentaires** et dans le menu déroulant, choisissez l'option **Configurer des champs de données personnalisés**.

   La fenêtre de propriétés du matériel s'affiche.
3. Dans la fenêtre de propriétés du matériel, sélectionnez la section **Champs personnalisés** et cliquez sur le bouton **Ajouter**.

   La fenêtre **Ajouter un champ** s'ouvre.
4. Dans la fenêtre **Ajouter un champ**, indiquez le nom du champ personnalisé qui s'affichera dans les propriétés du matériel.

   Vous pouvez créer plusieurs champs personnalisés avec des noms uniques.
5. Cliquez sur le bouton **OK**.

Les champs personnalisés ajoutés s'afficheront dans la section **Champs personnalisés** des propriétés du matériel. Vous pouvez utiliser des champs personnalisés pour l'indication d'informations spécifiques sur les appareils. Par exemple, le numéro de la demande intérieure d'acquisition de matériel.

Licences

Cette section présente les notions principales relatives à la licence de Kaspersky Security Center 15.1.

Événements de dépassement de la restriction de licence

Kaspersky Security Center permet d'obtenir des informations sur les événements de dépassement de la restriction de licence des applications Kaspersky installées sur les appareils clients.

Le niveau d'importance des événements de dépassement de la limite de licence est défini conformément aux règles suivantes :

- Si le nombre d'unités de licence utilisées se trouve entre 90 et 100 % du total des unités de licence de cette licence, l'événement avec le niveau d'importance **Information** est publié.
- Si le nombre d'unités de licence utilisées se trouve entre 100 et 110 % du total d'unités de licence de cette licence, l'événement avec le niveau d'importance **Avertissement** est publié.
- Si le nombre d'unités de licence utilisées dépasse 110 % du total d'unités de licence de cette licence, l'événement avec le niveau d'importance **Événement critique** est publié.

À propos des licences

Cette section contient des informations sur les licences des applications Kaspersky administrées via Kaspersky Security Center.

À propos de la licence

La *licence* est un droit d'utilisation limité dans le temps de Kaspersky Security Center, accordé selon les termes du Contrat de licence signé (Contrat de licence utilisateur final).

Le volume de services et la durée de validité dépendent de la licence sous laquelle l'application est utilisée.

Les types suivants de licences sont prévus :

- *Évaluation*

  Une licence gratuite conçue pour découvrir l'application. La licence d'évaluation présente une courte durée de validité.

  A l'expiration de la licence, Kaspersky Security Center cesse de remplir toutes ces fonctions. Pour continuer à utiliser l'application, vous devez acheter une licence commerciale.

  Vous pouvez utiliser l'application à l'aide d'une licence d'évaluation pendant une seule période d'évaluation.

- *Commerciale*

  Une licence payante.

  À l'expiration de la licence commerciale, les fonctionnalités clés de l'application sont désactivées. Pour continuer à utiliser Kaspersky Security Center, il faut renouveler la licence commerciale. Après l'expiration de la licence commerciale, vous ne pouvez plus utiliser l'application et vous devez la supprimer de votre appareil.

  Il est conseillé de renouveler votre licence avant son expiration, pour garantir une protection ininterrompue contre toutes les menaces de sécurité.

À propos du contrat de licence utilisateur final

Le Contrat de licence utilisateur final (ou CLUF) est un accord juridique conclu entre vous et AO Kaspersky Lab qui stimule les conditions d'utilisation du logiciel que vous avez acheté.

Veuillez lire attentivement le Contrat de licence avant de commencer à utiliser l'application.

Kaspersky Security Center et ses modules, par exemple l'Agent d'administration, font l'objet d'un CLUF qui leur est propre.

Vous pouvez prendre connaissance des conditions du Contrat de licence utilisateur final de Kaspersky Security Center de l'une des manières suivantes :

- Lors de l'installation de Kaspersky Security Center.
- Par la lecture du document license.txt inclus dans le kit de distribution de Kaspersky Security Center.
- Par la lecture du document license.txt inclus dans le dossier d'installation de Kaspersky Security Center.
- En téléchargeant le fichier license.txt sur le site de Kaspersky.

Vous pouvez prendre connaissance des conditions du Contrat de licence utilisateur final de l'Agent d'administration pour Windows, de l'Agent d'administration pour Mac et de l'Agent d'administration pour Linux de l'une des manières suivantes :

- Lors du téléchargement du paquet de distribution de l'Agent d'administration à partir des serveurs Web de Kaspersky.
- Pendant l'installation de l'Agent d'administration pour Windows, de l'Agent d'administration pour Mac ou de l'Agent d'administration pour Linux.
- En lisant le document license.txt inclus dans le paquet de distribution de l'Agent d'administration pour Windows, l'Agent d'administration pour Mac, ou de l'Agent d'administration pour Linux.
- En lisant le document license.txt dans le dossier d'installation de l'Agent d'administration pour Windows, de l'Agent d'administration pour Mac ou de l'Agent d'administration pour Linux.
- En téléchargeant le fichier license.txt sur le site de Kaspersky.

Vous acceptez les conditions du contrat de licence utilisateur final, en confirmant votre accord avec le texte du contrat de licence utilisateur final lors de l'installation de l'application. Si vous refusez les dispositions du Contrat de licence, annulez l'installation de l'application et n'utilisez pas l'application.

À propos du certificat de licence

Le *certificat de licence* est un document qui vous est transmis avec le fichier clé ou le code d'activation.

Il comporte les informations suivantes à propos de la licence :

- Identifiant de licence ou numéro de commande
- informations relatives à l'utilisateur qui reçoit la licence
- informations relatives à l'application qui peut être activée à l'aide de la licence
- restrictions associées au nombre d'unités concernées par la licence (par exemple, le nombre d'appareils sur lesquels l'application peut être utilisée avec la licence)
- début de durée de validité de la licence
- date de fin de la durée de validité de la licence ou durée de validité de la licence
- type de licence

À propos de la clé de licence

Une *clé de licence* est une séquence de caractères qui vous permet d'activer puis d'utiliser l'application conformément aux conditions du Contrat de licence utilisateur final. Les clés de licence sont créées par les experts de Kaspersky.

Vous pouvez ajouter une clé de licence à l'application d'une des manières suivantes : utiliser le *fichier clé* ou saisir le *code d'activation*. Une fois ajoutée, la clé de licence s'affiche dans l'interface de l'application sous la forme d'une séquence alphanumérique unique.

La clé de licence peut être bloquée par Kaspersky en cas de non-respect des conditions du Contrat de licence. Si la clé de licence est bloquée, vous devez ajouter une autre clé pour pouvoir utiliser l'application.

Une clé de licence peut être active ou complémentaire (ou de réserve).

Une *clé de licence active* est une clé actuellement utilisée par l'application. Une clé de licence active peut être ajoutée pour une licence d'évaluation ou commerciale. Il ne peut pas y avoir plus d'une clé de licence active par application.

Une *clé de licence complémentaire (ou de réserve)* est une clé de licence qui permet à l'utilisateur d'utiliser l'application, mais qui n'est pas active. La clé de licence complémentaire est automatiquement active si la validité de la licence associée à la clé de licence active expire. Une clé de licence complémentaire ne peut être ajoutée que si une clé de licence active a déjà été ajoutée.

Une clé de licence d'évaluation ne peut être ajoutée qu'en tant que clé de licence active. Une clé de licence d'essai ne sera pas acceptée comme clé de licence complémentaire.

À propos du fichier clé

Le *fichier clé* est un fichier doté d'une extension .key qui vous est fourni par Kaspersky. Les fichiers clés servent à activer l'application en ajoutant une clé de licence.

Vous recevez un fichier clé à l'adresse email que vous avez indiquée à l'achat de Kaspersky Security Center ou après la commande d'une version d'essai de Kaspersky Security Center.

L'activation de l'application à l'aide d'un fichier clé ne requiert pas de connexion aux serveurs d'activation de Kaspersky.

Vous pouvez restaurer un fichier clé qui a été supprimé par accident. Par exemple, vous pourriez avoir besoin d'un fichier clé pour enregistrer un Kaspersky CompanyAccount.

Pour restaurer le fichier clé, effectuez une des opérations suivantes :

- Contactez le fournisseur de licences.
- Obtenir le fichier clé sur le site Internet de Kaspersky à partir du code d'activation que vous possédez.
- Exportez un fichier de clé de licence à partir d'un autre Serveur d'administration.

À propos de l'abonnement

Abonnement à Kaspersky Security Center est une commande d'utilisation de l'application avec les paramètres sélectionnés (date de fin de l'abonnement, nombre de appareils protégés). L'abonnement à Kaspersky Security Center peut être enregistré auprès du fournisseur de services (par exemple, auprès du fournisseur d'accès à Internet). Il est possible de prolonger l'abonnement en mode manuel et automatique, ainsi que de le refuser.

L'abonnement peut être limité (par exemple pour un an) ou illimité (sans date de fin). Pour continuer à utiliser Kaspersky Security Center après la fin de l'abonnement limité, celui-ci doit être prolongé. L'abonnement illimité se prolonge automatiquement à condition d'avoir été payé en temps voulu au fournisseur de services.

Si l'abonnement est limité, une période de grâce peut être instituée à la fin de la validité pour le prolonger. Au cours de cette période, la fonctionnalité de l'application est conservée. Le fournisseur de services détermine l'existence et la durée de la période de grâce.

L'utilisation de Kaspersky Security Center sur abonnement nécessite l'application d'un code d'activation communiqué par le fournisseur de services.

Vous pouvez appliquer un autre code d'activation pour l'utilisation de Kaspersky Security Center uniquement après la fin de l'abonnement ou le refus de celui-ci.

Les ensembles d'actions possibles pour gérer l'abonnement peuvent varier en fonction du fournisseur de services. Celui-ci peut ne pas offrir de période de grâce pour le prolongement de l'abonnement au cours de laquelle la fonctionnalité de l'application est conservée.

Les codes d'activation reçus lors de l'abonnement ne peuvent pas être utilisés pour l'activation de versions précédentes de Kaspersky Security Center.

Lors de l'utilisation de l'application sur abonnement, Kaspersky Security Center s'adresse automatiquement au serveur d'activation dans un laps de temps déterminé jusqu'à la date de fin de l'abonnement. De cette manière, les informations d'abonnement sont synchronisées avec celles du serveur d'activation. Si l'accès au serveur via le DNS système n'est pas possible, l'application utilise les serveurs DNS publics. Vous pouvez prolonger l'abonnement sur le site Internet du fournisseur de services.

Vous pouvez mettre à jour les informations pour l'abonnement manuellement, sans attendre que Kaspersky Security Center accède au serveur d'activation. Par exemple, cela peut être utile lorsque vous modifiez les paramètres de l'abonnement.

Pour mettre à jour manuellement les informations sur l'abonnement, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le dossier **Licences Kaspersky**.
2. Cliquez sur **Actions supplémentaires**, puis dans la liste déroulante, sélectionnez **Synchroniser les paramètres d'abonnement avec le Serveur de licences**.

Les informations relatives à l'abonnement sont mises à jour sur le serveur d'activation.

À propos du code d'activation

Le *code d'activation* est une suite unique de 20 caractères alphanumériques. Vous saisissez un code d'activation pour ajouter une clé de licence qui active Kaspersky Security Center. Vous recevez le code d'activation à l'adresse email que vous avez indiquée après l'achat de Kaspersky Security Center ou après la commande d'une version d'essai de Kaspersky Security Center.

Pour activer l'application à l'aide du code d'activation, vous avez besoin d'un accès Internet pour vous connecter aux serveurs d'activation de Kaspersky. Si l'accès aux serveurs via le DNS système n'est pas possible, l'application utilise les serveurs DNS publics.

Si l'application a été activée à l'aide d'un code d'activation, dans certains cas après l'activation, l'application envoie des requêtes régulières au serveur d'activation de Kaspersky pour vérifier le statut de la clé de licence. Pour pouvoir envoyer des requêtes, vous devez fournir un accès Internet pour l'application.

Si vous avez perdu votre code d'activation après l'installation de l'application, contactez le partenaire Kaspersky auprès duquel vous avez acheté la licence.

Vous ne pouvez pas utiliser de fichiers clés pour activer des applications administrées ; seuls les codes d'activation sont acceptés.

Révocation d'un Contrat de licence utilisateur final

Si vous décidez d'arrêter la protection de vos appareils clients, vous pouvez désinstaller les applications de Kaspersky administrées et révoquer votre Contrat de licence utilisateur final (CLUF) pour ces applications.

Pour révoquer un CLUF pour les applications Kaspersky administrées :

1. Dans l'arborescence de la console, sélectionnez **Serveur d'administration → Avancé → CLUF acceptés**.

   Une liste des CLUF acceptés s'affiche lors de la création des paquets d'installation, lors de l'installation transparente des mises à jour ou lors du déploiement de Kaspersky Security for Mobile.

2. Dans la liste, sélectionnez le CLUF que vous souhaitez révoquer.

   Vous pouvez afficher les propriétés suivantes du CLUF :

   - Date d'acceptation du CLUF.
   - Nom de l'utilisateur ayant accepté le CLUF.
   - Lien vers les conditions du CLUF.
   - Liste des objets connectés au CLUF : noms des paquets d'installation, noms des mises à jour continues, noms des applications mobiles.

3. Cliquez sur le bouton **Révoquer le CLUF**.

   Une fenêtre qui s'ouvre vous informe que vous devez désinstaller l'application Kaspersky correspondant au CLUF.

4. Cliquez sur le bouton pour confirmer la révocation.

   Kaspersky Security Center vérifie si les paquets d'installation (correspondant à l'application Kaspersky administrée dont vous souhaitez révoquer le CLUF) sont supprimés.

   Vous ne pouvez révoquer que le CLUF pour une application Kaspersky administrée, dont les paquets d'installation sont supprimés.

Le CLUF est révoqué. Il ne s'affiche plus dans la liste des CLUF dans la section **Serveur d'administration → Avancé → CLUF acceptés**. Vous ne pouvez pas protéger les appareils clients à l'aide d'une application Kaspersky dont vous avez révoqué le CLUF.

À propos de la collecte des données

Données transférées à des tiers

Le service Google Firebase Cloud Messaging est utilisé lors de l'utilisation de la fonctionnalité d'administration des appareils mobiles du Logiciel afin de fournir en temps voulu des commandes aux appareils exécutant le système d'exploitation Android via le mécanisme de notification push. Si l'Utilisateur a configuré l'utilisation du service Google Firebase Cloud Messaging, l'Utilisateur accepte de fournir les informations suivantes au service Google Firebase Cloud Messaging en mode automatique : les identifiants d'installation des applications Kaspersky Endpoint Security for Android vers lesquelles les notifications push doivent être envoyées.

Pour bloquer l'échange d'informations avec le service Google Firebase Cloud Messaging, l'Utilisateur doit rétablir les paramètres d'utilisation du service Google Firebase Cloud Messaging à leurs valeurs d'usine.

Le service Apple Push Notification Service (APNs) est utilisé lors de l'utilisation de la fonctionnalité d'administration des appareils mobiles du Logiciel afin de fournir en temps voulu des commandes aux appareils exécutant le système d'exploitation iOS via le mécanisme de notification push. Si l'Utilisateur a installé un certificat APNs sur un Serveur MDM iOS, créé un profil MDM iOS avec une série de paramètres pour la connexion des appareils mobiles iOS au Logiciel et installé ce profil sur ses appareils mobiles, l'Utilisateur accepte de fournir les informations suivantes à APNs en mode automatique :

- Jeton : jeton push de l'appareil. Le serveur utilise ce jeton lors de l'envoi de notifications push à l'appareil.
- PushMagic : chaîne qui doit être incluse dans la notification push. La valeur de chaîne est générée par l'appareil.

Données traitées localement

L'application Kaspersky Security Center a été développée pour centraliser les principales tâches d'administration et assurer le système de protection du réseau d'une entreprise. Kaspersky Security Center offre à l'administrateur l'accès aux informations détaillées sur le niveau de sécurité du réseau de l'organisation et permet à l'administrateur de configurer tous les modules de protection élaborée à partir des applications de Kaspersky. L'application Kaspersky Security Center exécute les fonctions principales suivantes :

- Détection des appareils et de leurs utilisateurs sur le réseau de l'entreprise
- Création d'une hiérarchie de groupes d'administration pour la gestion des appareils
- Installation d'applications Kaspersky sur des appareils
- Gestion des paramètres et des tâches des applications installées
- Gestion des mises à jour pour Kaspersky et des applications tierces, recherche et correction des vulnérabilités
- Activation des applications de Kaspersky sur les appareils
- Administration des comptes utilisateurs
- Affichage des informations sur le fonctionnement des applications Kaspersky sur les appareils
- Affichage des rapports

Pour remplir ses principales fonctions, Kaspersky Security Center peut recevoir, stocker et traiter les informations suivantes :

- Informations sur les appareils du réseau de l'organisation reçues via l'analyse des domaines Windows, ou des contrôleurs de domaine Active Directory ou Samba, ou via l'analyse des plages IP. Le Serveur d'administration récupère les données indépendamment ou reçoit les données de l'Agent d'administration agissant en tant que point de distribution.
- Informations d'Active Directory et de Samba sur les unités organisationnelles, les domaines, les utilisateurs et les groupes. Le Serveur d'administration récupère les données indépendamment ou reçoit les données de l'Agent d'administration agissant en tant que point de distribution.

- Détails relatifs aux appareils administrés. L'Agent d'administration transfère les données répertoriées ci-dessous de l'appareil vers le Serveur d'administration. L'utilisateur saisit le nom d'affichage et la description de l'appareil dans l'interface de la Console d'administration ou dans l'interface de Kaspersky Security Center Web Console :

  - Spécifications techniques de l'appareil administré et de ses modules requis pour l'identification de l'appareil : nom d'affichage et description de l'appareil, nom et type du domaine Windows, nom de l'appareil dans l'environnement Windows, domaine DNS et nom DNS, adresse IPv4, adresse IPv6, emplacement réseau, adresse MAC, numéro de série, type de système d'exploitation, si l'appareil est une machine virtuelle avec le type d'hyperviseur et si l'appareil est une machine virtuelle dynamique dans le cadre de VDI.

  - Autres spécifications des appareils administrés et de leurs modules requises pour l'audit des appareils administrés et pour décider si certains correctifs et mises à jour spécifiques sont applicables : état de l'Agent de mises à jour Windows (WUA), architecture du système d'exploitation, fournisseur du système d'exploitation, numéro de version du système d'exploitation, ID de version du système d'exploitation, dossier d'emplacement du système d'exploitation ; si l'appareil est une machine virtuelle, le type de machine virtuelle, le nom du Serveur d'administration virtuel qui administre l'appareil, les données d'appareil cloud (région Cloud, VPC, zone de disponibilité Cloud, sous-réseau Cloud, zone de positionnement Cloud).

  - Détails relatifs aux actions sur les appareils administrés : date et heure de la dernière mise à jour, heure de la dernière apparition de l'appareil sur le réseau, état du temps d'attente au redémarrage et heure de mise sous tension de l'appareil.

  - Détails des comptes utilisateurs de l'appareil et de leurs sessions de travail.

- Données reçues lors de l'exécution des diagnostics à distance sur un appareil géré : fichiers de trace, informations système, détails des applications Kaspersky installées sur l'appareil, fichiers de vidage, journaux d'événements, résultats de l'exécution des scripts de diagnostic reçus du support technique de Kaspersky.

- Statistiques de fonctionnement des points de distribution si l'appareil est un point de distribution. L'Agent d'administration transfère les données de l'appareil vers le Serveur d'administration.

- Paramètres du point de distribution saisis par l'utilisateur dans la Console d'administration ou Kaspersky Security Center Web Console.

- Données nécessaires à la connexion des appareils mobiles au Serveur d'administration : certificat, port de connexion mobile, adresse de connexion au Serveur d'administration. L'Utilisateur saisit des données dans la Console d'administration ou dans Kaspersky Security Center Web Console.

- Détails des appareils mobiles transférés via le protocole MDM iOS. Les données répertoriées ci-dessous sont transférées à partir de l'appareil mobile vers le Serveur d'administration :

  - Caractéristiques techniques de l'appareil mobile et de ses modules requis pour l'identification de l'appareil : nom l'appareil, modèle, nom du système d'exploitation, numéro de version du système d'exploitation, numéro de modèle de l'appareil, numéro IMEI, UDID, MEID, numéro de série, volume de mémoire, version du firmware du modem, adresse MAC Bluetooth, adresse MAC Wi-Fi et détails de la carte SIM (ICCID en tant que partie de l'ID de carte SIM).

  - Détails du réseau mobile utilisé par l'appareil administré : type de réseau mobile, nom du réseau mobile en cours d'utilisation, nom du réseau mobile domestique, version des paramètres d'opérateur du réseau mobile, état de l'itinérance des appels et de l'itinérance des données, code de pays du réseau domicile, code de pays de résidence, code pays du réseau en cours d'utilisation et niveau de chiffrement.

  - Paramètres de sécurité de l'appareil mobile : utilisation d'un mot de passe et conformité de celui-ci avec les paramètres de la stratégie, liste des profils de configuration et des profils provisioning utilisés pour l'installation d'applications d'éditeurs tiers.

  - Date de la dernière synchronisation avec le Serveur d'administration et état de l'administration de l'appareil.

- Détails des applications Kaspersky installées sur l'appareil. L'application administrée transfère les données de l'appareil vers le Serveur d'administration via l'Agent d'administration :

  - Paramètres des applications Kaspersky installées sur l'appareil administré : nom et version de l'application Kaspersky, état, état de la protection en temps réel, date et heure de la dernière analyse de l'appareil, nombre de menaces détectées, nombre d'objets qui n'ont pas pu être désinfectés, disponibilité et état des modules de l'application, heure de la dernière mise à jour et version des bases antivirus, détails des paramètres et des tâches de l'application Kaspersky, informations sur les clés de licence active et de réserve, date d'installation et ID de l'application.

  - Statistiques sur le fonctionnement de l'application : événements liés aux modifications de l'état des modules de l'application Kaspersky sur l'appareil administré et sur les performances des tâches lancées par les modules de l'application.

  - État de l'appareil défini par l'application Kaspersky.

  - Tags attribués par l'application Kaspersky.

  - Ensemble de mises à jour installées et applicables pour l'application Kaspersky.

- Données comprises dans les événements des modules de Kaspersky Security Center et des applications administrées par Kaspersky. L'Agent d'administration transfère les données de l'appareil vers le Serveur d'administration.

- Données nécessaires à l'intégration de Kaspersky Security Center avec un système SIEM pour l'exportation d'événements. L'Utilisateur saisit des données dans la Console d'administration ou dans Kaspersky Security Center Web Console.

- Paramètres des composants de Kaspersky Security Center et des applications administrées par Kaspersky présentés dans les stratégies et les profils de stratégie. L'utilisateur entre des données dans la Console d'administration ou dans l'interface de Kaspersky Security Center Web Console.

- Paramètres des tâches des composants de Kaspersky Security Center et des applications administrées par Kaspersky. L'utilisateur entre des données dans la Console d'administration ou dans l'interface de Kaspersky Security Center Web Console.

- Données traitées par la fonction de la gestion des vulnérabilités et des correctifs. L'Agent d'administration transfère les données répertoriées ci-dessous de l'appareil vers le Serveur d'administration :
  - Détails relatifs aux applications et aux correctifs installés sur les appareils administrés (registre des applications).
  - Informations sur le matériel détecté sur les appareils administrés (Registre du matériel).

    Si l'Agent d'administration est installé sur un appareil exécutant Windows, il envoie au Serveur d'administration les informations suivantes sur le matériel de l'appareil :
    - Mémoire vive
    - Appareils de stockage de masse
    - Carte mère
    - Processeur
    - Adaptateurs réseau
    - Surveillance
    - Adaptateur vidéo
    - Carte son

    Si l'Agent d'administration est installé sur un appareil exécutant Linux ou macOS, il envoie au Serveur d'administration les informations suivantes sur le matériel de l'appareil, si ces informations sont fournies par le système d'exploitation :
    - Volume total de mémoire vive
    - Volume total des appareils de stockage de masse
    - Carte mère
    - Processeur
    - Adaptateurs réseau
  - Détails des vulnérabilités du logiciel tiers détectées sur les appareils administrés.
  - Détails des mises à jour disponibles pour les applications tierces installées sur les appareils administrés.
  - Détails des mises à jour Microsoft trouvées par la fonction WSUS.
  - Liste des mises à jour Microsoft trouvées par la fonctionnalité WSUS qui doivent être installées sur l'appareil.
- Données requises pour télécharger les mises à jour sur le Serveur d'administration isolé afin de corriger les vulnérabilités des logiciels tiers sur les appareils administrés. L'utilisateur saisit et transmet les données à l'aide de l'utilitaire klsclag du Serveur d'administration.
- Données nécessaires au fonctionnement de Kaspersky Security Center avec les environnements cloud (Amazon Web Services, Microsoft Azure, Google Cloud, Yandex Cloud). L'Utilisateur saisit des données dans la Console d'administration ou dans Kaspersky Security Center Web Console.

- Catégories définies par l'utilisateur pour les applications. L'utilisateur entre des données dans la Console d'administration ou dans l'interface de Kaspersky Security Center Web Console.

- Détails des fichiers exécutables détectés sur les appareils administrés par la fonctionnalité Contrôle des applications. L'utilisateur entre des données dans la Console d'administration ou dans l'interface de Kaspersky Security Center Web Console. Une liste complète des données est fournie dans les fichiers d'aide de l'application correspondante.

- Détails des fichiers placés dans la Sauvegarde. L'application administrée transfère les données de l'appareil vers le Serveur d'administration via l'Agent d'administration. Une liste complète des données est fournie dans les fichiers d'aide de l'application correspondante.

- Détails des fichiers placés en Quarantaine. L'application administrée transfère les données de l'appareil vers le Serveur d'administration via l'Agent d'administration. Une liste complète des données est fournie dans les fichiers d'aide de l'application correspondante.

- Détails des fichiers demandés par les spécialistes de Kaspersky pour une analyse détaillée. L'application administrée transfère les données de l'appareil vers le Serveur d'administration via l'Agent d'administration. Une liste complète des données est fournie dans les fichiers d'aide de l'application correspondante.

- Détails de l'état et du déclenchement des règles de Contrôle évolutif des anomalies. L'application administrée transfère les données de l'appareil vers le Serveur d'administration via l'Agent d'administration. Une liste complète des données est fournie dans les fichiers d'aide de l'application correspondante.

- Détails des appareils externes (unités de mémoire, outils de transfert d'informations, outils de copie papier des informations et bus de connexion) installés ou connectés à l'appareil administré et détectés par la fonctionnalité Contrôle des appareils. L'application administrée transfère les données de l'appareil vers le Serveur d'administration via l'Agent d'administration. Une liste complète des données est fournie dans les fichiers d'aide de l'application correspondante.

- Informations sur les appareils chiffrés et l'état de chiffrement. L'application administrée transfère les données de l'appareil vers le Serveur d'administration via l'Agent d'administration.

- Détails des erreurs de chiffrement des données sur les appareils effectuées à l'aide de la fonction de Chiffrement des données des applications Kaspersky. L'application administrée transfère les données de l'appareil vers le Serveur d'administration via l'Agent d'administration. Une liste complète des données est fournie dans les fichiers d'aide de l'application correspondante.

- Liste des contrôleurs logiques programmables (PLC) administrés. L'application administrée transfère les données de l'appareil vers le Serveur d'administration via l'Agent d'administration. Une liste complète des données est fournie dans les fichiers d'aide de l'application correspondante.

- Données nécessaires à la création d'une chaîne de développement des menaces. L'application administrée transfère les données de l'appareil vers le Serveur d'administration via l'Agent d'administration. Une liste complète des données est fournie dans les fichiers d'aide de l'application correspondante.

- Informations sur les tentatives d'accès aux services cloud par les employés d'une organisation. L'application administrée transfère les données de l'appareil vers le Serveur d'administration via l'Agent d'administration. Une liste complète des données est fournie dans les fichiers d'aide de l'application correspondante.

- Données requises pour l'intégration de Kaspersky Security Center avec le service Kaspersky Managed Detection and Response (le plug-in dédié doit être installé pour Kaspersky Security Center Web Console) : jeton de lancement d'intégration, jeton d'intégration et jeton de session utilisateur. L'Utilisateur saisit le jeton d'initiation d'intégration dans l'interface de Kaspersky Security Center Web Console : Le service Kaspersky MDR transfère le jeton d'intégration et le jeton de session utilisateur via le plug-in dédié.

- Détails des codes d'activation saisis ou des fichiers clés spécifiés. L'utilisateur entre des données dans la Console d'administration ou dans l'interface de Kaspersky Security Center Web Console.

- Comptes utilisateurs : nom, description, nom complet, adresse email, numéro de téléphone principal, mot de passe, clé secrète générée par le Serveur d'administration et mot de passe à usage unique pour la vérification en deux étapes. L'utilisateur entre des données dans la Console d'administration ou dans l'interface de Kaspersky Security Center Web Console.

- Données nécessaires à Identity and Access Manager pour l'authentification centralisée et pour fournir l'authentification unique (SSO) entre les applications Kaspersky intégrées à Kaspersky Security Center : paramètres d'installation et de configuration d'Identity and Access Manager, session utilisateur d'Identity and Access Manager, jetons Identity and Access Manager, statuts des applications clientes et statuts des serveurs de ressources. L'utilisateur entre des données dans la Console d'administration ou dans l'interface de Kaspersky Security Center Web Console.

- Historique des révisions des objets d'administration. L'utilisateur entre des données dans la Console d'administration ou dans l'interface de Kaspersky Security Center Web Console.

- Adresse IP de l'appareil sur lequel l'utilisateur a créé une révision. L'adresse IP est définie automatiquement par le Serveur d'administration.

- Registre des objets de gestion supprimés. L'utilisateur entre des données dans la Console d'administration ou dans l'interface de Kaspersky Security Center Web Console.

- Paquets d'installation créés à partir du fichier, ainsi que les paramètres d'installation. L'utilisateur entre des données dans la Console d'administration ou dans l'interface de Kaspersky Security Center Web Console.

- Données requises pour l'affichage des annonces de Kaspersky dans Kaspersky Security Center Web Console. L'Utilisateur saisit les données dans l'interface de Kaspersky Security Center Web Console.

- Les données requises pour assurer le fonctionnement des plug-ins des applications administrées dans Kaspersky Security Center Web Console et enregistrées par les plug-ins dans la base de données du Serveur d'administration pendant leur fonctionnement habituel. La description et les moyens de fournir les données sont fournis dans les fichiers d'aide de l'application correspondante.

- Paramètres utilisateur de Kaspersky Security Center Web Console : langue de localisation et thème de l'interface, paramètres d'affichage du panneau de surveillance, informations sur l'état des notifications (lue/non lue), état des colonnes dans les feuilles de calcul (Afficher/Masquer), mode Progression de la formation. L'Utilisateur saisit les données dans l'interface de Kaspersky Security Center Web Console.

- Journal des événements Kaspersky pour les modules Kaspersky Security Center et les applications administrées Kaspersky. Le journal des événements Kaspersky est stocké sur chaque appareil et n'est jamais transféré vers le Serveur d'administration.

- Certificats pour la connexion sécurisée des appareils administrés avec les modules de Kaspersky Security Center. L'utilisateur saisit les données à l'aide de l'utilitaire klsetsrvcert du Serveur d'administration.

- Certificats permettant d'établir la confiance dans les ressources Internet internes de l'organisation. L'Utilisateur saisit les données dans l'interface de Kaspersky Security Center Web Console.

- Données requises pour le fonctionnement de Kaspersky Security Center dans des environnements cloud, tels qu'Amazon Web Services (AWS), Microsoft Azure, Google Cloud et Yandex.Cloud. Le Serveur d'administration reçoit les données de la machine virtuelle sur laquelle il s'exécute.

- Informations sur l'acceptation par l'Utilisateur des termes et conditions des accords légaux avec Kaspersky.

- Les données du Serveur d'administration que l'Utilisateur saisit dans les modules suivants :
  - Console d'administration
  - Kaspersky Security Center Web Console
  - Terminal de ligne de commande lors de l'utilisation de l'utilitaire klsclag
  - Modules interagissant avec le Serveur d'administration via les objets d'automatisation klakaut et Kaspersky Security Center OpenAPI
- Toutes les données saisies par l'utilisateur dans la Console d'administration ou l'interface de Kaspersky Security Center Web Console.

Les données répertoriées ci-dessus peuvent être présentes dans Kaspersky Security Center si l'une des méthodes suivantes est appliquée :

- L'Utilisateur saisit des données dans l'interface des modules suivants :
  - Console d'administration
  - Kaspersky Security Center Web Console
  - Terminal de ligne de commande lors de l'utilisation de l'utilitaire klsclag
  - Modules interagissant avec le Serveur d'administration via les objets d'automatisation klakaut et Kaspersky Security Center OpenAPI
- L'Agent d'administration reçoit automatiquement les données de l'appareil et les transfère au Serveur d'administration.
- L'Agent d'administration reçoit les données récupérées par l'application administrée Kaspersky et les transfère au Serveur d'administration. Les listes de données traitées par les applications administrées par Kaspersky sont fournies dans les fichiers d'aide des applications correspondantes.
- Le Serveur d'administration obtient indépendamment les informations sur les appareils en réseau ou de l'Agent d'administration agissant comme point de distribution.
- Les données sont transférées de l'appareil mobile vers le Serveur d'administration à l'aide du protocole MDM iOS.

Les données répertoriées sont stockées dans la base de données du Serveur d'administration. Les noms d'utilisateur et les mots de passe sont chiffrés.

Toutes les données répertoriées plus haut peuvent être transférées à Kaspersky uniquement via des fichiers de vidage, des fichiers de traçage ou des fichiers journaux des modules de Kaspersky Security Center, y compris les fichiers journaux créés par les programmes d'installation et les utilitaires.

Les fichiers dump, les fichiers de traçage et les fichiers journaux des modules de Kaspersky Security Center contiennent des données aléatoires du Serveur d'administration, de l'Agent d'administration, de la Console d'administration, du serveur MDM iOS et de Kaspersky Security Center Web Console. Ces fichiers peuvent contenir des données personnelles et sensibles. Les fichiers dump, les fichiers de traçage et les fichiers journaux sont stockés sur l'appareil sous une forme non chiffrée. Les fichiers dump, les fichiers de traçage et les fichiers journaux ne sont pas transmis automatiquement à Kaspersky. Toutefois, l'administrateur peut transférer les données à Kaspersky manuellement sur demande du Support Technique en vue de résoudre des problèmes de fonctionnement de Kaspersky Security Center.

En suivant les liens de la Console d'administration ou de Kaspersky Security Center 14 Web Console, l'utilisateur accepte le transfert automatique des données suivantes :

- Code de Kaspersky Security Center
- Version de Kaspersky Security Center
- Localisation de Kaspersky Security Center
- ID de licence
- Type de licence
- Si la licence a été achetée via un partenaire

La liste des données fournies via chaque lien dépend de la finalité et de l'emplacement du lien.

Kaspersky utilise toutes les informations reçues sous forme anonyme et uniquement à des fins statistiques. Les statistiques récapitulatives sont générées automatiquement à partir des informations reçues à l'origine et ne contiennent aucune donnée personnelle ou confidentielle. Dès que de nouvelles données sont accumulées, les données précédentes sont effacées (une fois par an). Les statistiques récapitulatives sont stockées pour une durée indéterminée.

Kaspersky protège les informations obtenues conformément à la législation et aux règles de Kaspersky. Les données sont transmises par un canal sécurisé.

Options de licence de Kaspersky Security Center

Kaspersky Security Center peut fonctionner dans les modes suivants :

- **Sans licence (fonctionnalité de base)**

  Kaspersky Security Center fonctionne dans ce mode avant l'activation de l'application ou après l'expiration de la licence commerciale. Kaspersky Security Center avec la prise en charge de la fonctionnalité de base de la Console d'administration est livré parmi les applications de Kaspersky conçues pour la protection des réseaux de l'entreprise. Il peut également être téléchargé depuis le site Internet de Kaspersky.

- **Licence commerciale**

  Si vous avez besoin de fonctionnalités supplémentaires qui ne sont pas comprises dans les fonctionnalités de base de la Console d'administration, vous devez acheter une licence commerciale.

  Lors de l'ajout d'une clé de licence dans la fenêtre des propriétés du Serveur d'administration, assurez-vous d'ajouter une clé de licence qui vous permet d'utiliser Kaspersky Security Center. Vous pouvez trouver ces informations sur le site Internet de Kaspersky. Chaque page Internet de solution contient la liste des applications incluses dans cette solution. Le Serveur d'administration peut accepter des clés de licence non prises en charge, par exemple une clé de licence pour Kaspersky Endpoint Security Cloud, mais ces clés de licence n'offrent pas de nouvelles fonctionnalités en plus des fonctionnalités de base de la Console d'administration.

Fonctionnalité ou propriété	Mode de fonctionnement de Kaspersky Security Center	
	Pas de licence	Licence commerciale
Fonctionnalité de base de la Console d'administration Les fonctions suivantes sont disponibles : • Création des Serveurs d'administration virtuels pour administrer le réseau des offices à distance et des entreprises clientes. • Formation d'une hiérarchie des groupes d'administration pour administrer l'ensemble d'appareils comme un tout unique. • Installation à distance des applications. • Configuration centralisée des paramètres des applications installées sur les appareils clients. • Contrôle d'état de sécurité antivirus de l'entreprise. • Administration des rôles des utilisateurs. • Réception des statistiques et des rapports sur le fonctionnement des applications, ainsi que la réception des notifications sur les événements critiques. • Travail centralisé avec les fichiers placés en quarantaine ou dans la sauvegarde, et avec les fichiers dont le traitement est différé. • Administration du processus de chiffrement et de protection des données. • Consultation et modification des groupes des applications sous licence existants. • Consultation et modification manuelle de la liste du matériel détecté suite au sondage du réseau. • Consultation de la liste des images des systèmes d'exploitation accessibles à l'installation à distance.	✓	✓
Gestion des vulnérabilités et des correctifs : fonctionnalité de base	✓	✓

Fonctionnalité ou propriété	Mode de fonctionnement de Kaspersky Security Center	
	Pas de licence	Licence commerciale
Les tâches suivantes ne requièrent pas de licence commerciale : • Tâche *Recherche de vulnérabilités et de mises à jour requises* Grâce à cette tâche, Kaspersky Security Center reçoit la liste des vulnérabilités détectées et des mises à jour requises pour les logiciels tiers installés sur les appareils administrés. • La tâche *Installation des mises à jour Windows Update* Cette tâche peut être utilisée uniquement pour installer les mises à jour Windows Update. Pour utiliser cette tâche, vous devez spécifier les mises à jour requises manuellement dans les paramètres de la tâche. • La tâche *Corriger les vulnérabilités* La tâche *Corriger les vulnérabilités* utilise les correctifs recommandés pour les logiciels Microsoft et les correctifs utilisateurs pour les logiciels tiers. Pour utiliser cette tâche, vous devez spécifier manuellement les correctifs utilisateur pour les vulnérabilités dans les paramètres de la tâche.		
Gestion des vulnérabilités et des correctifs : fonctionnalité avancée Les fonctions suivantes sont disponibles : • Installation à distance des mises à jour logicielles et correction des vulnérabilités automatiquement selon les règles que vous définissez. • Utilisation du Serveur d'administration comme serveur de mises à jour du serveur Windows (WSUS) pour fournir les mises à jour vers les services Windows Updates sur les appareils en mode centralisé et avec la fréquence définie.	–	✓

Fonctionnalité ou propriété	Mode de fonctionnement de Kaspersky Security Center	
	Pas de licence	Licence commerciale
Fonctionnalité d'administration des appareils mobiles de la Console d'administration basée sur MMC L'administration des appareils mobiles est conçue pour administrer les appareils mobiles MDM iOS et Android. Pour les appareils MDM iOS, les fonctions suivantes sont disponibles : • Ajout de nouveaux appareils administrés par Kaspersky Security Center. • Création et modification des profils de configuration, installation des profils de configuration sur les appareils mobiles. • Installation des applications sur les appareils mobiles via l'App Store® ou à l'aide de fichiers manifeste (.plist) ou de paquets d'installation mobiles (.ipa). • Exécution de commandes sur les appareils MDM iOS, y compris le verrouillage des appareils mobiles, la réinitialisation du mot de passe de l'appareil mobile et la suppression de toutes les données de l'appareil mobile. Pour les appareils Android, les fonctions suivantes sont disponibles : • Ajout de nouveaux appareils administrés par Kaspersky Security Center. • Administration de Kaspersky Endpoint Security for Android via une stratégie. • Exécution de commandes sur les appareils. L'appareil mobile est une unité d'administration de la fonctionnalité Administration des appareils mobiles. L'appareil mobile est considéré comme appareil administré quand il est connecté au Serveur des appareils mobiles.	–	✓ (Il faut ajouter une clé de licence dans les propriétés du Serveur d'administration.)
Protection des appareils mobiles dans Kaspersky Security Center Web Console Kaspersky Security Center Web Console met à votre disposition les fonctionnalités suivantes pour administrer les appareils mobiles Android et iOS : • Ajout de nouveaux appareils administrés par Kaspersky Security Center. • Gestion de Kaspersky Endpoint Security for Android et Kaspersky Security for iOS via des stratégies. • Envoi de commandes aux appareils mobiles via les protocoles appropriés et exécution des commandes.	–	✓ (Une clé de licence doit être ajoutée sur chaque appareil mobile.)

Fonctionnalité ou propriété	Mode de fonctionnement de Kaspersky Security Center	
	Pas de licence	Licence commerciale
Administration des systèmes Les fonctions suivantes sont disponibles : • Installation des systèmes d'exploitation et des applications. Kaspersky Security Center permet de créer les images des systèmes d'exploitation et de les déployer sur les appareils clients par le réseau, ainsi que d'exécuter l'installation à distance des applications de Kaspersky et d'autres éditeurs. Vous pouvez tirer les images du système d'exploitation des appareils et les transférer au Serveur d'administration. Finalement, les images des systèmes d'exploitation reçues sont conservées sur le Serveur d'administration dans le dossier partagé. L'image du système d'exploitation d'un appareil de référence est capturée, puis créée par une tâche de création du paquet d'installation. Vous pouvez utiliser les images reçues pour le déploiement sur les nouveaux appareils dans le réseau sur lesquels le système d'exploitation n'a pas encore été installé. Pour ce but, la technologie Preboot eXecution Environment (PXE) est utilisée. • Administration des groupes des applications sous licence. • Permission à distance de la connexion aux appareils clients via un module de Microsoft® Windows® nommé Remote Desktop Connection. • Connexion à distance aux appareils clients à l'aide du Partage du bureau Windows. • Connexion à distance via **Kaspersky Remote Desktop Session Viewer**.	–	✓

Fonctionnalité ou propriété	Mode de fonctionnement de Kaspersky Security Center	
	Pas de licence	Licence commerciale
Intégration avec des environnements Cloud Kaspersky Security Center ne fonctionne pas seulement avec des appareils sur site, mais il présente également des fonctionnalités spéciales pour travailler dans le Cloud, comme l'Assistant de configuration pour une utilisation dans le Cloud. Kaspersky Security Center fonctionne avec les machines virtuelles suivantes : • Instances Amazon EC2 • Machines virtuelles Microsoft Azure • Instances de machines virtuelles Google Cloud • Machines virtuelles Yandex.Cloud	–	✓
Exportation des événements dans les systèmes SIEM via le protocole Syslog Le protocole Syslog permet de transmettre n'importe quel événement survenu sur le Serveur d'administration de Kaspersky Security Center et dans les applications de Kaspersky installées sur les appareils administrés. Le protocole Syslog est un protocole standard d'enregistrement de messages. Vous pouvez l'utiliser pour exporter des événements vers n'importe quel système SIEM.	✓	✓

Particularités de l'octroi de la licence Kaspersky Security Center et des applications administrées

La licence du Serveur d'administration et les applications administrées possèdent les particularités suivantes :

- Vous pouvez ajouter une clé de licence ou un code d'activation valide à un Serveur d'administration pour activer la Gestion des vulnérabilités et des correctifs, l'Administration des appareils mobiles ou l'Intégration aux systèmes SIEM. Certaines fonctionnalités de Kaspersky Security Center ne sont accessibles qu'en fonction des fichiers de clés actifs ou des codes d'activation valides ajoutés au Serveur d'administration.
- Vous pouvez ajouter plusieurs codes d'activation et fichiers clés pour les applications administrées dans le stockage du Serveur d'administration.

Particularités de l'octroi de la licence de Kaspersky Security Center

Par exemple, si vous avez activé une des fonctions sous licence (par exemple, l'Administration des appareils mobiles), à l'aide d'un fichier clé, mais que vous souhaitez utiliser une fonction sous licence supplémentaire (par exemple, la Gestion des vulnérabilités et des correctifs), vous devez obtenir auprès de votre prestataire de services un fichier clé qui active les deux fonctionnalités, et activer le Serveur d'administration à l'aide de ce fichier clé.

Particularités de l'octroi de la licence des applications administrées

Pour l'obtention d'une licence des applications administrées, vous pouvez déployer automatiquement le code d'activation ou le fichier clé, ou utiliser un autre moyen qui vous convient. Les moyens suivants sont disponibles pour déployer le code d'activation ou le fichier clé :

- Déploiement automatique

  > Si vous utilisez différentes applications administrées et que vous devez absolument déployer un fichier clé ou un code d'activation spécifique sur les appareils, utilisez d'autres modes de déploiement du code d'activation ou du fichier clé.

  Kaspersky Security Center permet automatiquement de diffuser les clés de licence se trouvant sur les appareils. Par exemple, le stockage du Serveur d'administration contient trois clés de licence. Vous avez sélectionné la case à cocher **Distribuer automatiquement la clé de licence sur les appareils administrés** pour les trois clés de licence. Sur les appareils de l'entreprise, l'application de sécurité de Kaspersky, par exemple, Kaspersky Endpoint Security for Windows est installée. Un nouvel appareil a été détecté sur lequel il faut diffuser la clé de licence. L'application définit par exemple, que pour cet appareil, deux des clés de licence du stockage peuvent être appliquées à l'appareil : la clé de licence *Key_1* et la clé de licence *Key_2*. Une de ces clés de licence est déployée sur l'appareil. Une des clés de licence adaptées est diffusée, et dans ce cas, il n'est pas possible de savoir laquelle de ces deux clés sera diffusée sur l'appareil car le déploiement automatique des clés de licence ne prévoit pas l'intervention de l'administrateur.

  Lors du déploiement de la clé, les appareils sont recalculés pour cette clé de licence. Vous devez vous assurer que le nombre d'appareils sur lequel la clé de licence est diffusée ne dépasse pas la restriction de licence. Si le nombre d'appareils dépasse la restriction de licence, l'état *Critique* est attribué à tous les appareils non couverts par la licence.

- Ajout d'un fichier clé ou d'un code d'activation dans le paquet d'installation de l'application administrée

  En cas d'installation d'une application administrée à l'aide du paquet d'installation, vous pouvez indiquer le code d'activation ou le fichier clé dans ce paquet d'installation ou dans la stratégie de l'application. La clé de licence est diffusée sur les appareils administrés lors de la synchronisation ultérieure de l'appareil avec le Serveur d'administration.

- Déploiement au moyen de la tâche d'ajout de clé de licence pour une application administrée.

  En cas de l'utilisation de la tâche ajout de la clé de licence de l'application administrée, vous pouvez choisir la clé de licence qu'il faut diffuser sur les appareils, et sélectionner les appareils de la manière qui vous convient, par exemple, en sélectionnant un groupe d'administration ou une sélection d'appareils.

- Ajout d'un code d'activation ou d'un fichier clé manuellement sur les appareils

Applications Kaspersky. Déploiement centralisé

Cette section décrit les modes d'installation à distance des applications de Kaspersky et de leur suppression sur les appareils du réseau.

> Avant d'installer des applications sur des appareils clients, il faut s'assurer que la configuration matérielle et logicielle des appareils correspond à la configuration requise pour l'application.

L'Agent d'administration garantit la communication entre le Serveur d'administration et les appareils clients. C'est pourquoi il faut l'installer sur chaque appareil client qui va être connecté au système d'administration centralisée à distance. Sur l'appareil doté du Serveur d'administration, seule la version serveur de l'Agent d'administration peut être utilisée. Elle est incluse dans le Serveur d'administration et s'installe et est supprimée ensemble avec lui. Il n'est pas nécessaire d'installer l'Agent d'administration sur cet appareil.

L'installation de l'Agent d'administration s'effectue de la même façon que l'installation des applications, et peut être réalisée à distance aussi que localement. Lors du déploiement centralisé des applications de sécurité via la Console d'administration, vous pouvez installer l'Agent d'administration avec les applications de sécurité.

Les Agents d'administration peuvent différer selon les applications de Kaspersky, avec lesquelles ils doivent travailler. Dans certains cas uniquement l'installation locale de l'Agent d'administration est possible (cf. Manuel des applications appropriées). Vous devez seulement installer l'Agent d'administration sur l'appareil client, une fois.

L'administration des applications de Kaspersky via la Console d'administration est exécutée à l'aide des plug-ins d'administration. Par conséquent, pour recevoir l'accès à l'administration des applications via Kaspersky Security Center, le plug-in d'administration de ces applications doit être installé sur le poste de travail de l'administrateur.

Vous pouvez réaliser l'installation à distance des applications depuis le poste de travail de l'administrateur dans la fenêtre principale de Kaspersky Security Center.

Pour l'installation à distance du logiciel, il faut créer la tâche d'installation à distance.

La tâche formée d'installation à distance sera exécutée selon sa programmation. Vous pouvez interrompre la procédure d'installation, en arrêtant manuellement l'exécution de la tâche.

Si l'installation à distance de l'application renvoie une erreur, assurez-vous que les conditions requises pour la préparation de l'appareil sont remplies.

Vous pouvez suivre l'avancement de l'installation à distance des applications de Kaspersky dans le réseau à l'aide du rapport de déploiement.

Les informations détaillées sur l'administration des applications dénombrées via Kaspersky Security Center sont fournies dans les Manuels correspondants aux applications.

Remplacement d'application de sécurité d'éditeurs tiers

Pour installer des applications de sécurité de Kaspersky à l'aide des outils de Kaspersky Security Center, il faut peut-être supprimer tout logiciel tiers incompatible avec l'application à installer. Kaspersky Security Center offre plusieurs méthodes pour retirer des applications tiers.

Supprimez les applications incompatibles à l'aide du programme d'installation

Cette option est disponible uniquement dans la Console d'administration basée sur la console de gestion Microsoft.

La méthode qui consiste à supprimer les applications incompatibles convient à plusieurs types d'installation. Avant l'installation de l'application de sécurité, toutes les applications incompatibles sont supprimées automatiquement si, dans la fenêtre des propriétés du paquet d'installation de cette application de sécurité (section **Applications incompatibles**), l'option **Supprimer automatiquement les applications incompatibles** a été sélectionnée.

Suppression des applications incompatibles pour configurer l'installation à distance d'une application

Vous pouvez activer l'option **Supprimer automatiquement les applications incompatibles** lorsque vous configurez l'installation à distance d'une application de sécurité. Dans la Console d'administration basée sur la console de gestion Microsoft (MMC), cette option est disponible uniquement dans l'Assistant de l'installation à distance. Dans Kaspersky Security Center Web Console, cette option se trouve dans l'assistant de déploiement de la protection. Si cette option est activée, Kaspersky Security Center supprime les applications incompatibles avant d'installer une application de sécurité sur un appareil administré.

Instructions pour :

- Console d'administration : Suppression des applications incompatibles à l'aide de l'Assistant de l'installation à distance
- Kaspersky Security Center Web Console : Suppression des applications incompatibles avant l'installation

Suppression des applications incompatibles à l'aide d'une tâche distincte

Les applications incompatibles sont supprimées à l'aide de la tâche **Tâche de désinstallation à distance d'une application**. Il faut lancer la tâche sur les appareils avant la tâche d'installation de l'application de sécurité. Par exemple, dans la tâche d'installation, vous pouvez sélectionner **Après l'exécution d'une autre tâche** en tant que type de programmation lorsque l'autre tâche est **Tâche de désinstallation à distance d'une application**.

Ce mode de suppression est recommandé si le programme d'installation de l'application de sécurité ne parvient pas à supprimer une des applications incompatibles.

Instructions pratiques pour la Console d'administration : Création d'une tâche.

Installation des applications à l'aide de la tâche d'installation à distance

Kaspersky Security Center permet d'installer à distance des applications sur les appareils à l'aide des tâches d'installation à distance. Les tâches sont créées et attribuées à des appareils à l'aide d'un Assistant. Pour pouvoir attribuer une tâche plus vite et plus facilement, vous pouvez désigner les appareils (jusqu'à 1 000 appareils) dans la fenêtre de l'Assistant de la manière qui vous convient le plus :

- **Sélectionner les appareils détectés sur le réseau par le Serveur d'administration**. Dans ce cas la tâche est affectée à un ensemble d'appareils. L'ensemble d'appareils peut reprendre aussi bien des appareils de groupes d'administration que des appareils non définis.
- **Définir les adresses des appareils manuellement ou les importer à partir d'une liste**. Vous pouvez définir les noms NetBIOS, les noms DNS, les adresses IP, ainsi que les plages d'adresses IP auxquels il convient d'affecter la tâche.

- **Attribuer la tâche à une sélection d'appareils**. Dans ce cas, la tâche est affectée aux appareils qui appartiennent à une sélection préalable. Vous pouvez spécifier la sélection prédéfinie ou une sélection personnalisée que vous avez créée.

- **Attribuer la tâche à un groupe d'administration**. Dans ce cas, la tâche est affectée aux appareils qui appartiennent à un groupe d'administration déjà créé.

Pour éviter les problèmes pouvant survenir lors de l'installation de l'application sur un appareil client sans Agent d'administration installé, il faut procéder comme décrit dans le déploiement forcé via la tâche d'installation à distance de Kaspersky Security Center.

Installation de l'application sur les appareils sélectionnés

Pour installer l'application sur les appareils sélectionnés, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le dossier **Tâches**.

2. Exécutez le processus de création d'une tâche en cliquant sur le bouton **Créer une tâche**.

   Ceci permet de lancer l'Assistant de création d'une tâche. Suivez les instructions de l'assistant.

   Dans la fenêtre **Sélection du type de tâche** de l'Assistant de création d'une tâche, dans l'entrée **Serveur d'administration de Kaspersky Security Center** sélectionnez **Installation à distance d'une application** comme type de tâche.

   Suite au fonctionnement de l'Assistant de création d'une tâche, la tâche d'installation à distance de l'application pour l'ensemble sélectionné d'appareils sera créée. La tâche créée est affichée dans l'espace de travail du dossier **Tâches**.

3. Lancez la tâche à la main ou attendez son lancement conformément à la programmation que vous avez indiquée dans les paramètres de la tâche.

Suite à l'exécution de la tâche d'installation à distance, l'application sélectionnée sera installée sur les appareils sélectionnés.

Installation de l'application sur les appareils clients d'un groupe d'administration

Pour installer l'application sur les appareils clients d'un groupe d'administration, procédez comme suit :

1. Connectez-vous au Serveur d'administration sous l'administration duquel le groupe d'administration nécessaire se trouve.

2. Dans l'arborescence de la console, sélectionnez le groupe d'administration.

3. Dans l'espace de travail du groupe, sélectionnez l'onglet **Tâches**.

4. Exécutez le processus de création d'une tâche en cliquant sur le bouton **Créer une tâche**.

   Ceci permet de lancer l'Assistant de création d'une tâche. Suivez les instructions de l'assistant.

   Dans la fenêtre **Sélection du type de tâche** de l'Assistant de création d'une tâche, dans l'entrée **Serveur d'administration de Kaspersky Security Center** sélectionnez **Installation à distance d'une application** comme type de tâche.

   Suite au fonctionnement de l'Assistant de création d'une tâche, la tâche de groupe d'installation à distance de l'application sélectionnée sera créée. La tâche créée s'affiche dans l'espace de travail du groupe d'administration, sous l'onglet **Tâches**.

5. Lancez la tâche à la main ou attendez son lancement conformément à la programmation que vous avez indiquée dans les paramètres de la tâche.

Suite à l'exécution de la tâche d'installation à distance, l'application sélectionnée est installée sur les appareils client du groupe d'administration.

Installation de l'application à l'aide des stratégies de groupe Active Directory

Kaspersky Security Center permet d'installer les applications de Kaspersky sur les appareils administrés à l'aide des stratégies de groupe Active Directory.

> L'installation des applications à l'aide des stratégies de groupe Active Directory est possible uniquement lors de l'utilisation des paquets d'installation incluant l'Agent d'administration.

Pour installer l'application à l'aide des stratégies de groupe Active Directory, procédez comme suit :

1. Commencez à configurer l'installation de l'application à l'aide de l'Assistant de l'installation à distance.

2. Dans la fenêtre **Définition des paramètres de la tâche d'installation à distance** de l'Assistant de l'installation à distance, sélectionnez l'option **Assigner l'installation du paquet d'installation dans les stratégies de groupe d'Active Directory**.

3. Dans la fenêtre **Sélection des comptes utilisateurs pour accéder aux appareils** de l'Assistant de l'installation à distance, sélectionnez l'option **Compte utilisateur requis (&Agent d'administration non utilisé)**.

4. Ajoutez au compte les privilèges d'administrateur sur l'appareil où Kaspersky Security Center est installé ou au compte inclus dans le groupe de domaine Propriétaires créateurs de la stratégie du groupe.

5. Accordez les autorisations au compte sélectionné :

    a. Accédez à **Panneau de configuration** → **Outils d'administration** et ouvrez **Gestion des stratégies de groupe**.

    b. Cliquez sur le nœud avec le domaine requis.

    c. Cliquez sur la section **Délégation**.

    d. Choisissez l'option **Lier les objets de stratégie de groupe** dans la liste déroulante **Autorisation**.

    e. Cliquez sur **Ajouter**.

    f. Dans la fenêtre **Sélectionner un utilisateur, un ordinateur ou un groupe** qui s'ouvre, sélectionnez le compte requis.

    g. Cliquez sur **OK** pour fermer la fenêtre **Sélectionner un utilisateur, un ordinateur ou un groupe**.

    h. Dans la liste **Groupes et utilisateurs**, sélectionnez le compte que vous venez d'ajouter, puis cliquez sur **Avancé** → **Avancé**.

    i. Dans la liste des **entrées d'autorisation**, double-cliquez sur le compte que vous venez d'ajouter.

    j. Accordez les autorisations suivantes :

    - **Créer des objets du groupe**
    - **Supprimer des objets du groupe**
    - **Créer des objets conteneurs de stratégie de groupe**
    - **Supprimer des objets conteneurs de stratégie de groupe**

    k. Cliquez sur le bouton **OK** afin d'enregistrer les modifications.

6. Définissez d'autres paramètres en suivant les instructions de l'Assistant.

7. Lancez la tâche créée d'installation à distance ou attendez son lancement programmé.

Finalement, le mécanisme suivant de l'installation à distance sera lancé :

1. Après le lancement de la tâche dans chaque domaine comprenant les appareils clients de l'ensemble, les objets suivants seront créés :

    - L'objet de la stratégie de groupe (OSG) avec le nom **Kaspersky_AK{GUID}**.
    - Un groupe de sécurité qui correspond à l'objet de la stratégie de groupe. Ce groupe de sécurité contient les appareils clients sur lesquels la tâche se diffuse. Le contenu du groupe de sécurité détermine la zone d'action de l'objet de la stratégie du groupe.

2. Kaspersky Security Center installe les applications Kaspersky sélectionnées sur les appareils clients directement depuis le dossier KLSHARE, c'est-à-dire le dossier réseau partagé de l'application. Dans le dossier d'installation de Kaspersky Security Center, un sous-dossier auxiliaire sera créé contenant le fichier .msi de l'application à installer.

3. Lors de l'ajout de nouveaux appareils dans la zone d'action d'une tâche, ils seront ajoutés au groupe de protection après le lancement suivant d'une tâche. Si dans la programmation d'une tâche, l'option **Lancer les tâches non exécutées** est sélectionnée, les appareils seront immédiatement ajoutés au groupe de protection.

4. Lors de la suppression des appareils depuis la zone d'action d'une tâche, leur suppression depuis le groupe de sécurité se passera lors du prochain lancement d'une tâche.

5. Lorsqu'une tâche est supprimée à partir d'Active Directory, l'OSG, le lien vers cet OSG et le groupe de protection correspondant sont supprimés également.

Si vous voulez utiliser un autre schéma d'installation via Active Directory, vous pouvez manuellement configurer les paramètres d'installation. Cela peut être utile, par exemple, dans les cas suivants :

- Quand l'administrateur de protection antivirus ne possède pas les privilèges d'apporter les modifications de certains domaines dans Active Directory.

- Si le paquet d'installation doit être placé sur une ressource de réseau distincte.

- S'il est nécessaire de lier un OSG à des sous-divisions concrètes d'Active Directory.

Les options suivantes d'utilisation d'un autre schéma d'installation via Active Directory sont disponibles :

- Si l'installation doit être effectuée directement depuis le dossier partagé de Kaspersky Security Center, vous devez indiquer dans les propriétés de l'OSG le fichier d'extension msi, situé dans le sous-dossier exec du dossier du paquet d'installation de l'application concernée.

- Si le paquet d'installation doit être placé dans une autre ressource de réseau, il faut y copier tout le contenu du dossier exec, puisque, excepté le fichier avec extension msi, ce dossier contient les fichiers de configuration formés au moment de création du paquet d'installation. Pour que la clé de licence soit installée avec l'application, il faut aussi copier le fichier clé dans ce dossier.

Installation à distance des applications sur les appareils macOS

Pour installer des applications sur des appareils exécutant macOS à l'aide de la tâche de programme d'installation à distance, procédez comme suit :

1. Créez une archive constituée d'un paquet d'installation et d'un script d'installation .sh.

2. Dans l'assistant de création d'une tâche, désactivez l'option **Vérifier le type de système d'exploitation avant le téléchargement**.

Vous pouvez également utiliser la tâche **Exécuter des scripts à distance**. L'article suivant décrit la procédure à suivre pour configurer les fichiers pour cette tâche : Installation à distance d'applications sur les appareils à l'aide de la tâche Exécuter des scripts à distance.

Installation des applications sur les Serveurs d'administration secondaires

Pour installer l'application sur les Serveurs d'administration secondaires, procédez comme suit :

1. Connectez-vous au Serveur d'administration qui gère les Serveurs d'administration secondaires nécessaires.

2. Assurez-vous que le paquet d'installation correspondant à l'application à installer se trouve sur chaque Serveur d'administration secondaire sélectionné. Si le paquet d'installation manque sur un des Serveurs secondaires, diffusez-le à l'aide d'une tâche de diffusion du paquet d'installation.

3. Lancez la création de la tâche d'installation de l'application sur les Serveurs d'administration secondaires à l'aide d'un des moyens suivants :

   - Si vous voulez former la tâche pour les Serveurs secondaires du groupe d'administration sélectionné, lancez la création de la tâche de groupe d'installation à distance pour ce groupe.

   - Si vous voulez créer une tâche pour un ensemble de serveurs secondaires, lancez la création d'une tâche d'installation à distance pour un ensemble d'appareils.

   Finalement, l'Assistant de création de la tâche d'installation à distance démarre pour vous guider. Suivez les instructions de l'assistant.

   Dans la fenêtre **Sélection du type de tâche** de l'Assistant de création d'une tâche, dans l'entrée **Serveur d'administration de Kaspersky Security Center**, ouvrez le dossier **Avancé** et sélectionnez le type de tâche **Installation à distance de l'application sur les Serveurs d'administration secondaires**.

   Suite au fonctionnement de l'Assistant de création d'une tâche, la tâche d'installation à distance de l'application sélectionnée sur les Serveurs d'administration secondaire sera créée.

4. Lancez la tâche à la main ou attendez son lancement conformément à la programmation que vous avez indiquée dans les paramètres de la tâche.

Suite à l'exécution de la tâche d'installation à distance, l'application sélectionnée sera installée sur les Serveurs d'administration secondaires.

Installation des applications à l'aide de l'Assistant de l'installation à distance

Pour l'installation des applications Kaspersky, vous pouvez utiliser l'Assistant de l'installation à distance. L'Assistant de l'installation à distance permet de réaliser l'installation à distance des applications, en utilisant les paquets d'installation créés spécialement ou directement depuis la paquet de distribution.

Pour que la tâche d'installation à distance fonctionne correctement sur l'appareil client, sur lequel l'Agent d'administration n'est pas installé, il est nécessaire d'ouvrir les ports TCP 139 et 445, UDP 137 et 138. Ces ports sont ouverts par défaut pour tous les appareils inclus dans le domaine. En cas d'erreurs réseau, consultez la Base de connaissances de Kaspersky Security Center.

Pour installer l'application sur les appareils sélectionnés à l'aide de l'Assistant de l'installation à distance, procédez comme suit :

1. Dans l'arborescence de la console, localisez le dossier **Installation à distance** et sélectionnez le sous-dossier **Paquets d'installation**.

2. Dans l'espace de travail du dossier, sélectionnez le paquet d'installation du programme à installer.

3. Dans le menu contextuel du paquet d'installation, sélectionnez l'option **Installer une application**.

   L'assistant de l'installation à distance démarre.

4. La fenêtre **Sélectionner les appareils à installer** permet de composer une liste des appareils sur lesquels l'application sera installée :

   - **Installer sur un groupe d'appareils administrés**

     Si cette option a été sélectionnée, la tâche d'installation à distance de l'application sera créée pour le groupe des appareils.

   - **Sélectionner les appareils à installer**

     Si cette option a été sélectionnée, la tâche d'installation à distance de l'application sera créée pour l'ensemble d'appareils. L'ensemble d'appareils peut contenir les appareils administrés ainsi que les appareils non définis.

5. Dans la fenêtre **Définition des paramètres de la tâche d'installation à distance**, configurez les paramètres de l'installation à distance de l'application.

   Le groupe de paramètres **Forcer le téléchargement du paquet d'installation** permet de sélectionner le mode d'envoi des fichiers nécessaires pour l'installation de l'application sur les appareils clients :

   - **En utilisant l'Agent d'administration**

     Si l'option est activée, l'Agent d'administration installé sur les appareils clients fournit les paquets d'installation à ces derniers.

     Si cette option est désactivée, les paquets d'installation sont fournis à l'aide des outils du système d'exploitation des appareils client.

     Il est recommandé d'activer cette option si la tâche concerne des appareils sur lesquels un Agent d'administration est installé.

     Cette option est activée par défaut.

   - **En utilisant les ressources du système d'exploitation via le Serveur d'administration**

     Si cette option est activée, les fichiers sont transmis aux appareils clients à l'aide des outils du système d'exploitation des appareils clients via le Serveur d'administration. Cette option peut être activée si l'Agent d'administration n'est pas installé sur l'appareil client, mais que l'appareil client fait partie du même réseau que le Serveur d'administration.

     Cette option est activée par défaut.

   - **En utilisant les ressources du système d'exploitation via les points de distribution**

     Si l'option est activée, les paquets d'installation sont transmis sur les appareils clients via les outils du système d'exploitation par les points de distribution. Cette option peut être sélectionnée si au moins un point de distribution se trouve sur le réseau.

     Si l'option **À l'aide de l'Agent d'administration** est activée, les fichiers seront livrés via les outils du système d'exploitation uniquement dans le cas où il n'est pas possible d'utiliser les moyens de l'Agent d'administration.

     Par défaut, l'option est activée pour les tâches d'installation à distance créées sur le Serveur d'administration virtuel.

   - **Nombre de tentatives d'installation**

Si, lors de l'exécution de la tâche d'installation à distance, Kaspersky Security Center ne parvient pas à installer une application sur un appareil administré conformément au nombre d'exécutions du programme d'installation paramétré, Kaspersky Security Center arrête de distribuer le paquet d'installation à cet appareil administré et ne démarre plus le programme d'installation sur l'appareil.

L'option `Nombre de tentatives d'installation` vous permet d'enregistrer les ressources de l'appareil administré, mais également de réduire le trafic (désinstallation, exécution du fichier MSI et messages d'erreur).

Des tentatives de démarrage de tâches récurrentes peuvent indiquer un problème d'installation sur l'appareil. L'administrateur doit résoudre le problème conformément au nombre d'essais d'installation (par exemple, par allocation d'un espace disque suffisant, suppression des applications incompatibles ou modification des paramètres d'autres applications qui empêchent l'installation) et le redémarrage de la tâche (manuellement ou selon un planning).

Si l'installation n'est finalement pas réalisée, le problème est considéré comme insoluble et toutes les tâches supplémentaires à entreprendre sont déclarées coûteuses à cause de la consommation inutile de ressources et de bande passante.

Lorsque la tâche est créée, le compteur de tentatives est défini sur `0`. Chaque exécution du programme d'installation qui renvoie une erreur sur l'appareil incrémente la valeur du compteur.

Si le nombre de tentatives paramétré est dépassé et que l'appareil est prêt pour l'installation de l'application, vous pouvez augmenter la valeur du paramètre `Nombre de tentatives d'installation` et lancer la tâche d'installation de l'application. Sinon, vous pouvez aussi créer une nouvelle tâche d'installation à distance.

Définissez quoi faire avec les appareils clients administrés par un autre Serveur d'administration :

- **Installer sur tous les appareils**

  L'application est installée même sur les appareils administrés par d'autres Serveurs d'administration.

  Par défaut, cette option est sélectionnée. Vous n'avez pas à modifier ce paramètre si vous n'avez qu'un seul Serveur d'administration sur votre réseau.

- **Installer uniquement sur les appareils administrés via &ce Serveur d'administration**

  L'application est installée uniquement sur les appareils administrés par ce Serveur d'administration. Sélectionnez cette option si vous avez plus d'un Serveur d'administration dans votre réseau et que vous souhaitez évitez les conflits entre eux.

Configurez les paramètres avancés :

- **Ne pas réinstaller l'application si elle est déjà installée**

  Si l'option est activée, l'application sélectionnée n'est pas installé à nouveau, si l'appareil client en est déjà équipé.

  Si l'option est désactivée, l'application sera malgré tout installée.

  Cette option est activée par défaut.

- **Réparer l'installation du paquet d'installation dans les stratégies de groupe d'Active Directory**

Si l'option est activée, le paquet d'installation s'installera à l'aide des stratégies de groupes Active Directory.

L'option est disponible si le paquet d'installation de l'Agent d'administration est sélectionné.

Cette option est Inactif par défaut.

6. Dans la fenêtre **Sélection de la clé de licence**, sélectionnez la clé de licence et son mode de diffusion :

- **&Ne pas placer la clé de licence dans le paquet d'installation (recommandé)**

  La clé est diffusée automatiquement à tous les appareils avec lesquels elle est compatible :
  - Si la diffusion automatique est activée dans les propriétés de la clé.
  - si la tâche **Ajout de la clé** est créée.

- **&Placer la clé de licence dans le paquet d'installation**

  La clé est diffusée sur les appareils avec le paquet d'installation.

  Il n'est pas recommandé de distribuer la clé à l'aide de cette méthode, car les droits d'accès en lecture partagés sont activés sur le référentiel des paquets d'installation.

La fenêtre **Sélection d'une clé de licence** est affichée si le paquet d'installation n'inclut pas de clé de licence.

Si le paquet d'installation inclut une clé de licence, la fenêtre **Propriétés de la clé de licence** contenant les informations sur la clé s'affiche.

7. Dans la fenêtre **Configuration du redémarrage du système d'exploitation**, définissez s'il faut ou non redémarrer les appareils si un redémarrage du système d'exploitation est requis au cours de l'installation des applications sur ceux-ci :

- **Ne pas redémarrer l'appareil**

  Si cette option a été sélectionnée, l'appareil ne sera pas redémarré après l'installation de l'application de sécurité.

- **Redémarrer l'appareil**

  Si cette option a été sélectionnée, l'appareil sera redémarré après l'installation de l'application de sécurité.

- **Confirmer l'action auprès de l'utilisateur**

  Si cette option a été sélectionnée, une notification sur la nécessité de redémarrage de l'appareil s'affichera après l'installation de l'application de sécurité. Le lien **Modifier** permet de modifier le texte du message, ainsi que la période d'affichage du message et le temps d'exécution du redémarrage automatique.

  Cette option est sélectionnée par défaut.

- **Forcer la fermeture des applications dans les sessions bloquées**

  Si cette option est activée, les applications présentes sur un appareil verrouillé doivent être verrouillées avant le redémarrage.

  Cette option est Inactif par défaut.

8. La fenêtre **Sélection des comptes utilisateurs pour accéder aux appareils** permet d'ajouter les comptes utilisateurs qui seront utilisés pour l'exécution de la tâche d'installation à distance :

   - **Compte utilisateur &non requis (Agent d'administration installé)**

     Si cette option est sélectionnée, il n'est pas nécessaire d'indiquer le compte utilisateur au nom duquel l'installateur de l'application sera lancé. La tâche est lancée sous le même compte utilisateur que le compte du service du Serveur d'administration.

     Si l'agent d'administration n'est pas installé sur les appareils clients, l'option n'est pas disponible.

   - **Compte utilisateur requis (&Agent d'administration non utilisé)**

     Sélectionnez cette option si l'Agent d'administration n'est pas installé sur les appareils pour lesquels vous affectez la tâche d'installation à distance. Dans ce cas, vous pouvez spécifier un compte utilisateur ou un certificat SSH pour installer l'application.

     - **Compte utilisateur local**. Si cette option est sélectionnée, spécifiez le compte utilisateur sous lequel le programme d'installation de l'application sera exécuté. Cliquez sur le bouton **Ajouter**, sélectionnez **Compte utilisateur local**, puis indiquez les informations d'identification du compte utilisateur.

       Vous pouvez désigner plusieurs comptes utilisateurs si aucun d'entre eux ne possède les privilèges nécessaires sur tous les appareils auxquels vous affectez la tâche. Dans ce cas, tous les comptes ajoutés sont utilisés pour exécuter la tâche, dans un ordre consécutif, de haut en bas.

     - **Certificat SSH**. Si vous souhaitez installer l'application sur un appareil client basé sur Linux, vous pouvez indiquer un certificat SSH au lieu d'un compte utilisateur. Cliquez sur le bouton **Ajouter**, sélectionnez **Certificat SSH**, puis indiquez les clés privée et publique du certificat.

       Pour générer une clé privée, vous pouvez utiliser l'utilitaire ssh-keygen. Notez que Kaspersky Security Center prend en charge le format PEM des clés privées, mais que l'utilitaire ssh-keygen génère par défaut des clés SSH au format OPENSSH. Le format OPENSSH n'est pas pris en charge par Kaspersky Security Center. Pour créer une clé privée au format PEM pris en charge, ajoutez l'option -m PEM dans la commande ssh-keygen. Par exemple :

       ```
       ssh-keygen -m PEM -t rsa -b 4096 -C "<user email>"
       ```

9. Dans la fenêtre **Lancement de l'installation**, cliquez sur le bouton **Suivant** pour créer et lancer la tâche d'installation à distance sur les appareils choisis.

   Si, dans la fenêtre **Lancement de l'installation**, l'option **&Ne pas lancer la tâche immédiatement à la fin de l'Assistant de l'installation à distance** est sélectionnée, la tâche d'installation à distance ne démarre pas. Vous pouvez lancer cette tâche manuellement plus tard. Le nom de la tâche correspond à celui du paquet d'installation de l'application : **Installation <Installation package name>**.

Pour installer l'application sur les appareils du groupe d'administration à l'aide de l'Assistant de l'installation à distance :

1. Connectez-vous au Serveur d'administration sous l'administration duquel le groupe d'administration nécessaire se trouve.

2. Dans l'arborescence de la console, sélectionnez le groupe d'administration.

3. Dans l'espace de travail du groupe, cliquez sur le bouton **Exécuter l'action**, et, dans la liste déroulante, sélectionnez **Installer une application**.

   Finalement, l'Assistant de l'installation à distance démarre. Suivez les instructions de l'assistant.

4. A la dernière étape de l'Assistant, cliquez sur le bouton **Suivant** pour créer et lancer la tâche d'installation à distance sur les appareils choisis.

Quand l'assistant de l'installation à distance a terminé, Kaspersky Security Center effectue les actions suivantes :

- Crée le paquet d'installation pour installer l'application (s'il n'a pas été créé auparavant). Le paquet d'installation est situé dans le dossier **Installation à distance**, dans le sous-dossier **Paquets d'installation**, sous un nom mentionnant le nom et la version de l'application. Vous pouvez utiliser ce paquet d'installation pour installer l'application ultérieurement.

- Crée et lance la tâche d'installation à distance pour un ensemble d'appareils ou pour un groupe d'administration. La tâche d'installation à distance créée se place dans le dossier **Tâches** ou s'ajoute aux tâches du groupe d'administration pour lequel elle a été créée. Vous pouvez lancer cette tâche manuellement plus tard. Le nom de la tâche correspond à celui du paquet d'installation de l'application : **Installation <Installation package name>**.

Utilisation des plug-ins d'administration

L'administration des applications de Kaspersky via la Console d'administration est exécutée à l'aide des plug-ins d'administration. Chaque application de Kaspersky qui peut être administrée via Kaspersky Security Center possède un plug-in d'administration. À l'aide du plug-in d'administration des applications, il est possible d'exécuter les actions suivantes dans la Console d'administration :

- Créer et modifier les stratégies et les paramètres de l'application, ainsi que les paramètres des tâches de cette application.

- Obtenir les informations sur les tâches de l'application, sur les événements dans son fonctionnement, et sur les statistiques de fonctionnement de l'application obtenues depuis les appareils clients.

Pour consulter la liste des plug-ins installés et ses versions, procédez comme suit :

1. Dans l'arborescence de la Console d'administration, cliquez-droit sur le **Serveur d'administration <nom_du_serveur>**, puis sélectionnez l'option **Propriétés**.

2. Cliquez sur **Avancé → Informations sur les plug-ins d'administration des applications installés**.

La liste des plug-ins d'administration installés et de leurs versions s'affiche dans le volet droit.

Vous pouvez installer les plug-ins pour les applications administrées à l'aide de l'Assistant de démarrage rapide du Serveur d'administration lors de la configuration initiale de Kaspersky Security Center. Vous pouvez également installer les plug-ins d'administration manuellement.

Pour installer manuellement un plug-in d'administration, procédez comme suit :

1. Téléchargez le plug-in d'administration de l'application Kaspersky et la version requise (par exemple, Kaspersky Endpoint Security for Windows 12.6) depuis la page du Support Technique de Kaspersky.

2. Si la Console d'administration est lancée, fermez-la.

3. Décompressez le fichier du plug-in téléchargé et exécutez le fichier klcfginst.msi ou klcfginst.exe. Suivez les instructions de l'Assistant.

4. Une fois l'installation terminée, lancez la Console d'administration et assurez-vous que le plug-in figure dans la liste des plug-ins installés, comme décrit dans la procédure précédente.

Lorsque vous exécutez la Console d'administration après l'installation d'un plug-in d'administration qui prend en charge l'Assistant de configuration initiale des applications administrées, cet Assistant se lance automatiquement. Vous pouvez suivre les étapes de l'Assistant de configuration initiale des applications administrées pour créer des stratégies et des tâches d'application par défaut de Kaspersky. Le lancement automatique de l'assistant est possible uniquement lorsque vous lancez la Console d'administration après l'installation initiale du plug-in ou après la mise à jour du plug-in d'administration vers une version compatible avec une autre version de l'application Kaspersky pour laquelle les tâches et les stratégies ne sont pas encore créées. Vous pouvez également lancer manuellement l'Assistant de configuration initiale des applications administrées.

Pour lancer manuellement l'Assistant de configuration initiale des applications administrées, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez l'entrée **Serveur d'administration**.

2. Dans le menu contextuel du nœud Serveur d'administration, sélectionnez l'option **Toutes les tâches → Assistant de configuration initiale des applications administrées**.

3. L'Assistant de configuration initiale des applications administrées s'ouvre. Suivez les étapes de l'Assistant pour créer les stratégies et les tâches d'application Kaspersky par défaut.

Pour supprimer un plug-in d'administration, procédez comme suit :

1. Si la Console d'administration est lancée, fermez-la.

2. Ouvrez l'Éditeur du registre Windows.

3. Trouvez la clé suivante :

   - `HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\28\Plugins` pour système 32 bits.

   - `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\28\Plugins` pour système 64 bits.

   La clé contient les plug-ins d'administration installés. Pour chaque plug-in, la valeur `DisplayName` contient le nom du plug-in et la valeur `UninstallString` la commande de désinstallation du plug-in.

4. Trouvez la clé du plug-in que vous souhaitez désinstaller et copiez sa valeur `UninstallString` dans le presse-papiers.

5. Collez la valeur dans la chaîne de commande et exécutez-la avec les droits d'administrateur système.

La version du plug-in d'administration ne doit pas être antérieure à la version de l'application administrée de Kaspersky. Si vous mettez à jour l'application Kaspersky sur les appareils, vous devez installer le plug-in d'administration de la même version.

À l'ouverture d'une stratégie créée dans une version antérieure du plug-in, il vous est demandé d'accepter la Déclaration de Kaspersky Security Network.

Lorsque vous désinstallez Kaspersky Security Center Web Console, tous les plug-ins d'administration sont également désinstallés.

Si vous ouvrez et enregistrez la stratégie dans la version du plug-in ultérieure à la version de l'application administrée, la stratégie sera mise à jour et vous ne pourrez pas l'ouvrir dans le plug-in de la version antérieure.

Consultation du rapport sur le déploiement de la protection

Pour suivre le processus de déploiement de la protection dans le réseau, il est possible d'utiliser le rapport sur le déploiement de la protection.

Pour consulter le rapport sur le déploiement de la protection, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez l'entrée portant le nom du Serveur d'administration requis.

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

3. Dans l'espace de travail du dossier **Rapports**, sélectionnez le modèle de rapport **Rapport sur le déploiement de la protection**.

Le rapport sera créé dans l'espace de travail. Ce rapport contient les informations relatives au déploiement de la protection sur tous les appareils du réseau.

Vous pouvez former un nouveau rapport sur le déploiement de la protection et indiquer quel type d'information il faut y inclure :

- Pour un groupe d'administration.

- Pour un ensemble d'appareils.

- Pour une sélection d'appareils.
- Pour tous les appareils.

Dans le cadre de Kaspersky Security Center, on considère que la protection est déployée sur l'appareil quand une application de sécurité y est installée et que la protection en temps réel fonctionne.

Désinstallation à distance des applications

Kaspersky Security Center permet de supprimer à distance des applications sur les appareils à l'aide de tâches de désinstallation à distance. Les tâches sont créées et attribuées à des appareils à l'aide d'un Assistant. Pour pouvoir attribuer une tâche plus vite et plus facilement aux appareils, vous pouvez désigner les appareils dans la fenêtre de l'Assistant de la manière qui vous convient le plus :

- **Sélectionner les appareils détectés sur le réseau par le Serveur d'administration**. Dans ce cas la tâche est affectée à un ensemble d'appareils. L'ensemble d'appareils peut reprendre aussi bien des appareils de groupes d'administration que des appareils non définis.
- **Définir les adresses des appareils manuellement ou les importer à partir d'une liste**. Vous pouvez définir les noms NetBIOS, les noms DNS, les adresses IP, ainsi que les plages d'adresses IP auxquels il convient d'affecter la tâche.
- **Attribuer la tâche à une sélection d'appareils**. Dans ce cas, la tâche est affectée aux appareils qui appartiennent à une sélection préalable. Vous pouvez spécifier la sélection prédéfinie ou une sélection personnalisée que vous avez créée.
- **Attribuer la tâche à un groupe d'administration**. Dans ce cas, la tâche est affectée aux appareils qui appartiennent à un groupe d'administration déjà créé.

Problèmes de suppression à distance

Lors de la suppression à distance d'applications tierces, les administrateurs peuvent tomber sur un avertissement indiquant : « Désinstallation à distance terminée sur l'appareil avec avertissement : l'application à supprimer n'est pas installée. » Ce problème survient généralement lorsque l'application à supprimer est installée uniquement pour l'utilisateur individuel actuellement connecté. Si l'utilisateur n'est pas connecté, une telle application devient invisible et ne peut pas être supprimée à distance.

Ce comportement diffère des applications destinées à être utilisées par plusieurs utilisateurs sur le même appareil, où les applications sont globalement visibles et accessibles par tous les utilisateurs de l'appareil.

Dans Kaspersky Security Center, l'algorithme du registre des applications traite différemment les applications destinées à des utilisateurs individuels et celles destinées à plusieurs utilisateurs :

- Les applications de plusieurs utilisateurs sont conservées dans une liste actualisée en temps réel des applications installées.
- Les applications destinées à des utilisateurs individuels sont contrôlées à l'aide d'un mécanisme de mise en cache.

  Si un utilisateur était connecté au moment de la détection de l'application, Kaspersky Security Center met en cache les informations sur les applications de cet utilisateur. Même si l'utilisateur se déconnecte par la suite, Kaspersky Security Center continue d'afficher ces applications comme étant installées en fonction des données mises en cache, bien que celles-ci ne soient plus visibles ou accessibles sur l'appareil.

Cette divergence peut entraîner des situations où Kaspersky Security Center identifie une application comme étant installée en fonction des données mises en cache, mais où la tâche de suppression de l'application échoue parce que l'application n'est pas accessible lorsque l'utilisateur est déconnecté.

Par défaut, la durée de vie des données d'application mises en cache est fixée à 30 jours. Les administrateurs peuvent modifier ce paramètre pour réduire la durée du cache, ce qui permet de minimiser les écarts entre les données affichées et la visibilité réelle de l'application sur les appareils.

Pour ajuster la durée de vie du cache à 1 heure (3 600 secondes), exécutez la commande suivante sur le Serveur d'administration :

```
klscflag -fset -pv klserver -n KLNAG_INV_PERUSER_APPS_CACHE_NONACTIVE_SIDS_LIFETIME_SEC
-t d -v 3600
```

Après avoir exécuté cette commande, redémarrez le Serveur d'administration pour que les modifications prennent effet.

Source d'informations sur les applications installées

L'Agent d'administration récupère des informations sur les logiciels installés sur les appareils Windows à partir des clés de registre suivantes :

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall

  Contient des informations sur les applications installées pour tous les utilisateurs.
- HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall

  Contient des informations sur les applications installées pour tous les utilisateurs.
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall

  Contient des informations sur les applications installées pour l'utilisateur actuel.
- HKEY_USER<...>\Software\Microsoft\Windows\CurrentVersion\Uninstall

  Contient des informations sur les applications installées pour des utilisateurs particuliers.

Désinstallation à distance d'une application sur les appareils clients du groupe d'administration

Pour désinstaller à distance l'application sur les appareils clients d'un groupe d'administration, procédez comme suit :

1. Connectez-vous au Serveur d'administration sous l'administration duquel le groupe d'administration nécessaire se trouve.
2. Dans l'arborescence de la console, sélectionnez le groupe d'administration.
3. Dans l'espace de travail du groupe, sélectionnez l'onglet **Tâches**.
4. Exécutez le processus de création d'une tâche en cliquant sur le bouton **Nouvelle tâche**.

   Ceci permet de lancer l'Assistant de création d'une tâche. Suivez les instructions de l'assistant.

   Dans la fenêtre **Sélection du type de tâche** de l'Assistant de création d'une tâche, dans l'entrée **Serveur d'administration de Kaspersky Security Center**, dans le dossier **Avancé** sélectionnez le type de tâche **Tâche de désinstallation à distance d'une application**.

   Suite au fonctionnement de l'Assistant de création d'une tâche, la tâche de groupe de désinstallation à distance de l'application sélectionnée sera créée. La tâche créée s'affiche dans l'espace de travail du groupe d'administration, sous l'onglet **Tâches**.
5. Lancez la tâche à la main ou attendez son lancement conformément à la programmation que vous avez indiquée dans les paramètres de la tâche.

Suite à l'exécution de la tâche de désinstallation à distance, l'application sélectionnée est supprimée des appareils clients du groupe d'administration.

Désinstallation à distance de l'application des appareils sélectionnés

Pour désinstaller à distance l'application des appareils sélectionnés, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le dossier **Tâches**.
2. Exécutez la création de tâche en cliquant sur **Nouvelle tâche**.

   Ceci permet de lancer l'Assistant de création d'une tâche. Suivez les instructions de l'assistant.

   Dans la fenêtre **Sélection du type de tâche** de l'Assistant de création d'une tâche, dans l'entrée **Serveur d'administration de Kaspersky Security Center**, dans le dossier **Avancé** sélectionnez le type de tâche **Tâche de désinstallation à distance d'une application**.

   Suite au fonctionnement de l'Assistant de création d'une tâche, la tâche de désinstallation à distance de l'application pour l'ensemble d'appareils sélectionné sera créée. La tâche créée est affichée dans l'espace de travail du dossier **Tâches**.
3. Lancez la tâche à la main ou attendez son lancement conformément à la programmation que vous avez indiquée dans les paramètres de la tâche.

Suite à l'exécution de la tâche d'installation à distance, l'application sélectionnée sera supprimée des appareils sélectionnés.

Fonctionnement avec les paquets d'installation

Lors de la création de la tâche d'installation à distance, les paquets d'installation sont utilisés. Ces paquets contiennent un ensemble de paramètres nécessaires à l'installation de l'application.

Les paquets d'installation peuvent contenir le fichier clé. Il est déconseillé de placer les paquets d'installation qui contiennent le fichier clé en accès libre.

Vous pouvez utiliser le même paquet d'installation plusieurs fois.

Les paquets d'installation créés par le Serveur d'administration se placent dans l'arborescence de la console, dans le dossier **Installation à distance**, dans le sous-dossier **Paquets d'installation**. Sur le Serveur d'administration les paquets d'installation sont sauvegardés dans le dossier partagé spécifié, dans le sous-dossier de service Packages.

Le cas échéant, vous pouvez supprimer un paquet d'installation du sous-dossier **Paquets d'installation** en suivant les instructions de l'article Suppression d'un objet.

Ne modifiez pas manuellement le contenu des paquets d'installation dans un dossier partagé. Au besoin, vous pouvez créer une copie du paquet d'installation, y apporter les modifications nécessaires et créer d'autres tâches d'installation.

Génération du paquet d'installation

Cet article décrit la procédure de création des types de paquets d'installation suivants :

- Paquet d'installation d'une application Kaspersky
- Paquet d'installation d'un fichier exécutable donné
- Paquet d'installation d'une application issue de la base de données Kaspersky

Il ne faut pas créer manuellement le paquet d'installation pour l'installation à distance de l'Agent d'administration. Il se crée de manière automatique lors de l'installation de l'application Kaspersky Security Center et se situe dans le dossier **Paquets d'installation**. Si le paquet pour l'installation à distance de l'Agent d'administration a été supprimé, il est possible de le recréer en sélectionnant le fichier nagent.kud, situé dans le dossier NetAgent du paquet de distribution de Kaspersky Security Center.

Afin de créer un paquet d'installation, procédez comme suit :

1. Connectez-vous au Serveur d'administration nécessaire.
2. Dans l'arborescence de la console, sélectionnez **Avancé** → **Installation à distance** → **Paquets d'installation**.

3. Lancez le processus de création d'un nouveau paquet d'installation par un des moyens suivants :

   - Cliquez avec le bouton droit de la souris sur le dossier **Paquets d'installation**, puis sélectionnez **Nouveau → &Paquet d'installation** dans le menu contextuel.
   - Dans la zone vide de la liste des paquets d'installation, cliquez avec le bouton droit de la souris, puis sélectionnez **Créer → &Paquet d'installation** dans le menu contextuel.
   - Cliquez sur **Créer un paquet d'installation** dans la section d'administration de la liste des paquets d'installation.

   L'Assistant de création du paquet d'installation se lance.

4. Sélectionnez un des types de paquets d'installation suivants en cliquant sur l'icône correspondante :

   - Paquet d'installation d'une application Kaspersky.
   - Paquet d'installation d'un fichier exécutable donné.
   - Paquet d'installation d'une application issue de la base de données Kaspersky.

5. Indiquez le nom du paquet d'installation à créer.

   Vous pouvez indiquer n'importe quel nom.

6. Sélectionnez l'application ou le fichier exécutable pour lequel le paquet d'installation doit être créé d'une des façons suivantes :

   - Cliquez sur le bouton **Parcourir** et, dans la fenêtre standard **Ouvrir** de Windows, sélectionnez le paquet de distribution de l'application nécessaire situé sur les disques disponibles.

     Cette option s'applique si vous décidez de créer le paquet d'installation pour l'application Kaspersky ou pour un fichier exécutable en particulier.

   - Cliquez sur le bouton **Parcourir** et, dans la fenêtre **Sélection de l'application**, sélectionnez le paquet de distribution de l'application nécessaire.

     Cette option s'applique si vous décidez de créer le paquet d'installation de l'application à partir de la base de données de Kaspersky.

   Si vous créez un paquet d'installation pour le Serveur d'administration, sélectionnez le fichier sc.kud. Le fichier sc.kud se trouve dans le dossier racine du paquet de distribution de Kaspersky Security Center.

   N'indiquez pas dans les paramètres des paquets d'installation les données des comptes utilisateur privilégiés.

7. Passez en revue le Contrat de licence utilisateur final et la Politique de confidentialité.

   Lors de la création du paquet d'installation pour une application, il se peut que vous soyez invité à consulter et à accepter le Contrat de licence utilisateur final et la Politique de confidentialité de l'application en question.

   Lisez les deux documents. Si vous acceptez toutes les conditions du Contrat de licence et de la Politique de confidentialité, confirmez-le en cochant les cases appropriées.

   L'installation de l'application se poursuit sur votre appareil, et la création du paquet d'installation reprend.

   > Si vous créez un paquet d'installation pour l'application Kaspersky Endpoint Security for Mac, vous pouvez choisir la langue du Contrat de licence utilisateur final et de la Politique de confidentialité.

8. Si nécessaire, activez l'installation automatique des modules système.

   Si vous créez le paquet d'installation de l'application à partir de la base de données de Kaspersky, vous pouvez activer l'installation automatique des modules système nécessaires. L'Assistant de création du paquet d'installation affiche la liste de tous les modules système général possibles pour l'application sélectionnée. Par la suite, vous pouvez accéder à cette liste dans les propriétés du paquet d'installation.

   Si vous créez le paquet d'installation du correctif, la liste reprendra tous les modules système nécessaires au déploiement de ce correctif.

9. Cliquez sur le bouton **Terminer** pour terminer le processus de création du paquet.

Une fois que l'Assistant de création du paquet d'installation a terminé, le paquet d'installation créé est affiché dans l'espace de travail du dossier **Paquets d'installation** dans l'arborescence de la console.

Création de paquets d'installation autonomes

Vous et les autres utilisateurs d'appareils de votre organisation pouvez utiliser des paquets d'installation autonomes pour installer l'Agent d'administration sur des appareils manuellement.

Le paquet d'installation autonome est un fichier exécutable (installer.exe) qui peut être stocké sur un Serveur Web ou dans un dossier partagé, ou bien transmis à l'appareil client par n'importe quelle méthode. Vous pouvez également envoyer un lien vers le paquet d'installation autonome par e-mail. Sur l'appareil client, l'utilisateur peut exécuter en local le fichier reçu pour installer une application sans recourir à Kaspersky Security Center.

> Assurez-vous que le paquet d'installation autonome n'est pas disponible pour des personnes non autorisées.

Vous pouvez créer des paquets d'installation autonomes pour toutes les applications Kaspersky et pour les applications tierces pour Windows, macOS et Linux. Pour créer un paquet d'installation autonome pour une application tierce, vous devez d'abord créer un paquet d'installation personnalisé.

La source pour créer des paquets d'installation autonomes sont les paquets d'installation figurant dans la liste créée sur le Serveur d'administration.

Pour créer un paquet d'installation autonome :

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

   Une liste des paquets d'installation disponibles sur le Serveur d'administration s'affiche.

2. Dans la liste des paquets d'installation, sélectionnez un paquet d'installation pour lequel vous souhaitez créer un paquet autonome.

3. Dans le menu contextuel, sélectionnez **&Créer un paquet d'installation autonome**.

   Finalement, l'Assistant de création du paquet d'installation autonome se lance. Parcourez les étapes de l'Assistant à l'aide du bouton **Suivant**.

4. Sur la première page de l'Assistant, si vous avez sélectionné un paquet d'installation pour l'application Kaspersky et souhaitez installer l'Agent d'administration avec l'application sélectionnée, assurez-vous que l'option **&Installer l'Agent d'administration avec cette application** est activée.

   Cette option est activée par défaut. Nous recommandons d'activer cette option si vous n'êtes pas sûr que l'Agent d'administration est installé sur l'appareil. Si l'Agent d'administration est déjà installé sur l'appareil, après l'installation du paquet d'installation autonome avec l'Agent d'administration, l'Agent d'administration est mis à jour vers la version la plus récente.

   Si vous désactivez cette option, l'Agent d'administration n'est pas installé sur l'appareil et l'appareil n'est pas administré.

   Si un paquet d'installation autonome pour l'application sélectionnée existe déjà sur le Serveur d'administration, l'assistant vous en informe. Dans ce cas, vous devez sélectionner l'une des actions suivantes :

   - **Créer un paquet d'installation autonome**. Sélectionnez cette option, par exemple, si vous souhaitez créer un paquet d'installation autonome pour une nouvelle version d'application et que vous souhaitez également conserver un paquet d'installation autonome que vous avez créé pour une version d'application précédente. Le nouveau paquet d'installation autonome est placé dans un autre dossier.

   - **Utiliser le paquet d'installation autonome existant**. Sélectionnez cette option si vous souhaitez utiliser un paquet d'installation autonome existant. Le processus de création du paquet n'est pas démarré.

   - **Reconstruire le paquet d'installation autonome existant**. Sélectionnez cette option si vous souhaitez créer de nouveau un paquet d'installation autonome pour la même application. Le paquet d'installation autonome est placé dans le même dossier.

5. Sur la page suivante de l'Assistant, sélectionnez l'option **Déplacer les appareils non définis dans ce groupe** et indiquez un groupe d'administration vers lequel vous souhaitez déplacer l'appareil client après l'installation de l'Agent d'administration.

   Par défaut, l'appareil est déplacé vers le groupe **Appareils administrés**.

   Si vous ne souhaitez pas déplacer l'appareil client vers un groupe d'administration après l'installation de l'Agent d'administration, sélectionnez l'option **Ne pas déplacer les appareils**.

6. Sur la page suivante de l'Assistant, lorsque le processus de création du paquet d'installation autonome est terminé, le résultat de la création du paquet autonome et un chemin d'accès à ce dernier sont affichés.

   Vous pouvez cliquer sur les liens et effectuer l'une des opérations suivantes :

   - Ouvrez le dossier contenant le paquet d'installation autonome.

   - Lien email vers le paquet d'installation autonome créé. Pour effectuer cette opération, vous devez lancer une application de messagerie.

   - Exemple de code HTML pour la publication de liens sur un site Web. Un fichier TXT est créé et ouvert dans une application associée à un format TXT. Dans le fichier, une balise HTML <a> avec des attributs s'affiche.

7. Sur la page suivante de l'Assistant, si vous souhaitez ouvrir la liste des paquets d'installation autonomes, activez l'option **Ouvrir la liste des paquets autonomes**.

8. Cliquez sur le bouton **Terminer**.

   Le Assistant de création du paquet d'installation autonome se ferme.

Le paquet d'installation autonome est créé et placé dans le sous-dossier PkgInst du dossier partagé du Serveur d'administration. Vous pouvez afficher la liste des paquets autonomes en cliquant sur le bouton **Consulter la liste des paquets autonomes** situé au-dessus de la liste des paquets d'installation.

Génération des paquets d'installation personnalisés

Vous pouvez utiliser des paquets d'installation personnalisés pour effectuer les opérations suivantes :

- Pour installer n'importe quelle application (par exemple, un éditeur de texte) sur un appareil client, par exemple, au moyen d'une tâche.
- Pour créer un paquet d'installation autonome.

Un paquet d'installation personnalisé est un dossier avec un ensemble de fichiers. La source permettant de créer un paquet d'installation personnalisé est un *fichier archive*. Le fichier archive contient le ou les fichiers à inclure dans le paquet d'installation personnalisé. En créant un paquet d'installation personnalisé, vous pouvez spécifier des paramètres de ligne de commande pour installer l'application en mode silencieux par exemple.

Pour créer le paquet d'installation personnalisé :

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

   Une liste des paquets d'installation disponibles sur le Serveur d'administration s'affiche.

2. Au-dessus de la liste des paquets d'installation, cliquez sur le bouton **Créer un paquet d'installation**.

   L'Assistant de création du paquet d'installation se lance. Parcourez les étapes de l'Assistant à l'aide du bouton **Suivant**.

3. À la première page de l'Assistant, sélectionnez **Créer un paquet d'installation pour le fichier exécutable indiqué**.

4. Sur la page suivante de l'Assistant, spécifiez le nom du paquet d'installation personnalisé.

5. Sur la page suivante de l'Assistant, cliquez sur le bouton **Parcourir** et, dans une fenêtre standard **Ouvrir** de Windows, choisissez un fichier d'archive situé sur les disques disponibles pour créer un paquet d'installation personnalisé.

   Vous pouvez télécharger une archive ZIP, CAB, TAR ou TAR.GZ. Il est impossible de créer un paquet d'installation à partir d'un fichier SFX (archive auto-extractible).

   Les fichiers sont téléchargés sur le Serveur d'administration de Kaspersky Security Center.

6. Sur la page suivante de l'Assistant, spécifiez les paramètres de ligne de commande d'un fichier exécutable.

   Vous pouvez spécifier des paramètres de ligne de commande pour installer l'application à partir du paquet d'installation en mode silencieux par exemple. La spécification des paramètres de ligne de commande est facultative.

   Si vous le souhaitez, configurez les options suivantes :

   - **Copier tout le dossi&er dans le paquet d'installation**

     Sélectionnez cette option si le fichier exécutable est accompagné de fichiers supplémentaires requis pour l'installation de l'application. Avant d'activer cette option, assurez-vous que tous les fichiers requis sont stockés dans le même dossier. Si cette option est activée, l'application ajoute l'intégralité du contenu du dossier, y compris le fichier exécutable spécifié, au paquet d'installation.

   - **Convertissez les paramètres en valeurs recommandées pour les applications reconnues par Kaspersky Security Center**

     L'application sera installée avec les paramètres recommandés si la base de données de Kaspersky contient des informations sur l'application spécifiée.

     Si vous avez entré les paramètres dans le champ **Ligne de commande du fichier exécutable**, ils sont redéfinis avec les paramètres recommandés.

     Cette option est activée par défaut.

     La base de données de Kaspersky est créée et gérée par les analystes de Kaspersky. Les analystes de Kaspersky définissent les paramètres d'installation optimaux pour chaque application ajoutée à la base de données. Les paramètres sont définis pour garantir la réussite de l'installation à distance d'une application sur un appareil client. La base de données est automatiquement mise à jour sur le Serveur d'administration lorsque vous exécutez la tâche Télécharger les mises à jour sur le référentiel du Serveur d'administration.

   Le processus de création du paquet d'installation personnalisé se lance.

   L'Assistant vous informe lorsque le processus est terminé.

   Si la création du paquet d'installation personnalisé échoue, un message correspondant s'affiche.

7. Cliquez sur le bouton **Finish** pour fermer l'Assistant.

   Le paquet d'installation que vous avez créé est téléchargé dans le sous-dossier Paquets du dossier partagé du Serveur d'administration. Après le téléchargement, le paquet d'installation personnalisé apparaît dans la liste des paquets d'installation.

Dans la liste des paquets d'installation sur le Serveur d'administration, vous pouvez afficher et modifier les propriétés des paquets d'installation personnalisés.

Consultation et modification des propriétés des paquets d'installation personnalisés

Après avoir créé un paquet d'installation personnalisé, vous pouvez consulter des informations générales sur le paquet d'installation et spécifier les paramètres d'installation dans la fenêtre des propriétés.

Pour consulter et modifier les propriétés d'un paquet d'installation personnalisé :

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

   Une liste des paquets d'installation disponibles sur le Serveur d'administration s'affiche.

2. Dans le menu contextuel du paquet d'installation, sélectionnez l'option **Propriétés**.

   La fenêtre des propriétés du paquet d'installation sélectionné s'ouvre.

3. Consulter les informations suivantes :

   - Nom de l'archive d'installation
   - Nom de l'application intégrée au paquet d'installation personnalisé
   - Version de l'application
   - Date de création du paquet d'installation
   - Chemin d'accès au paquet d'installation personnalisé sur le Serveur d'administration
   - Ligne de commande du fichier exécutable

4. Définissez les paramètres suivants :

   - Nom de l'archive d'installation
   - **Installer les modules système général requis**

     Si cette option est activée, l'application, avant d'installer une mise à jour, installe automatiquement tous les composants généraux système (prérequis) requis pour l'installation de la mise à jour. Par exemple, il peut s'agir des mises à jour du système d'exploitation.

     Si cette option est désactivée, vous devrez peut-être installer les prérequis manuellement.

     Cette option est Inactif par défaut.

     Cette option est disponible uniquement lorsque l'application ajoutée au paquet d'installation est reconnue par Kaspersky Security Center.

   - **Ligne de commande du fichier exécutable**

     Si l'application nécessite des paramètres supplémentaires pour une installation en mode silencieux, spécifiez-les dans ce champ. Pour plus d'informations, voir la documentation du fournisseur.

     Vous pouvez aussi entrer d'autres paramètres.

     Cette option est disponible uniquement pour les paquets qui ne sont pas créés sur la base des applications Kaspersky.

5. Cliquez sur le bouton **OK** ou **Appliquer** pour enregistrer les modifications, le cas échéant.

Les nouveaux paramètres sont enregistrés.

Obtention du paquet d'installation de l'Agent d'administration à partir du kit de distribution de Kaspersky Security Center

Vous pouvez obtenir le paquet d'installation de l'Agent d'administration à partir du kit de distribution de Kaspersky Security Center, sans avoir à installer Kaspersky Security Center. Ensuite, vous pouvez utiliser le paquet d'installation pour installer l'Agent d'administration sur les appareils clients.

Pour obtenir le paquet d'installation de l'Agent d'administration à partir du kit de distribution de Kaspersky Security Center :

1. Exécutez le fichier exécutable ksc_<version number>.<build number>_full_<localization language>.exe à partir du kit de distribution de Kaspersky Security Center.
2. Dans la fenêtre qui s'ouvre, cliquez sur le lien **Extraire les paquets d'installation**.
3. Dans la liste des paquets d'installation, cochez la case à côté du paquet d'installation de l'Agent d'administration, puis cliquez sur le bouton **Suivant**.
4. Si nécessaire, cliquez sur le bouton **Parcourir** pour changer le dossier affiché dans lequel extraire le paquet d'installation.
5. Cliquez sur le bouton **Extraire**.

   L'application extrait le paquet d'installation de l'Agent d'administration.
6. Une fois le processus terminé, cliquez sur le bouton **Fermer**.

Le paquet d'installation de l'Agent d'administration est extrait dans le dossier sélectionné.

Vous pouvez utiliser le paquet d'installation pour installer l'Agent d'administration par l'une des méthodes suivantes :

- Localement en exécutant le fichier setup.exe à partir du dossier extrait
- Par installation silencieuse
- À l'aide des stratégies de groupe de Microsoft Windows

Propagation des paquets d'installation sur les Serveurs d'administration secondaires

Pour propager les paquets d'installation sur les Serveurs d'administration secondaires, procédez comme suit :

1. Connectez-vous au Serveur d'administration qui gère les Serveurs d'administration secondaires nécessaires.
2. Lancez la création de la tâche de propagation du paquet d'installation sur les Serveurs d'administration secondaires à l'aide d'un des moyens suivants :

   - Si vous voulez former la tâche pour les Serveurs secondaires du groupe d'administration sélectionné, lancez la création de la tâche de groupe pour ce groupe.
   - Si vous voulez créer une tâche pour un ensemble de Serveurs d'administration secondaires, lancez la création d'une tâche pour un ensemble d'appareils.

   Ceci permet de lancer l'assistant de création d'une tâche. Suivez les instructions de l'assistant.

   Dans la fenêtre **Sélection du type de tâche** de l'Assistant de création d'une tâche, sous l'entrée **Serveur d'administration de Kaspersky Security Center**, dans le dossier **Avancé** sélectionnez le type de tâche **Diffusion du paquet d'installation**.

   Suite au fonctionnement de l'Assistant de création d'une tâche, la tâche de propagation des paquets d'installation sélectionnés sur les Serveurs d'administration secondaire sera créée.
3. Lancez la tâche manuellement ou attendez son lancement conformément à la planification que vous avez indiquée dans les paramètres de la tâche.

Suite à l'exécution de la tâche, les paquets d'installation sélectionnés seront copiés sur les Serveurs d'administration secondaires.

Propagation des paquets d'installation à l'aide des points de distribution

Vous pouvez utiliser les points de distribution pour la propagation de paquets d'installation dans le cadre du groupe d'administration.

Une fois que les points de distribution ont reçu les paquets d'installation depuis le Serveur d'administration, ils les diffusent automatiquement aux appareils clients à l'aide d'une multidiffusion IP. La diffusion IP de nouveaux paquets d'installation dans le cadre du groupe d'administration est effectuée une fois. Si l'appareil client était déconnecté du réseau de la société au moment de la diffusion, l'Agent d'administration télécharge automatiquement le paquet d'installation requis depuis le point de distribution lors du lancement de la tâche d'installation.

Transfert dans Kaspersky Security Center des informations sur les résultats d'installation de l'application

Après la création du paquet d'installation de l'application, vous pouvez configurer le paquet d'installation de telle manière pour que les informations diagnostiques sur les résultats d'installation de l'application soient transmises dans Kaspersky Security Center. Pour les paquets d'installation des applications de Kaspersky, le transfert des informations diagnostiques sur les résultat d'installation de l'application est configuré par défaut et la configuration complémentaire n'est pas requise.

Pour configurer la transmission de l'information diagnostique dans Kaspersky Security Center sur le résultat d'installation de l'application, procédez comme suit :

1. Passez dans le dossier du paquet d'installation formé par les moyens de Kaspersky Security Center pour l'application sélectionnée. Ce dossier est situé dans le dossier partagé qui était indiqué lors de l'installation de Kaspersky Security Center.

2. Ouvrez le fichier avec l'extension kpd ou kud pour la rédaction (par exemple, à l'aide du traitement de texte Notepad Microsoft Windows).

   Le fichier a le format du fichier ini de configuration ordinaire.

3. Ajouter les lignes suivantes dans le fichier :

   ```
   [SetupProcessResult]
   Wait=1
   ```

   Cette commande configure l'application Kaspersky Security Center de telle manière, pour qu'elle attende la fin d'installation de l'application, pour laquelle le paquet d'installation est formé, et pour qu'elle analyse le code de retour du programme d'installation. S'il faut désactiver la transmission de l'information diagnostique, saisissez la valeur 0 pour la clé Wait.

4. Introduisez la description des codes de retour de l'installation réussite. Pour cela, ajoutez les lignes suivantes dans le fichier :

   ```
   [SetupProcessResult_SuccessCodes]
   <return code>=[<description>]
   <return code 1>=[<description>]
   ...
   ```

   Les valeurs facultatives figurent entre crochets.

   Syntaxe des lignes :

   - `<return code>`. N'importe quel nombre correspondant au code de retour du programme d'installation. Le nombre des codes de retour peut être aléatoire.
   - `<description>`. La description de texte du résultat d'installation. La description peut être absente.

5. Introduisez la description des codes de retour pour l'installation erronée. Pour cela, ajoutez les lignes suivantes dans le fichier :

   ```
   [SetupProcessResult_ErrorCodes]
   <return code>=[<description>]
   <return code 1>=[<description>]
   ...
   ```

   La syntaxe des lignes correspond à la syntaxe des codes de retour lors de l'installation réussite.

6. Fermer le fichier kpd ou .kud, en sauvegardant toutes les modifications accomplies.

L'information sur les résultats d'installation de l'application, indiquée par l'utilisateur, sera enregistrée dans les journaux de Kaspersky Security Center et sera affichée dans la liste des événements, dans les rapports et dans les résultats d'exécution des tâches.

Définition de l'adresse du Serveur proxy KSN pour les paquets d'installation

Si l'adresse ou le domaine du Serveur d'administration change, vous pouvez définir l'adresse du serveur Proxy KSN pour le paquet d'installation.

Pour définir l'adresse du serveur proxy KSN pour le paquet d'installation :

1. Dans l'arborescence de la console dans le dossier **Installation à distance** sélectionnez le sous-dossier **Paquets d'installation**.
2. Dans le menu qui s'ouvre, sélectionnez **Propriétés**.
3. Dans la fenêtre des propriétés qui s'ouvre, sélectionnez la sous-section **Général**.
4. Dans la sous-section **Général** de la fenêtre des propriétés, saisissez 'adresse du serveur proxy KSN.

Les paquets d'installation utiliseront cette adresse par défaut.

Récupération des version actuelles des applications

Kaspersky Security Center vous permet de recevoir les versions actuelles des applications corporatives exposées sur les serveurs de Kaspersky.

Pour recevoir des versions actuelles des applications corporatives de Kaspersky, procédez comme suit :

1. Exécutez une des actions suivantes :

   - Dans l'arborescence de la console, sélectionnez le nœud avec le nom du Serveur d'administration requis, assurez-vous que l'onglet **Surveillance** est sélectionné et dans la section **Déploiement** cliquez sur le lien **Des nouvelles versions des applications Kaspersky sont disponibles**.

     Le lien **Des nouvelles versions des applications Kaspersky sont disponibles** devient visible quand le Serveur d'administration détecte une nouvelle version de l'application corporative sur le serveur Kaspersky.

   - Dans l'arborescence de la console, sélectionnez **Avancé → Installation à distance → Paquets d'installation**, dans l'espace de travail, cliquez sur **Actions supplémentaires** et, dans la liste déroulante, sélectionnez **Consulter les versions actuelles des applications Kaspersky**.

   La liste de la version actuelle des applications Kaspersky s'affiche.

2. Vous pouvez filtrer la liste des applications Kaspersky pour simplifier la recherche de l'application requise.

   En haut de la fenêtre **Versions actuelles des applications**, cliquez sur le lien **Filtrer** pour filtrer la liste des applications selon les critères suivants :

   - **Modules**. Utilisez ce critère pour filtrer la liste des applications de Kaspersky en fonction des zones de protection utilisées sur votre réseau.
   - **Type de logiciels à télécharger**. Utilisez ce critère pour filtrer la liste des applications de Kaspersky selon le type d'application.
   - **Types de mises à jour et de logiciels à afficher**. Utilisez ce critère pour afficher les applications Kaspersky disponibles par version spécifique.
   - **Langues d'affichage des applications et des mises à jour**. Utilisez ce critère pour afficher les applications Kaspersky avec une langue de localisation spécifique.

   Cliquez sur le bouton **Appliquer** pour appliquer les filtres sélectionnés.

3. Sélectionnez dans la liste l'application nécessaire.

4. Téléchargez le paquet de distribution de l'application en cliquant sur le lien dans la chaîne **Adresse Internet du paquet de distribution**.

   Les mises à jour des applications administrées peuvent nécessiter l'installation d'une version minimale spécifique de Kaspersky Security Center. Si cette version est postérieure à votre version actuelle, ces mises à jour sont affichées mais ne peuvent pas être approuvées. De plus, aucun paquet d'installation ne peut être créé à partir de ces mises à jour tant que vous n'avez pas mis à niveau Kaspersky Security Center. Vous êtes invité à mettre à niveau votre instance de Kaspersky Security Center vers la version minimale requise.

Si pour l'application sélectionnée, le bouton **&Télécharger les applications et créer les paquets d'installation** s'affiche, vous pouvez cliquer sur ce bouton pour télécharger le paquet de distribution de l'application et pour créer automatiquement le paquet d'installation. Dans ce cas, Kaspersky Security Center télécharge le paquet de distribution de l'application sur le Serveur d'administration dans le dossier partagé indiqué lors de l'installation de Kaspersky Security Center. Le paquet d'installation, créé automatiquement s'affiche dans le dossier **Installation à distance** de l'arborescence de la console, dans le sous-dossier **Paquets d'installation**.

Une fois la fenêtre **Versions actuelles des applications** fermée, le lien **Des nouvelles versions des applications Kaspersky sont disponibles** disparaît de la section **Déploiement**.

Vous pouvez créer les paquets d'installation des nouvelles versions des applications et travailler avec les paquets d'installation créés dans le dossier **Installation à distance** de l'arborescence de la console, dans le sous-dossier **Paquets d'installation**.

Vous pouvez aussi ouvrir la fenêtre **Versions actuelles des applications** en cliquant sur le lien **Consulter les versions actuelles des applications Kaspersky** dans l'espace de travail du dossier **Paquets d'installation**.

Préparation de l'appareil Windows pour l'installation à distance

L'installation à distance d'une application sur un appareil client peut se terminer avec une erreur pour les raisons suivantes :

- La tâche a déjà été exécutée sur cet appareil.

  En ce cas, son exécution n'est pas requise de nouveau.

- L'appareil a été coupé pendant le lancement de la tâche.

  Dans ce cas il faut activer l'appareil, puis lancer à nouveau la tâche.

- Il n'y a pas de communication entre le Serveur d'administration et l'Agent d'administration installé sur l'appareil client.

  Pour identifier la cause du problème, vous pouvez utiliser l'utilitaire de diagnostic à distance de l'appareil (klactgui).

- Les problèmes suivants peuvent survenir lors de l'installation d'une application à distance si l'Agent d'administration n'est pas installé sur l'appareil :

  - **Désactiver le partage de fichiers simple** est activé sur l'appareil client.
  - Le service Server ne fonctionne pas sur l'appareil client.
  - Les ports nécessaires sont fermés sur l'appareil client.
  - Le compte utilisateur sous lequel la tâche est exécutée ne jouit pas assez de privilèges.

  Pour éviter les problèmes pouvant survenir lors de l'installation de l'application sur un appareil client sans Agent d'administration installé, il faut procéder comme décrit dans le déploiement forcé via la tâche d'installation à distance de Kaspersky Security Center.

Auparavant, l'utilitaire riprep était utilisé pour préparer un appareil en vue d'une installation à distance. Cette méthode de configuration des systèmes d'exploitation est aujourd'hui considérée comme obsolète. L'utilisation de l'utilitaire riprep n'est pas recommandée sur les systèmes d'exploitation plus récents que Windows XP et Windows Server 2003 R2.

Préparation d'un appareil Linux et installation de l'Agent d'administration sur un appareil Linux à distance

L'installation de l'Agent d'administration comprend deux étapes :

- Préparation de l'appareil Linux
- Installation à distance de l'Agent d'administration

Préparation de l'appareil Linux

Pour préparer l'appareil fonctionnant sous le système d'exploitation Linux à l'installation à distance de l'Agent d'administration, procédez comme suit :

1. Assurez-vous que l'appareil sur lequel vous voulez installer l'Agent d'administration pour Linux fonctionne sur une des distributions Linux supportées.

2. Téléchargez le paquet d'installation de l'Agent d'administration via l'interface de l'application ou depuis le site Internet de Kaspersky.

3. Assurez-vous que le logiciel suivant est installé sur l'appareil Linux cible :

   - Sudo (pour Ubuntu 10.04, version de Sudo 1.7.2p1 ou version ultérieure)
   - Interpréteur Perl version 5.10 ou ultérieure

4. Lancez l'analyse de la configuration de l'appareil :

   a. Vérifiez que la connexion à l'appareil à l'aide de l'application client SSH (par exemple, l'application PuTTY) est possible.

   Si vous ne pouvez pas vous connecter à l'appareil, ouvrez le fichier `/etc/ssh/sshd_config` et veillez à ce que les paramètres suivants aient les valeurs :

   ```
   PasswordAuthentication no
   ChallengeResponseAuthentication yes
   ```

   > Ne modifiez pas le fichier /etc/ssh/sshd_config si vous pouvez vous connecter à l'appareil sans problèmes ; dans le cas contraire, vous pouvez rencontrer un échec de l'authentification SSH lors de l'exécution d'une tâche d'installation à distance.

   Enregistrez le fichier (si besoin) et relancez le service SSH à l'aide de la commande `sudo service ssh restart`.

   b. Désactivez le mot de passe de la demande sudo pour le compte utilisateur utilisé pour la connexion à l'appareil.

   c. Utilisez la commande `visudo` pour ouvrir le fichier de configuration sudoers.

   Dans le fichier que vous avez ouvert, ajoutez la ligne suivante à la fin du fichier : `<username> ALL = (ALL) NOPASSWD: ALL`. Dans ce cas, `< username >` est le compte utilisateur qui sera utilisé pour la connexion à l'appareil via le protocole SSH. Si vous utilisez le système d'exploitation Astra Linux, ajoutez dans le fichier /etc/sudoers la dernière ligne avec le texte suivant : `%astra-admin ALL=(ALL:ALL) NOPASSWD: ALL`

   d. Enregistrez le fichier sudoers et fermez-le.

   e. Connectez-vous à nouveau à l'appareil via SSH et vérifiez que le service Sudo ne requiert pas de mot de passe à l'aide de la commande `sudo whoami`.

5. Ouvrez le fichier `/etc/systemd/logind.conf`, puis effectuez l'une des opérations suivantes :

   - Spécifiez no comme valeur pour le paramètre KillUserProcesses : `KillUserProcesses=no`.
   - Pour le paramètre KillExcludeUsers, saisissez le nom d'utilisateur du compte sous lequel l'installation à distance doit être effectuée, par exemple, `KillExcludeUsers=root`.

   Si la machine cible exécute Astra Linux, ajoutez la chaîne `export PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin` dans le fichier `/home/<nom d'utilisateur>/.bashrc`, où `<nom d'utilisateur>` est le compte à utiliser pour la connexion de l'appareil via SSH.

   Pour appliquer le paramètre modifié, redémarrez l'appareil Linux ou exécutez la commande suivante :

   ```
   $ sudo systemctl restart systemd-logind.service
   ```

6. Si vous souhaitez installer l'Agent d'administration sur des appareils dotés du système d'exploitation SUSE Linux Enterprise Server 15, installer le paquet insserv-compat en premier pour configurer l'Agent d'administration.

7. Si vous souhaitez installer l'Agent d'administration sur des appareils dotés du système d'exploitation Astra Linux à l'aide de l'environnement logiciel fermé, exécutez les étapes complémentaires de préparation des appareils Astra Linux.

8. Si vous souhaitez installer l'Agent d'administration sur des appareils qui utilisent le système d'exploitation RED OS 7.3.4 ou une version ultérieure ou MSVSPHERE 9.2 ou une version ultérieure, installez le paquet libxcrypt-compat pour assurer le bon fonctionnement de l'Agent d'administration.

Installation à distance de l'Agent d'administration

Pour installer l'Agent d'administration sur l'appareil localement, procédez comme suit :

1. Téléchargez et créez le paquet d'installation :

   a. Avant l'installation du paquet sur l'appareil, assurez-vous que les dépendances (les applications, les bibliothèques) liées au paquet en question sont installées.

   Vous pouvez indépendamment consulter les dépendances liées à chaque paquet en utilisant les utilitaires spécifiques à ce distributif Linux sur lequel le paquet sera installé. Vous pouvez consulter les informations relatives aux utilitaires dans la documentation de votre système d'exploitation.

   b. Pour la création du paquet d'installation à distance, utilisez les fichiers :

   - klnagent.kpd
   - akinstall.sh
   - Paquet .deb ou .rpm de l'Agent d'administration

2. Créez la tâche d'installation à distance de l'application avec les paramètres :

   - Dans la page **Paramètres** de l'assistant de création d'une tâche, cochez la case **En utilisant les ressources du système d'exploitation via le Serveur d'administration**. Décochez toutes les autres cases.
   - Dans la page **Sélection du compte utilisateur pour exécuter la tâche**, définissez les paramètres du compte utilisateur servant à connecter l'appareil via SSH.

3. Lancez la tâche d'installation à distance de l'application. Utilisez l'option de la commande `su` pour préserver l'environnement : `-m, -p, --preserve-environment`.

Préparation d'un appareil exécutant SUSE Linux Enterprise Server 15 pour l'installation de l'Agent d'administration

Pour installer l'Agent d'administration sur un appareil doté du système d'exploitation SUSE Linux Enterprise Server 15,

Avant l'installation de l'Agent d'administration, exécutez la commande suivante :

```
$ sudo zypper install insserv-compat
```

Cela vous permet d'installer le paquet insserv-compat et de configurer correctement l'Agent d'administration.

Exécutez la commande `rpm -q insserv-compat` pour vérifier si le paquet est déjà installé.

Si votre réseau comprend de nombreux appareils exécutant SUSE Linux Enterprise Server 15, vous pouvez utiliser le logiciel spécial pour configurer et gérer l'infrastructure de l'entreprise. En utilisant ce logiciel, vous pouvez installer automatiquement le paquet insserv-compat sur tous les appareils nécessaires à la fois. Par exemple, vous pouvez utiliser Puppet, Ansible, Chef ou vous pouvez créer votre propre script en utilisant n'importe quelle méthode qui vous convient.

Si l'appareil ne dispose pas des clés de signature GPG pour SUSE Linux Enterprise, l'avertissement suivant peut s'afficher : `Package header is not signed!` Sélectionnez l'option `i` pour ignorer l'avertissement.

Outre l'installation du paquet insserv-compat, assurez-vous que vous avez complètement préparé vos appareils Linux. Après cela, déployer et installer l'Agent d'administration.

Préparation de l'appareil fonctionnant sous le système d'exploitation macOS à l'installation à distance de l'Agent d'administration

Pour préparer l'appareil fonctionnant sous le système d'exploitation macOS à l'installation à distance de l'Agent d'administration, procédez comme suit :

1. Vérifiez sur sudo est installé sur l'appareil macOS cible.

2. Lancez l'analyse de la configuration de l'appareil :

   a. Assurez-vous que le port 22 est ouvert sur l'appareil client. Pour ce faire, dans les **Préférences Système**, ouvrez le volet **Partage**, puis assurez-vous que la case **Connexion** à distance est cochée.

   Vous pouvez vous connecter à l'appareil client via Secure Shell (SSH) uniquement via le port 22. Vous ne pouvez pas modifier le numéro de port.

   Vous pouvez utiliser la commande `ssh <nom_de_l'appareil>` pour vous connecter à distance à l'appareil macOS. Dans le volet **Partage**, vous pouvez utiliser l'option **Autoriser l'accès à** pour définir l'étendue des utilisateurs autorisés à accéder à l'appareil macOS.

   b. Désactivez le mot de passe de la demande sudo pour le compte utilisateur utilisé pour la connexion à l'appareil.

   Utilisez la commande `sudo visudo` dans Terminal pour ouvrir le fichier de configuration sudoers. Dans le fichier que vous avez ouvert, dans l'entrée `Spécification des privilèges de l'utilisateur`, indiquez ce qui suit : `username ALL = (ALL) NOPASSWD: ALL`. Dans ce cas, `username` représente le compte utilisateur qui sera utilisé pour établir la connexion à l'appareil à l'aide du protocole SSH.

   c. Enregistrez le fichier sudoers et fermez-le.

   d. Connectez-vous à nouveau à l'appareil via SSH et vérifiez que le service Sudo ne requiert pas de mot de passe à l'aide de la commande `sudo whoami`.

3. Téléchargez et créez le paquet d'installation :

   a. Téléchargez le paquet d'installation de l'Agent d'administration à l'aide de l'une des méthodes suivantes :

      - Dans l'arborescence de la console, ouvrez le menu contextuel sur **Installation à distance → Paquets d'installation** et sélectionnez **Afficher les versions actuelles des applications** parmi les paquets disponibles
      - Téléchargez la version appropriée de l'Agent d'administration depuis le site Internet du Support Technique à l'adresse https://support.kaspersky.com/
      - Demandez le paquet d'installation aux spécialistes du Support Technique

   b. Pour la création du paquet d'installation à distance, utilisez les fichiers :

      - klnagent.kud
      - install.sh
      - klnagentmac.dmg

4. Créez la tâche d'installation à distance de l'application avec les paramètres :

   - Dans la page **Paramètres** de l'Assistant de création d'une tâche, cochez la case **En utilisant les ressources du système d'exploitation via le Serveur d'administration**. Décochez toutes les autres cases.
   - Dans la page **Sélection du compte utilisateur pour exécuter la tâche**, pour exécuter la tâche, définissez les paramètres du compte utilisateur servant à connecter l'appareil via SSH.

L'appareil client est prêt pour l'installation à distance de l'Agent d'administration au moyen de la tâche correspondante que vous avez créée.

Applications Kaspersky : licence et activation

Cette section décrit les possibilités de Kaspersky Security Center sur l'utilisation des clés de licence des applications administrées de Kaspersky.

Kaspersky Security Center permet de diffuser de manière centralisée les clés de licence des applications de Kaspersky sur les appareils clients, suivre l'utilisation des clés et de prolonger la durée de validité des licences.

Lors de l'ajout de la clé de licence à l'aide de Kaspersky Security Center, les propriétés de la clé de licence sont enregistrées sur le Serveur d'administration. Sur la base de ces informations, l'application crée un rapport sur les clés de licence utilisées et notifie l'administrateur de l'expiration de la durée de validité des licences et du dépassement des restrictions de licence énoncées dans les propriétés des clés de licence. Vous pouvez configurer les paramètres de notifications sur l'utilisation des clés de licence dans la composition des paramètres du Serveur d'administration.

Licence des applications administrées

Les applications Kaspersky installées sur les appareils administrés doivent disposer d'une licence sous la forme d'un fichier clé ou d'un code d'activation pour chaque application. Le déploiement d'un fichier clé ou d'un code d'activation peut s'effectuer comme suit :

- Déploiement automatique
- Le paquet d'installation d'une application administrée
- La tâche *Ajout de clé de licence* pour une application administrée
- L'activation manuelle d'une application administrée

Vous pouvez ajouter une nouvelle clé de licence active ou de réserve par l'une des méthodes répertoriées ci-dessus. Une application Kaspersky utilise une clé active à l'instant présent et stocke une clé de réserve à appliquer après l'expiration de la clé active. L'application pour laquelle vous ajoutez une clé de licence définit si la clé est active ou de réserve. La définition de clé ne dépend pas de la méthode que vous utilisez pour ajouter une nouvelle clé de licence.

Déploiement automatique

Si vous utilisez différentes applications administrées et que vous devez absolument déployer un fichier clé ou un code d'activation spécifique sur les appareils, utilisez d'autres modes de déploiement du code d'activation ou du fichier clé.

Kaspersky Security Center permet automatiquement de diffuser les clés de licence se trouvant sur les appareils. Par exemple, le stockage du Serveur d'administration contient trois clés de licence. Vous avez sélectionné la case **Distribuer automatiquement la clé de licence sur les appareils administrés** pour les trois clés de licence. Sur les appareils de l'entreprise, l'application de sécurité de Kaspersky, par exemple, Kaspersky Endpoint Security for Windows est installée. Un nouvel appareil a été détecté sur lequel il faut diffuser la clé de licence. L'application définit pour cet appareil, par exemple, que deux des clés de licence du stockage, la clé de licence dénommée *Clé_1* et la clé de licence dénommée *Clé_2* peuvent être déployées. Une de ces clés de licence est déployée sur l'appareil. Une des clés de licence adaptées est diffusée, et dans ce cas, il n'est pas possible de savoir laquelle de ces deux clés sera diffusée sur l'appareil car le déploiement automatique des clés de licence ne prévoit pas l'intervention de l'administrateur.

Lors du déploiement de la clé, les appareils sont recalculés pour cette clé de licence. Vous devez vous assurer que le nombre d'appareils sur lequel la clé de licence est diffusée ne dépasse pas la restriction de licence. Si le nombre d'appareils dépasse la restriction de licence, l'état *Critique* est attribué à tous les appareils non couverts par la licence.

Avant le déploiement, le fichier clé ou le code d'activation doit être ajouté au Stockage du Serveur d'administration.

Instructions pour :

- Console d'administration :
  - Ajout de la clé de licence dans le stockage du Serveur d'administration
  - Diffusion automatique de la clé de licence

  ou

- Kaspersky Security Center Web Console :
  - Ajout de la clé de licence dans le stockage du Serveur d'administration
  - Diffusion automatique de la clé de licence

Veuillez noter qu'une clé de licence diffusée automatiquement peut ne pas s'afficher dans le stockage du Serveur d'Administration virtuel dans les cas suivants :

- La clé de licence n'est pas valide pour l'application.
- Le Serveur d'administration virtuel n'a pas d'appareils administrés.
- La clé de licence a déjà été utilisée pour des appareils administrés par un autre Serveur d'administration virtuel et la limite du nombre d'appareils a été atteinte.

Ajout d'un fichier clé ou d'un code d'activation dans le paquet d'installation de l'application administrée

Pour des raisons de sécurité, cette option n'est pas recommandée. Un fichier clé ou un code d'activation ajouté à un paquet d'installation peut être compromis.

En cas d'installation d'une application administrée à l'aide du paquet d'installation, vous pouvez indiquer le code d'activation ou le fichier clé dans ce paquet d'installation ou dans la stratégie de l'application. La clé de licence est diffusée sur les appareils administrés lors de la synchronisation ultérieure de l'appareil avec le Serveur d'administration.

Instructions pour :

- Console d'administration :
  - Génération du paquet d'installation
  - Installation des applications sur les appareils clients

  ou

- Kaspersky Security Center Web Console : Ajout d'une clé de licence à un paquet d'installation

Déploiement par la tâche Ajout de clé de licence pour une application administrée

En cas de l'utilisation de la tâche *Ajout de la clé de licence* de l'application administrée, vous pouvez choisir la clé de licence qu'il faut diffuser sur les appareils, et sélectionner les appareils de la manière qui vous convient, par exemple, en sélectionnant un groupe d'administration ou une sélection d'appareils.

Avant le déploiement, le fichier clé ou le code d'activation doit être ajouté au Stockage du Serveur d'administration.

Instructions pour :

- Console d'administration :
  - Ajout de la clé de licence dans le stockage du Serveur d'administration
  - Déploiement d'une clé de licence sur les appareils clients

  ou
- Kaspersky Security Center Web Console :
  - Ajout de la clé de licence dans le stockage du Serveur d'administration
  - Déploiement d'une clé de licence sur les appareils clients

Ajout d'un code d'activation ou d'un fichier clé manuellement sur les appareils

Vous pouvez activer l'application Kaspersky installée localement, avec les outils fournis dans l'interface de l'application. Consultez la documentation de l'application installée.

Consultation des informations sur les clés de licence utilisées

Pour consulter les informations sur les clés de licence utilisées,

Dans l'arborescence de la console, sélectionnez le dossier **Licences pour les logiciels de Kaspersky**.

L'espace de travail du dossier affiche la liste des clés de licence utilisées sur les appareils clients.

A côté de chaque clé de licence, une icône, correspondant au type de son utilisation, s'affiche :

- : l'information sur la clé de licence utilisée est reçue depuis l'appareil client connecté au Serveur d'administration. Le fichier de cette clé de licence n'est pas enregistré sur le Serveur d'administration.
- : la clé de licence se trouve dans le stockage du Serveur d'administration. La diffusion automatique de cette clé de licence est désactivée.
- : la clé de licence se trouve dans le stockage du Serveur d'administration. La diffusion automatique de cette clé de licence est activée.

Vous pouvez consulter les informations sur les clés de licence utilisées pour l'activation de l'application d'un appareil client, en ouvrant la section **Applications** de la fenêtre des propriétés de l'appareil client.

Pour définir les paramètres actualisés des clés de licence du Serveur d'administration virtuel, le Serveur d'administration envoie une requête sur les serveurs d'activation de Kaspersky au moins une fois par jour. Si l'accès aux serveurs via le DNS système n'est pas possible, l'application utilise les serveurs DNS publics.

Si la clé de licence provient d'un appareil client, vous ne pouvez pas l'exporter en tant que fichier.

Ajout de la clé de licence dans le stockage du Serveur d'administration

Pour ajouter une clé de licence dans le stockage du Serveur d'administration, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le dossier **Licences pour les logiciels de Kaspersky**.
2. Lancez la tâche d'ajout de la clé de licence à l'aide d'un des moyens suivants :
   - Sélectionnez **Ajouter un code d'activation ou un fichier clé** dans le menu contextuel de la liste des clés de licence.
   - Cliquez sur le lien **&Ajouter un code d'activation ou un fichier clé** dans l'espace de travail de la liste des clés de licence.
   - Cliquez sur le bouton **&Ajouter un code d'activation ou un fichier clé**.

   Assistant d'ajout de clé de licence démarre.
3. Sélectionnez comment vous souhaitez activer le Serveur d'administration : en utilisant un code d'activation ou en utilisant un fichier clé.
4. Spécifiez votre code d'activation ou un fichier clé.
5. Sélectionnez l'option **Distribuer automatiquement la clé de licence sur les appareils administrés** si vous souhaitez distribuer immédiatement une clé de licence pertinente sur votre réseau. Si vous ne sélectionnez pas cette option, vous pouvez manuellement distribuer une clé de licence plus tard.

En conséquence, le fichier clé est téléchargé et l'Assistant d'ajout de clé de licence est terminé. Vous pouvez maintenant voir la clé de licence ajoutée dans la liste des licences Kaspersky.

Suppression de la clé de licence du Serveur d'administration

Pour supprimer une clé de licence du Serveur d'administration, procédez comme suit :

1. Dans le menu contextuel Serveur d'administration, sélectionnez l'option **Propriétés**.
2. Dans la fenêtre des propriétés du Serveur d'administration qui s'ouvre, sélectionnez la section **Clés de licence**.
3. Supprimez la clé de licence en cliquant sur le bouton **Supprimer**.

   Ceci supprime la clé de licence.

Si une clé de licence de réserve a été ajoutée, la clé de licence de réserve devient automatiquement la clé de licence active après la suppression de l'ancienne clé de licence active.

Suite à la suppression de la clé de licence active, les fonctions Gestion des vulnérabilités et des correctifs et Administration des appareils mobiles ne seront plus accessibles au Serveur d'administration. Vous pouvez ajouter de nouveau la clé de licence supprimée ou ajouter une autre clé de licence.

Déploiement d'une clé de licence sur les appareils clients

Kaspersky Security Center permet de diffuser la clé de licence sur les appareils clients à l'aide de la tâche de *diffusion de la clé de licence*.

Avant le déploiement, ajoutez une clé de licence au stockage du Serveur d'administration.

Afin de diffuser une clé de licence sur les appareils clients, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le dossier **Licences pour les logiciels de Kaspersky**.
2. Dans l'espace de travail de la liste des clés de licence, cliquez sur le bouton **Distribuer automatiquement la clé de licence sur les appareils administrés**.

   L'**Assistant de création d'une tâche d'activation de l'application** démarre. Parcourez les étapes de l'Assistant à l'aide du bouton **Suivant**.
3. Dans la liste des applications, sélectionnez l'application pour laquelle vous souhaitez créer une tâche.

4. À l'étape **Ajout d'une clé** de l'assistant, ajoutez la clé de licence d'une des manières suivantes :

   - Sélectionnez l'option **Code d'activation** pour ajouter un code d'activation depuis le stockage de Kaspersky Security Center.

     Cliquez sur **Parcourir**. Dans la fenêtre qui s'ouvre, sélectionnez le code d'activation, puis cliquez sur **OK**.

   - Sélectionnez l'option **Fichier clé ou clé**, puis procédez comme suit :

     a. Cliquez sur **Parcourir**.

     b. Dans le menu contextuel, sélectionnez une des options suivantes :

     - **Fichier clé depuis un dossier**.

       Dans la fenêtre qui s'ouvre, sélectionnez le fichier clé sur votre appareil, puis cliquez sur **Ouvrir**.

     - **Clé du référentiel Kaspersky Security Center**.

       Dans la fenêtre qui s'ouvre, sélectionnez la clé dans le stockage de Kaspersky Security Center, puis cliquez sur **OK**.

5. Si vous souhaitez remplacer la clé de licence active, décochez la case par défaut **Utiliser la clé en tant que clé de réserve**.

   Par exemple, cela est nécessaire lorsque l'organisation change et que la clé d'une autre organisation est requise sur l'appareil, ou si la clé a été réémise et qu'une nouvelle licence expire avant la licence actuelle. Pour éviter les erreurs, il convient de décocher la case **Utiliser la clé en tant que clé de réserve**.

   Si vous souhaitez en savoir plus sur les problèmes qui peuvent survenir lors de l'ajout d'une clé de licence à Kaspersky Security Center Windows et les moyens de les résoudre, consultez la Base de connaissances de Kaspersky Security Center.

6. Vérifiez les informations sur la clé de licence, puis cliquez sur **Suivant**.

7. À cette étape de l'Assistant, sélectionnez les appareils auxquels vous souhaitez affecter la tâche d'ajout d'une clé. Vous pouvez spécifier des appareils (jusqu'à 1 000 appareils) de l'une des manières suivantes :

   - **Sélectionner les appareils détectés sur le réseau par le Serveur d'administration**. Dans ce cas la tâche est affectée à un ensemble d'appareils. L'ensemble d'appareils peut reprendre aussi bien des appareils de groupes d'administration que des appareils non définis.

   - **Définir les adresses des appareils manuellement ou les importer à partir d'une liste**. Vous pouvez définir les noms NetBIOS, les noms DNS, les adresses IP, ainsi que les plages d'adresses IP auxquels il convient d'affecter la tâche.

   - **Attribuer la tâche à une sélection d'appareils**. Dans ce cas, la tâche est affectée aux appareils qui appartiennent à une sélection préalable. Vous pouvez spécifier la sélection prédéfinie ou une sélection personnalisée que vous avez créée.

   - **Attribuer la tâche à un groupe d'administration**. Dans ce cas, la tâche est affectée aux appareils qui appartiennent à un groupe d'administration déjà créé.

8. À l'étape **Planifier la tâche** de l'Assistant, planifiez le lancement de la tâche :

- **Lancement planifié** :
  - Une fois

    La tâche est exécutée une seule fois, à la date et à l'heure indiquées (par défaut, le jour de la création de la tâche).

  - Manuel

    La tâche ne s'exécute pas automatiquement. Vous pouvez uniquement la lancer manuellement.

    Cette option est sélectionnée par défaut.

  - Lors du téléchargement des mises à jour dans le stockage

    La tâche s'exécute après le téléchargement des mises à jour dans le stockage. Par exemple, vous pouvez utiliser cette programmation pour rechercher les vulnérabilités et les mises à jour requises.

  - Lors de la détection d'une attaque de virus

    La tâche s'exécute après un événement *Attaque de virus* de virus. Sélectionnez les types d'application qui vont surveiller les propagations de virus. Les types suivants de Application sont présent :

    - Antivirus pour postes de travail et serveurs de fichiers
    - Antivirus de protection du périmètre
    - Antivirus pour systèmes de messagerie

    Tous les types d'application sont cochés par défaut.

    Il se peut que vous souhaitiez exécuter différentes tâches en fonction du type d'application de sécurité qui signale une propagation de virus. Dans ce cas, supprimez la sélection des types d'application dont vous n'avez pas besoin.

  - Après l'exécution d'une autre tâche

La tâche actuelle démarre à la fin d'une autre tâche. Cette option ne fonctionne que si les deux tâches sont affectées aux mêmes appareils. Par exemple, vous pouvez exécuter la tâche *Administration des appareils* avec l'option **&Activer l'appareil** et, une fois celle-ci terminée, exécuter la tâche de *recherche de virus* comme tâche de déclenchement.

Il faut sélectionner la tâche de déclenchement dans le tableau et l'état avec lequel cette tâche doit se terminer (**Terminée avec succès** ou **Échec**).

Si nécessaire, vous pouvez rechercher, trier et filtrer les tâches dans le tableau comme suit :

- Saisissez le nom de la tâche dans le champ de recherche pour rechercher une tâche par son nom.
- Cliquez sur l'icône de tri pour trier les tâches par nom.

  Par défaut, les tâches sont triées par ordre alphabétique croissant.
- Cliquez sur l'icône du filtre, et dans la fenêtre qui s'ouvre, filtrez les tâches par groupe, puis cliquez sur le bouton **Appliquer**.

- **Lancer les tâches non exécutées**

  Cette option détermine le comportement d'une tâche si un appareil client n'est pas visible sur le réseau quand la tâche est sur le point de démarrer.

  Si la case est Activé, lors du lancement suivant de l'application de Kaspersky sur cet appareil client, une tentative de lancement de la tâche sera faite. Si la programmation de la tâche est **Manuel**, **Une fois** ou **Immédiatement**, la tâche est immédiatement lancée dès que l'appareil apparaît sur le réseau ou immédiatement après l'inclusion de l'appareil dans la zone d'action de la tâche.

  Si cette option est désactivée, seules les tâches planifiées s'exécutent sur les appareils clients. Pour les planifications **Manuel**, **Une fois** et **Immédiatement**, les tâches s'exécutent uniquement sur les appareils clients qui sont visibles sur le réseau. Par exemple, vous pouvez désactiver cette option pour une tâche qui consomme des ressources que vous voulez exécuter uniquement en dehors des heures de bureau.

  Cette option est Inactif par défaut.

- **Adopter un décalage aléatoire automatique pour les lancements de tâche**

  Si cette option est activée, la tâche est lancée sur les appareils clients de manière aléatoire au cours d'un intervalle défini. C'est ce qu'on appelle un *lancement échelonné d'une tâche*. Un lancement échelonné de tâche permet d'éviter la communication simultanée d'un nombre important d'appareils clients avec le Serveur d'administration lors du lancement de la tâche programmée.

  Le temps du lancement aléatoire est automatiquement calculée lors de la création d'une tâche selon le nombre d'appareils clients sur lesquels la tâche est diffusée. Par la suite, la tâche démarre toujours à l'heure de lancement calculée. Toutefois, quand les paramètres de la tâche sont modifiés ou si la tâche est lancée manuellement, la valeur calculée de l'heure de lancement de la tâche est modifiée.

  Si la case n'est pas cochée, le lancement de la tâche sur les appareils clients s'opère selon la planification.

- **Décaler aléatoirement le lancement de la tâche dans un intervalle de (min.)**

Si cette option est activée, la tâche est lancée sur les appareils clients de manière aléatoire au cours de l'intervalle défini. Un lancement échelonné de tâche permet d'éviter la communication simultanée d'un nombre important d'appareils clients avec le Serveur d'administration lors du lancement de la tâche programmée.

Si la case n'est pas cochée, le lancement de la tâche sur les appareils clients s'opère selon la planification.

Cette option est Inactif par défaut. Par défaut, la valeur de cet intervalle est de une minute.

9. À l'étape **Définition du nom de la tâche** de l'Assistant, indiquez le nom de la tâche. Le nom de la tâche ne peut pas contenir plus de 100 symboles et contenir de symboles spéciaux ("*<>?\:|).

10. À l'étape **Fin de la création de la tâche** de l'Assistant, cliquez sur le bouton **Terminer** pour quitter l'Assistant.

    Si vous souhaitez que la tâche démarre directement à la fin de l'Assistant, cochez la case **Lancer la tâche à la fin de l'Assistant**.

Les tâches créées à l'aide de l'**Assistant de création d'une tâche d'activation de l'application** sont des tâches destinées à des appareils spécifiques situées dans le dossier **Tâches** de l'arborescence de console.

Vous pouvez aussi créer une tâche de groupe ou une tâche locale de diffusion de la clé de licence à l'aide de l'Assistant de création de la tâche pour le groupe d'administration et pour l'appareil client.

Diffusion automatique de la clé de licence

Kaspersky Security Center permet de diffuser automatiquement sur les appareils administrés les clés de licence placées dans le stockage des clés sur le Serveur d'administration. La diffusion automatique des clés de licence ne s'applique pas aux appareils du dossier **Appareils non définis**.

Afin de diffuser automatiquement une clé de licence sur les appareils administrés, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le dossier **Licences pour les logiciels de Kaspersky**.

2. Dans l'espace de travail du dossier, sélectionnez la clé de licence que vous souhaitez diffuser automatiquement sur l'appareil.

3. Ouvrez la fenêtre des propriétés de la clé de licence sélectionnée à l'aide d'un des moyens suivants :

   - Dans le menu contextuel de la clé de licence, sélectionnez l'option **Propriétés**.

   - En cliquant sur le lien **Consulter les propriétés de la clé de licence** dans la zone d'informations correspondant à la clé de licence sélectionnée.

4. Dans la fenêtre ouverte des propriétés de la clé de licence, cochez la case **Clé de licence diffusée automatiquement**. Fermez la fenêtre des propriétés de la clé de licence.

La clé de licence sera automatiquement distribuée à tous les appareils compatibles.

La diffusion de la clé de licence est exécutée via les moyens de l'Agent d'administration. Aucune tâche de distribution de la clé de licence n'est créée pour l'application.

Lors de la distribution automatique de la clé de licence, la limite de licences sur le nombre d'appareils est prise en compte. (La restriction de licence est définie dans les propriétés de la clé de licence.) Si la limite liée à la restriction de licence est atteinte, la diffusion de la clé de licence sur les appareils s'arrête automatiquement.

Le Serveur d'administration virtuel distribue automatiquement les clés de licence depuis son stockage et depuis le stockage du Serveur d'administration. Voici nos recommandations :

- Utilisez la tâche *Ajouter une clé de licence* pour sélectionner la clé de licence qui doit être déployée sur les appareils.
- Évitez de désactiver l'option **Autoriser le déploiement automatique des clés de licence de ce Serveur d'administration virtuel sur ses appareils** dans les paramètres du Serveur d'administration virtuel. Sinon, le Serveur d'administration virtuel ne distribuera pas les clés de licence aux appareils, y compris les clés de licence du stockage du Serveur d'administration.

Si vous sélectionnez la case **Clé de licence diffusée automatiquement** dans la fenêtre des propriétés de la clé de licence, une clé de licence est immédiatement distribuée sur votre réseau. Si vous ne sélectionnez pas cette option, vous pouvez manuellement distribuer une clé de licence plus tard.

Création et consultation du rapport sur les clés de licence utilisées

Pour créer le rapport sur les clés de licence utilisées sur les appareils clients, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez l'entrée portant le nom du Serveur d'administration requis.
2. Dans l'espace de travail de l'entrée, sélectionnez l'onglet **Rapports**.
3. Choisissez le modèle du rapport **Rapport sur les clés de licence utilisées** ou créez un modèle de rapport du même type.

L'espace de travail du rapport d'utilisation des clés de licence affichera les informations sur les clés de licence actives et de réserve utilisées sur les appareils clients. Le rapport contient aussi les informations sur les appareils sur lesquels les clés de licence sont utilisées, ainsi que les informations sur les restrictions définies dans les propriétés des clés de licence.

Affichage des informations sur les clés de licence d'application

Pour découvrir les clés de licence utilisées pour une application Kaspersky, procédez comme suit :

1. Dans l'arborescence de la console de Kaspersky Security Center, sélectionnez l'entrée **Appareils administrés**, puis accédez à l'onglet **Appareils**.
2. Ouvrez le menu contextuel de l'appareil requis d'un clic droit, puis sélectionnez l'option **Propriétés**.
3. Dans la fenêtre des propriétés de l'appareil qui s'ouvre, sélectionnez la section **Applications**.

4. Dans la liste des applications qui s'affiche, choisissez l'application dont vous voulez afficher les clés de licence, puis cliquez sur le bouton **Propriétés**.

5. Dans la fenêtre des propriétés de l'application qui s'ouvre, sélectionnez la section **Clés de licence**.

   Les informations sont affichées dans l'espace de travail de cette section.

Exportation d'un fichier de clé de licence

Si votre clé de licence a été supprimée par accident et que vous souhaitez la restaurer, vous pouvez exporter un fichier de clé de licence à partir d'un autre Serveur d'administration.

Pour exporter le fichier de la clé de licence, dans la zone fonctionnelle **Exporter le fichier clé : Gestion des clés**, vous devez disposer du droit **Fonctions générales**.

Si la clé de licence provient d'un appareil client, vous ne pouvez pas l'exporter.

Pour exporter une clé de licence, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le dossier **Licences pour les logiciels de Kaspersky**.

2. Dans la liste, sélectionnez la clé de licence que vous souhaitez exporter sous forme de fichier.

3. Dans la zone d'informations qui s'ouvre, cliquez sur le lien **Exporter le fichier clé**.

4. Dans la fenêtre qui s'ouvre, indiquez le chemin d'accès au dossier dans lequel vous souhaitez enregistrer le fichier de clé de licence, puis indiquez un nom de fichier. Ensuite, cliquez sur **Enregistrer**.

Le fichier de clé de licence au format .key est exporté dans le dossier sélectionné.

Si la clé de licence dont vous avez exporté le fichier a été ajoutée au répertoire du Serveur d'administration en tant que code d'activation et que vous souhaitez ajouter le fichier de clé de licence exporté dans le répertoire d'un autre Serveur d'administration, vous devez l'ajouter en tant que code d'activation et non en tant que fichier de clé. Dans le cas contraire, une erreur se produit. Vous devez ouvrir le fichier de clé de licence exporté dans n'importe quel éditeur de texte pratique, puis copier le code d'activation.

Configuration de la protection réseau

Cette section fournit des informations sur la configuration manuelle des stratégies et des tâches, sur les rôles des utilisateurs et sur la création d'une structure de groupe d'administration et d'une hiérarchie des tâches.

Scénario : Configuration de la protection réseau

L'Assistant de démarrage rapide de l'application crée des stratégies et des tâches en utilisant les paramètres par défaut. Ces paramètres peuvent s'avérer imparfaits, ou même être interdits par l'organisation. Par conséquent, nous vous recommandons d'adapter ces stratégies et tâches et de créer d'autres stratégies et tâches, si elles sont nécessaires à votre réseau.

Prérequis

Avant de démarrer, assurez-vous que vous avez :

- Installé le Serveur d'administration de Kaspersky Security Center
- Installé Kaspersky Security Center Web Console (facultatif)
- Achevé le scénario d'installation principal de Kaspersky Security Center
- Achevé l'Assistant de configuration initiale de l'application ou créé manuellement les stratégies et tâches suivantes dans le groupe d'administration **Appareils administrés** :
  - La stratégie de Kaspersky Endpoint Security
  - La tâche de groupe de mise à jour de Kaspersky Endpoint Security
  - La stratégie de l'Agent d'administration
  - Tâche *Recherche de vulnérabilités et de mises à jour requises*

La configuration de la protection réseau se fait par étapes :

1. **Configuration et propagation des stratégies et des profils de stratégie de Kaspersky**

   Pour configurer et propager les paramètres des applications Kaspersky installées sur les appareils administrés, deux méthodes différentes de gestion de la sécurité sont possibles : centrés sur l'utilisateur ou sur l'appareil. Ces deux méthodes peuvent aussi être associées. Pour mettre en œuvre une gestion de la sécurité centrée sur le périphérique, vous pouvez utiliser les outils fournis dans la console d'administration basée sur Microsoft Management Console ou Kaspersky Security Center Web Console. L'administration de la sécurité centrée sur l'utilisateur ne peut être mise en œuvre par via Kaspersky Security Center Web Console.

2. **Configuration des tâches de gestion à distance des applications Kaspersky**

   Vérifiez les tâches créées avec l'assistant de démarrage rapide de l'application et adaptez si nécessaire.

   Instructions pour :

   - Console d'administration :
     - Paramétrage de la tâche de groupe de mise à jour de Kaspersky Endpoint Security
     - Planification de la tâche Recherche de vulnérabilités et des mises à jour requises
   - Kaspersky Security Center Web Console :
     - Paramétrage de la tâche de groupe de mise à jour de Kaspersky Endpoint Security

- La tâche Recherche de vulnérabilités et de mises à jour requises est créée

Le cas échéant, créez des tâches supplémentaires gérer les applications Kaspersky installées sur les machines clientes.

3. **Évaluation et limitation de la charge d'événements sur la base de données**

   Les informations sur les événements qui se produisent pendant le fonctionnement des applications administrées sont transmises de l'appareil client et enregistrées dans la base de données du Serveur d'administration. Pour réduire la charge sur le Serveur d'administration, évaluez et limitez le nombre maximal d'événements stockables dans la base de données.

   Instructions pour :

   - Console d'administration : Définition du nombre maximum d'événements
   - Kaspersky Security Center Web Console : Définition du nombre maximum d'événements

Résultats

À la fin de ce scénario, votre réseau sera protégé par la configuration des applications, tâches et événements de Kaspersky reçus par le serveur d'administration :

- Les applications de Kaspersky sont configurées en fonction des stratégies et des profils de stratégie.
- Les applications sont administrées via un ensemble de tâches.
- Le nombre maximal d'événements pouvant être stockés dans la base de données est défini.

Lorsque la configuration de la protection est terminée, vous pouvez procéder à la configuration des mises à jour régulières des bases de données et des applications Kaspersky.

Pour en savoir plus sur la configuration des réponses automatiques aux menaces détectées par Kaspersky Sandbox, veuillez consulter l'Aide en ligne de Kaspersky Sandbox 2.0.

Configuration et diffusion des stratégies : approche centrée sur l'appareil

Quand vous aurez terminé ce scénario, les applications seront configurées sur tous les appareils administrés conformément aux stratégies et aux profils de stratégie de l'application que vous avez définis.

Prérequis

Avant de commencer, vérifiez que vous avez installé le Serveur d'administration de Kaspersky Security Center et Kaspersky Security Center Web Console (facultatif). Si vous avez installé la Kaspersky Security Center Web Console, vous pouvez aussi vouloir la gestion de la sécurité centrée sur l'utilisateur comme alternative ou option supplémentaire à l'approche centrée sur l'appareil.

Étapes

Le scénario d'administration des applications de Kaspersky axé sur l'appareil comprend les étapes suivantes :

1 Configuration des stratégies des applications

Configurez les paramètres pour les applications de Kaspersky installées sur les appareils administrés par la création d'une stratégie pour chaque application. L'ensemble de ces stratégies seront propagées sur les appareils clients.

Si vous configurez la protection de votre réseau dans l'Assistant de configuration initiale de l'application, Kaspersky Security Center crée la stratégie par défaut pour les applications suivantes :

- Kaspersky Endpoint Security for Windows : pour les appareils clients Windows
- Kaspersky Endpoint Security for Linux : pour les appareils clients Linux

Si vous terminez cette procédure de configuration avec l'assistant, vous ne devez pas créer une nouvelle stratégie pour cette application. Continuez vers la configuration manuelle d'une stratégie de Kaspersky Endpoint Security.

Si vous disposez d'une structure hiérarchique de plusieurs Serveurs d'administration et/ou groupes d'administration, les Serveurs d'administration secondaires et les groupes d'administration enfants héritent des stratégies du Serveur d'administration principal par défaut. Vous pouvez forcer l'héritage par les groupes enfants et les Serveurs d'administration secondaires pour empêcher toute modification des paramètres configurés dans la stratégie en amont. Si vous voulez imposer l'héritage d'une partie uniquement des paramètres, vous pouvez les verrouiller dans la stratégie en amont. Les paramètres qui ne sont pas verrouillés pourront être modifiés dans les stratégies en aval. La hiérarchie de stratégies créée vous permettra d'administrer efficacement les appareils dans les groupes d'administration.

Instructions pour :

- Console d'administration : création d'une stratégie
- Kaspersky Security Center Web Console : création d'une stratégie

2 Création de profils de stratégie (facultatif)

Si vous souhaitez que les appareils au sein d'un même groupe d'administration soient exécutées sous des paramètres de stratégie divergents, créez des profils de stratégie pour ces appareils. Un profil de stratégie est un sous-ensemble nommé de paramètres de stratégie. Un profil de stratégie est un sous-ensemble nommé de paramètres de stratégie qui est diffusé sur les appareils avec la stratégie et qui vient compléter la stratégie quand une condition définie, la *condition d'activation du profil*, est remplie. Les profils contiennent uniquement les paramètres qui se distinguent de la stratégie " de base " en vigueur sur l'appareil administré (ordinateur, appareil mobile).

Grâce aux conditions d'activation du profil, vous pouvez appliquer différents profils de stratégie, par exemple, aux appareils situés dans une unité ou un groupe de sécurité d'Active Directory défini, avec une configuration matériel particulière ou avec des tags définis. Utilisez les tags pour filtrer les appareils qui répondent aux critères définis. Par exemple, vous pouvez créer un tag *Windows*, l'attribuez à tous les appareils qui tournent sous Windows, puis désignez ce tag comme condition d'activation pour un profil de stratégie. Par conséquent, les applications de Kaspersky installées sur tous les appareils tournant sous Windows seront administrées par leur propre profil de stratégie.

Instructions pour :

- Console d'administration :
  - Création d'un profil de stratégie
  - Création d'une règle d'activation du profil de stratégie
- Kaspersky Security Center Web Console :
  - Création d'un profil de stratégie

- Création d'une règle d'activation du profil de stratégie

3. **Propagation des stratégies et des profils de stratégie sur les appareils administrés**

   Par défaut, le Serveur d'administration se synchronise automatiquement avec les appareils administrés toutes les 15 minutes. Vous pouvez aussi contourner la synchronisation automatique et exécuter manuellement la synchronisation par la commande Forcer la synchronisation. De plus, la synchronisation est forcée après la création ou la modification d'une stratégie ou d'un profil de stratégie. Lors de la synchronisation, les stratégies et profils de stratégie neufs ou modifiés sont propagés aux appareils administrés.

   Si vous utilisez la Kaspersky Security Center Web Console, vous pouvez vérifier si les stratégies et les profils de stratégie ont été livrés à un appareil. Kaspersky Security Center indique la date et l'heure de remise dans les propriétés de l'appareil.

   Instructions pour :

   - Console d'administration : Synchronisation forcée
   - Kaspersky Security Center Web Console : synchronisation forcée

Résultats

Une fois le scénario centré sur l'appareil terminé, les applications de Kaspersky sont configurées selon les paramètres spécifiés et propagés par la hiérarchie des stratégies.

Les stratégies et les profils de stratégie de l'application configurés sont appliqués automatiquement aux nouveaux appareils ajoutés aux groupes d'administration.

À propos des méthodes d'administration de la sécurité centrées sur l'appareil et l'utilisateur

Vous pouvez gérer les paramètres de sécurité du point de vue des fonctionnalités de l'appareil et des rôles utilisateurs. La première approche s'appelle *gestion de la sécurité centrée sur l'appareil* et la seconde s'appelle *gestion de la sécurité centrée sur l'utilisateur*. Pour appliquer différents paramètres d'application à différents appareils, vous pouvez utiliser un type d'administration ou les deux types d'administration ensemble. Pour mettre en œuvre une gestion de la sécurité centrée sur l'appareil, vous pouvez utiliser les outils fournis dans la Console d'administration basée sur Microsoft Management Console ou Kaspersky Security Center Web Console. L'administration de la sécurité centrée sur l'utilisateur ne peut être mise en œuvre par via la Kaspersky Security Center Web Console.

La gestion de la sécurité centrée sur l'appareil vous permet d'appliquer différents paramètres d'application de sécurité aux appareils administrés en fonction de leurs caractéristiques. Par exemple, vous pouvez appliquer différents paramètres aux appareils alloués à des groupes d'administration différents. Vous pouvez également différencier les appareils en fonction de leur utilisation dans Active Directory ou de leurs spécifications matérielles.

La gestion de la sécurité centrée sur l'utilisateur vous permet d'appliquer différents paramètres d'application de sécurité à différents rôles d'utilisateur. Vous pouvez créer plusieurs rôles d'utilisateur, attribuer un rôle d'utilisateur approprié à chaque utilisateur et définir différents paramètres d'application pour les appareils appartenant à des utilisateurs dotés de rôles différents. Ainsi, vous souhaitez peut-être appliquer des paramètres des applications divergents pour les appareils des comptables et des collaborateurs des ressources humaines (RH). Par conséquent, lorsque l'administration de la sécurité centrée sur l'utilisateur est mise en œuvre, chaque département (les départements de comptabilité et RH) dispose de sa propre configuration de paramètres pour gérer les applications de Kaspersky. Une configuration de paramètres définit les paramètres d'application pouvant être modifiés par les utilisateurs et ceux définis de manière obligatoire et verrouillés par l'administrateur.

Utilisez une gestion de la sécurité centrée sur l'utilisateur pour pouvoir appliquer des paramètres d'application spécifiques pour des utilisateurs individuels. Cela peut être nécessaire lorsqu'un employé a un rôle unique dans l'entreprise ou lorsque vous souhaitez surveiller les problèmes de sécurité liés aux appareils d'une personne en particulier. Selon le rôle de cet employé dans l'entreprise, vous pouvez étendre ou limiter les droits de cette personne pour modifier les paramètres de l'application. Par exemple, vous souhaiterez peut-être étendre les droits d'un administrateur système qui gère les appareils clients d'une agence locale.

Il est également possible de combiner l'administration de la sécurité centrée sur l'appareil et celle centrée sur l'utilisateur. Par exemple, vous pouvez configurer une stratégie pour une application définie pour chaque groupe d'administration, puis créer des profils des stratégies pour un ou plusieurs rôles d'utilisateurs de votre entreprise. Dans ce cas, les stratégies et les profils de stratégie s'appliquent selon l'ordre suivant :

1. Les stratégies créées pour la gestion de la sécurité centrée sur l'appareil s'appliquent.
2. Elles sont modifiées par les profils de stratégie selon les priorités du profil de stratégie.
3. Les stratégies sont modifiées par les profils de stratégie associés aux rôles d'utilisateur.

Configuration manuelle d'une stratégie de Kaspersky Endpoint Security

Cette section fournit des recommandations sur la configuration de la stratégie de Kaspersky Endpoint Security créée par l'Assistant de configuration initiale de l'application. Vous pouvez effectuer la configuration dans la fenêtre des propriétés de la stratégie.

En cas de modification d'un paramètre, il convient de cliquer sur le bouton avec le cadenas au-dessus du paramètre pour que la valeur du paramètre soit appliquée sur le poste de travail.

Configuration de la stratégie dans la section Protection avancée

> Pour obtenir une description complète des paramètres dans cette section, veuillez consulter la documentation de Kaspersky Endpoint Security for Windows.

Dans la section **Protection avancée**, vous pouvez configurer l'utilisation de Kaspersky Security Network pour Kaspersky Endpoint Security for Windows. Vous pouvez également configurer les modules de Kaspersky Endpoint Security for Windows, tels que Détection comportementale, Protection contre les exploits, Prévention des intrusions et Réparation des actions malicieuses.

Dans la sous-section **Kaspersky Security Network**, nous vous recommandons d'activer l'option **Kaspersky Security Network**. L'utilisation de cette option aide à rediffuser et optimiser le trafic sur le réseau. Si l'option **Kaspersky Security Network** est désactivée, vous pouvez activer l'utilisation directe des serveurs KSN.

Configuration de la stratégie dans la section Protection principale

Pour obtenir une description complète des paramètres dans cette section, veuillez consulter la documentation de Kaspersky Endpoint Security for Windows.

Dans la section **Protection principale** de la fenêtre des propriétés de la stratégie, nous vous recommandons de définir des paramètres supplémentaires dans les sous-sections **Pare-feu** et **Protection contre les fichiers malicieux**.

La sous-section **Pare-feu** contient les paramètres qui vous permettent de contrôler l'activité réseau des applications sur les appareils clients. Un appareil client utilise un réseau auquel l'un des états suivants est attribué : public, local ou de confiance. Selon l'état du réseau, Kaspersky Endpoint Security peut autoriser ou interdire l'activité réseau sur un appareil. Lorsque vous ajoutez un nouveau réseau à votre organisation, vous devez lui attribuer un état de réseau approprié. Par exemple, si l'appareil client est un ordinateur portable, nous recommandons que cet appareil utilise le réseau public ou de confiance, car l'ordinateur portable n'est pas toujours connecté au réseau local. Dans la sous-section **Pare-feu**, vous pouvez vérifier si vous avez correctement attribué des états aux réseaux utilisés dans votre organisation.

Pour vérifier la liste des réseaux, procédez comme suit :

1. Dans les propriétés de la stratégie, accédez à **Protection principale** → **Pare-feu**.
2. Dans le groupe **Réseaux disponibles**, cliquez sur le bouton **Paramètres**.
3. Dans la fenêtre **Pare-feu** qui s'ouvre, accédez à l'onglet **Réseaux** pour consulter la liste des réseaux.

La sous-section **Protection contre les fichiers malicieux** permet de désactiver l'analyse des disques réseau. L'analyse des disques réseau peut placer une charge importante sur les disques réseau. Il est préférable de réaliser l'analyse directement sur les serveurs de fichiers.

Pour désactiver l'analyse des disques réseau, procédez comme suit :

1. Dans les propriétés de la stratégie, accédez à **Protection principale** → **Protection contre les fichiers malicieux**.
2. Dans le groupe **Niveau de sécurité**, cliquez sur le bouton **Paramètres**.
3. Dans la fenêtre **Protection contre les fichiers malicieux** qui s'ouvre, accédez à l'onglet **Général** et décochez la case **Tous les disques réseau**.

Configuration de la stratégie dans la section Paramètres généraux

Pour obtenir une description complète des paramètres dans cette section, veuillez consulter la documentation de Kaspersky Endpoint Security for Windows.

Dans la section **Paramètres généraux** de la fenêtre des propriétés de la stratégie, nous vous recommandons de définir des paramètres supplémentaires dans les sous-sections **Rapports et stockage** et **Interface**.

Dans la sous-section **Rapports et stockage**, accédez à la section **Transfert des données au Serveur d'administration**. La case **À propos des applications exécutables** détermine si la base de données du Serveur d'administration enregistre les informations relatives à toutes les versions de tous les modules des applications sur les appareils dans le réseau de l'entreprise. Quand cette case est cochée, les informations enregistrées peuvent occuper un espace considérable dans la base de données de Kaspersky Security Center (des dizaines de gigaoctets). Décochez la case **À propos des applications exécutables** si elle est sélectionnée dans la stratégie de niveau supérieur.

Si la Console d'administration gère la protection contre les menaces sur le réseau de l'entreprise en mode centralisé, désactivez l'affichage de l'interface utilisateur de Kaspersky Endpoint Security for Windows sur les postes de travail. Pour ce faire, dans la sous-section **Interface**, accédez à la section **Interaction avec l'utilisateur**, puis sélectionnez l'option **Ne pas afficher**.

Pour activer la protection par mot de passe sur les postes de travail, dans la sous-section **Interface**, accédez à la section **Protection par mot de passe**, cliquez sur le bouton **Paramètres**, puis cochez la case **Activer la protection par mot de passe**.

Configuration de la stratégie dans la section Configuration d'événement

Il faut désactiver, dans la section **Configuration de l'événement**, la conservation de tous les événements sur le Serveur d'administration, à l'exception des événements ci-après :

- Sous l'onglet **Critique** :
  - *Le lancement automatique de l'application est désactivé*
  - *Accès interdit*
  - *Le lancement de l'application est interdit*
  - *Désinfection impossible*
  - *Contrat de licence utilisateur final violé*
  - *Impossible de charger le module de chiffrement*
  - *Impossible de lancer deux tâches simultanément*
  - *Une menace active a été détectée. Il faut lancer la procédure de désinfection avancée*
  - *Une attaque réseau a été détectée*
  - *Certains modules n'ont pas été mis à jour*
  - *Erreur d'activation*
  - *Erreur d'activation du mode portable*
  - *Erreur d'interaction avec Kaspersky Security Center*
  - *Erreur de désactivation du mode portable*
  - *Erreur de modification de la sélection de modules de l'application*
  - *Erreur d'application des règles de chiffrement/déchiffrement des fichiers*
  - *La stratégie ne peut pas être appliquée*
  - *Le processus est terminé*
  - *L'activité réseau est interdite*
- Dans l'onglet **Erreur de fonctionnement** : *Erreur dans les paramètres de la tâche. Les paramètres ne sont pas appliqués*

- Sous l'onglet **Avertissement** :
  - *L'Autodéfense de l'application est désactivée*
  - *La clé de réserve est incorrecte*
  - *L'utilisateur a refusé la stratégie de chiffrement*
- Sous l'onglet **Information** : *Le lancement de l'application est interdit en mode test*

Configuration manuelle d'une tâche de groupe de mise à jour de Kaspersky Endpoint Security

L'option de planification optimale et recommandée pour Kaspersky Endpoint Security versions 10 et ultérieures est **Lors du téléchargement des mises à jour dans le stockage** quand la case **Adopter un décalage aléatoire automatique pour les lancements de tâche** est cochée.

Configuration manuelle d'une tâche de groupe d'analyse de l'appareil de Kaspersky Endpoint Security

L'Assistant de configuration initiale de l'application crée la tâche de groupe d'analyse d'un appareil. La programmation par défaut de la tâche est **Lancer tous les vendredi à 19:00** avec allocation aléatoire automatique et la case **Lancer les tâches non exécutées** est décochée.

Cela signifie que si les appareils de la société sont désactivés le vendredi à 18h30, la tâche d'analyse de l'appareil ne sera jamais lancée. Il faut configurer une programmation optimale de cette tâche sur la base du règlement de travail adopté par la société.

Planification de la tâche Recherche de vulnérabilités et des mises à jour requises

L'Assistant de configuration initiale de l'application crée une tâche *Recherche de vulnérabilités et de mises à jour requises* pour l'Agent d'administration. Par défaut, la programmation choisie pour cette tâche est **Lancer tous les mardi à 19:00** avec randomisation automatique et la case **Lancer les tâches non exécutées** est cochée.

Si le règlement de travail de la société prévoit la désactivation des appareils à ce moment, la tâche *Recherche de vulnérabilités et de mises à jour requises* est lancée après l'activation de l'appareil (le mercredi matin). Ce comportement est à éviter car la recherche de vulnérabilités peut augmenter la charge sur le processeur et le sous-système de disque de l'appareil. Vous devez configurer une programmation optimale de cette tâche sur la base du règlement de travail adopté par l'entreprise.

Configuration manuelle d'une tâche de groupe d'installation des mises à jour et de correction des vulnérabilités

L'Assistant de configuration initiale de l'application crée une tâche de groupe d'installation des mises à jour et de recherche de vulnérabilités pour l'Agent d'administration. Par défaut, le lancement de la tâche est prévu chaque jour à 1:00 avec allocation aléatoire automatique, et l'option **Lancer les tâches non exécutées** n'est pas activée.

Si le règlement de travail de la société prévoit la désactivation des appareils pendant la nuit, la tâche d'installation des mises à jour ne sera jamais exécutée. Il faut définir le calendrier optimum de la tâche de recherche de vulnérabilités sur la base du règlement de travail en vigueur dans la société. De plus, il ne faut pas oublier que l'installation des mises à jour peut requérir le redémarrage de l'appareil.

Définition du nombre d'événements maximal dans le stockage d'événements

Dans la section **Stockage d'événements** de la fenêtre de propriétés du Serveur d'administration, vous pouvez configurer les paramètres de stockage des événements dans la base de données du Serveur d'administration en limitant le nombre d'enregistrements sur les événements et la durée de stockage de ces derniers. Quand vous définissez le nombre maximal d'événements, l'application calcule un espace de stockage approximatif requis pour la quantité indiquée. Ce calcul approximatif permet d'évaluer si vous avez assez d'espace libre sur le disque pour éviter un débordement de base de données. Par défaut, la capacité de la base de données du Serveur d'administration est de 400 000 événements. La capacité maximale recommandée de la base de données est de 45 millions d'événements.

L'application vérifie la base de données toutes les 10 minutes. Si le nombre d'événements atteint la valeur maximale indiquée plus 10 000, l'application supprime les événements les plus anciens de manière à ne conserver que le nombre maximal d'événements indiqué.

Quand le Serveur d'administration supprime les anciens événements, il ne peut pas enregistrer les nouveaux événements dans la base de données. Durant cette période, les informations relatives aux événements qui ont été rejetés sont écrites dans le journal des événements Kaspersky. Les nouveaux événements sont placés dans une file d'attente et enregistrés dans la base de données dès que la suppression est terminée.

Pour limiter le nombre d'événements qui peut être stocké dans la base d'événements du Serveur d'administration :

1. Cliquez avec le bouton droit de la souris sur le Serveur d'administration, puis sélectionnez **Propriétés**.

   La fenêtre des propriétés du Serveur d'administration s'ouvre.

2. Dans l'espace de travail de la section **Stockage d'événements**, spécifiez le nombre maximal d'événements stockés dans la base de données.

3. Cliquez sur le bouton **OK**.

De plus, vous pouvez modifier les paramètres de n'importe quelle tâche pour enregistrer les événements liés à la progression de la tâche ou enregistrer uniquement les résultats de l'exécution de la tâche. Ainsi, vous diminuez le nombre d'événements dans la base de données, vous augmentez la vitesse de fonctionnement des scénarios liés à l'analyse du tableau des événements dans la base de données, et vous réduisez le risque que les événements critiques soient ignorés.

Définition de la durée maximale de stockage des informations sur les vulnérabilités corrigées

Pour définir la période de stockage maximale dans la base de données pour les informations sur les vulnérabilités qui ont déjà été corrigées sur les appareils administrés, procédez comme suit :

1. Cliquez avec le bouton droit de la souris sur le Serveur d'administration, puis sélectionnez **Propriétés**.

   La fenêtre des propriétés du Serveur d'administration s'ouvre.

2. Dans l'espace de travail de la section **Stockage d'événements**, indiquez la période de stockage maximale des informations sur les vulnérabilités corrigées dans la base de données.

   Par défaut, la période de stockage est de 90 jours.

3. Cliquez sur le bouton **OK**.

La période de stockage maximale des informations sur les vulnérabilités corrigées est limitée au nombre de jours indiqué. Après cela, la tâche de maintenance du Serveur d'administration supprimera les informations obsolètes de la base de données.

Gérer les tâches

Kaspersky Security Center gère les applications installées sur les appareils par la création et l'exécution de différentes tâches. Les tâches permettent d'exécuter l'installation, le lancement et l'arrêt des applications, l'analyse des fichiers, la mise à jour des bases de données et des modules des applications, les autres actions avec les applications.

Les tâches sont scindées en types suivants :

- *Tâches de groupe*. Tâches exécutées sur les appareils du groupe d'administration sélectionné.
- *Tâches du Serveur d'administration*. Tâches exécutées sur le Serveur d'administration.
- *Tâches pour un ensemble d'appareils*. Tâches exécutées sur les appareils sélectionnés peu importe leur inclusion dans les groupes d'administration.
- *Tâches locales*. Tâches exécutées sur un appareil particulier.

La création des tâches pour l'application est possible uniquement si le poste de travail de l'administrateur est doté du plug-in d'administration de l'application.

La liste des appareils (jusqu'à 1 000 appareils) pour lesquels la tâche sera créée peut être formée par une des méthodes suivantes :

- Sélectionner les appareils détectés sur le réseau par le Serveur d'administration.
- Définir la liste des appareils manuellement. Vous pouvez utiliser l'adresse IP (ou l'intervalle IP), le nom NetBIOS ou le nom DNS en tant que l'adresse de l'appareil.
- Importer la liste des appareils depuis le fichier au format TXT, contenant la liste des adresses des appareils ajoutés (chaque adresse doit se trouver dans une ligne séparée).

  Si la liste des appareils est importée depuis le fichier ou formée manuellement et les appareils sont identifiés selon le nom, uniquement les appareils dont les informations sont déjà enregistrées dans la base de données du Serveur d'administration peuvent être ajoutés dans la liste lors de la connexion des appareils ou lors de la recherche d'appareils.

Pour chaque application vous pouvez créer n'importe quel nombre de tâches de groupe, de tâches pour un ensemble d'appareils et des tâches locales.

L'échange des informations sur les tâches entre l'application installée sur l'appareil et la base d'informations de Kaspersky Security Center a lieu au moment de la connexion de l'Agent d'administration au Serveur d'administration.

Vous pouvez modifier les paramètres des tâches en l'exécution des tâches, copier, exporter ou importer, ainsi que supprimer les Tâches.

Les tâches ne sont lancées sur un appareil que lorsque l'application pour laquelle les tâches ont été créées est lancée. Si l'application est désactivée, toutes les tâches courantes sont annulées.

Les résultats de l'exécution des tâches sont enregistrés dans les journaux des événements Microsoft Windows et Kaspersky Security Center d'une manière centralisée sur le Serveur d'administration et d'une manière locale sur chaque appareil.

N'incluez pas de données confidentielles dans les paramètres des tâches. Par exemple, le mot de passe de l'administrateur de domaine.

Détails des tâches d'administration pour les applications qui prennent en charge l'architecture mutualisée.

Une tâche de groupe pour une application qui prend en charge l'architecture mutualisée est appliquée à l'application en fonction de la hiérarchie des Serveurs d'administration et des appareils clients. Le Serveur d'administration virtuel au départ duquel la tâche est créée doit se trouver dans le même groupe d'administration que l'appareil client sur lequel l'application a été installée ou dans un groupe de niveau inférieur.

Dans les événements qui correspondent aux résultats de l'exécution de la tâche, l'administrateur du fournisseur de service voit les informations relatives à l'appareil sur lequel la tâche est exécutée. Par contraste, en cas d'administration de locataire, un **Nœud multi-locataire** s'affiche.

Création d'une tâche

Dans la Console d'administration, il est possible de créer des tâches directement dans le dossier du groupe d'administration pour lequel la tâche de groupe est créée ou dans l'espace de travail du dossier **Tâches**.

Pour créer une tâche de groupe dans le dossier du groupe d'administration, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le groupe d'administration pour lequel il faut créer une tâche.
2. Dans l'espace de travail du groupe, sélectionnez l'onglet **Tâches**.
3. Exécutez le processus de création d'une tâche en cliquant sur le bouton **Créer une tâche**.

   Ceci permet de lancer l'Assistant de création d'une tâche. Suivez les instructions de l'assistant.

*Pour créer une tâche dans l'espace de travail du dossier **Tâches**, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le dossier **Tâches**.
2. Exécutez le processus de création d'une tâche en cliquant sur le bouton **Terminer**.

   Ceci permet de lancer l'Assistant de création d'une tâche. Suivez les instructions de l'assistant.

N'incluez pas de données confidentielles dans les paramètres des tâches. Par exemple, le mot de passe de l'administrateur de domaine.

Création d'une tâche du Serveur d'administration

Le Serveur d'administration exécute les tâches suivantes :

- Livrer des rapports
- Télécharger les mises à jour dans le stockage du serveur d'administration
- Sauvegarde des données du Serveur d'administration
- Maintenance du Serveur d'administration
- Synchronisation de Windows Update
- Créer un paquet d'installation sur l'image du système d'exploitation de l'appareil de référence
- Installer une application à distance
- Désinstaller une application à distance

- Diffusion du paquet d'installation
- Installation des applications sur les Serveurs d'administration secondaires à distance

Uniquement la tâche de diffusion automatique des rapports est disponible sur le Serveur d'administration virtuel, ainsi que la tâche de création du paquet d'installation sur la base de l'image du système d'exploitation de l'appareil d'étalon. Les mises à jour téléchargées sur le Serveur d'administration principal s'affichent dans le stockage du Serveur d'administration virtuel. La copie de sauvegarde des données du Serveur d'administration virtuel s'effectue dans le cadre de la copie de sauvegarde des données du Serveur d'administration principal.

Pour créer une tâche du Serveur d'administration, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le dossier **Tâches**.
2. Lancez le processus de création de la tâche par un des moyens suivants :
   - En sélectionnant **Nouveau** → **Tâche** dans le menu contextuel du dossier **Tâches** dans l'arborescence de la console.
   - En cliquant sur le bouton **Créer une tâche** dans l'espace de travail du dossier **Tâches**.

   Ceci permet de lancer l'Assistant de création d'une tâche. Suivez les instructions de l'assistant.

Les tâches Télécharger les mises à jour dans le stockage du Serveur d'administration, Synchronisation de Windows Update, Maintenance du Serveur d'administration et *Sauvegarde des données du Serveur d'administration* peuvent exister dans un seul exemplaire. Si les tâches *Télécharger les mises à jour dans le stockage du Serveur d'administration*, *Maintenance du Serveur d'administration*, *Sauvegarde des données du Serveur d'administration* et *Synchronisation de Windows Update* ont déjà été créées pour le Serveur d'administration, elles ne s'affichent pas dans la fenêtre de sélection du type de tâche de l'Assistant de création d'une tâche.

Création d'une tâche pour un ensemble d'appareils

Kaspersky Security Center permet de créer des tâches pour un ensemble d'appareils sélectionné d'une manière aléatoire. Les appareils dans l'ensemble peuvent être inclus dans des différents groupes d'administration ou ne faire partie d'un aucun groupe d'administration. Kaspersky Security Center permet d'exécuter les tâches principales suivantes pour un ensemble d'appareils :

- Installation d'une application à distance
- Envoyer le message à l'utilisateur
- Modifier le Serveur d'administration
- Administration des appareils
- Vérifier les mises à jour
- Diffuser les paquets d'installation

- Installation des applications sur les Serveurs d'administration secondaires à distance
- Désinstaller à distance une application

Pour créer une tâche pour un ensemble d'appareils, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le dossier **Tâches**.
2. Lancez le processus de création de la tâche par un des moyens suivants :
   - En sélectionnant **Nouveau** → **Tâche** dans le menu contextuel du dossier **Tâches** dans l'arborescence de la console.
   - En cliquant sur le bouton **Créer une tâche** dans l'espace de travail du dossier **Tâches**.

   Ceci permet de lancer l'Assistant de création d'une tâche. Suivez les instructions de l'assistant.

Création d'une tâche locale

Pour créer une tâche locale pour un appareil, procédez comme suit :

1. Dans l'espace de travail du groupe incluant l'appareil client, sélectionnez l'onglet **Appareils**.
2. Dans la liste des appareils, sous l'onglet **Appareils**, sélectionnez l'appareil pour lequel une tâche locale doit être créée.
3. Lancez le processus de création d'une tâche pour l'appareil sélectionné à l'aide d'un des moyens suivants :
   - En cliquant sur le bouton **Exécuter l'action** puis, dans la liste déroulante, en sélectionnant **Créer une tâche**.
   - En cliquant sur le lien **Créer une tâche** dans l'espace de travail de l'appareil.
   - Utilisez la fenêtre des propriétés de l'appareil :
     a. Dans le menu contextuel de l'appareil, sélectionnez l'option **Propriétés**.
     b. Dans la fenêtre des propriétés de l'appareil qui s'ouvre, sélectionnez la section **Tâches** et cliquez sur le bouton **Ajouter**.

   Ceci permet de lancer l'Assistant de création d'une tâche. Suivez les instructions de l'assistant.

Pour plus d'informations sur la création et la configuration des tâches locales, reportez-vous à la documentation des applications Kaspersky correspondantes.

Affichage d'une tâche de groupe héritée dans l'espace de travail du groupe imbriqué

Pour activer l'affichage des tâches héritées du groupe imbriqué dans l'espace de travail, procédez comme suit :

1. Sélectionnez l'onglet **Tâches** dans l'espace de travail d'un groupe imbriqué.
2. Dans l'espace de travail de l'onglet **Tâches**, cliquez sur le bouton **Afficher les tâches héritées**.

Ainsi, les tâches héritées s'affichent dans la liste des tâches avec l'icône :

- : si elles ont été héritées du groupe créé sur le Serveur d'administration principal.
- : si elles ont été héritées d'un groupe de niveau supérieur.

Lorsque le mode d'héritage est activé, la modification des tâches héritées n'est possible que dans les groupes où elles ont été créées. La modification des tâches héritées n'est pas disponible dans le groupe qui hérite les tâches.

Activation automatique des appareils avec le lancement de la tâche

Kaspersky Security Center n'exécute pas de tâches sur les appareils éteints. Vous pouvez configurer Kaspersky Security Center pour qu'il allume automatiquement ces appareils avant de démarrer une tâche, en utilisant la fonction Wake-on-LAN.

Pour configurer le démarrage automatique des appareils avant de démarrer une tâche :

1. Dans la fenêtre des propriétés des tâches, sélectionnez la section **Programmation**.
2. Pour configurer des actions sur les appareils, cliquez sur le lien **Avancé**.
3. Dans la fenêtre **Avancé** qui s'ouvre, cochez la case **Allumer les appareils en utilisant la fonctionnalité Wake-on-LAN avant le lancement de la tâche (min.)**. Ensuite, spécifiez le temps souhaité en minutes.

Par conséquent, pendant le nombre de minutes spécifié avant le démarrage de la tâche, Kaspersky Security Center allume les appareils et y charge le système d'exploitation à l'aide de la fonction Wake-on-LAN. Une fois la tâche terminée, les appareils sont automatiquement arrêtés si les utilisateurs de l'appareil ne se connectent pas au système. Notez que Kaspersky Security Center arrête automatiquement uniquement les appareils activés à l'aide de la fonction Wake-on-LAN.

Kaspersky Security Center peut démarrer automatiquement les systèmes d'exploitation uniquement sur les appareils prenant en charge la norme Wake-on-LAN (WoL).

Arrêt automatique de l'appareil après l'exécution de la tâche

Kaspersky Security Center permet de configurer une tâche de telle sorte que les appareils sur lesquels il est diffusé s'éteignent automatiquement quand la tâche est terminée.

Pour que les appareils soient automatiquement éteints après l'exécution des tâches, procédez comme suit :

1. Dans la fenêtre des propriétés des tâches, sélectionnez la section **Programmation**.
2. Cliquez sur le lien **Avancé** pour ouvrir la fenêtre de configuration des actions sur les appareils.
3. Dans la fenêtre **Avancé** qui s'affiche, cochez la case **Arrêter les appareils après la fin de la tâche**.

Limitation de la durée d'exécution de la tâche

Pour limiter la durée d'exécution de la tâche sur les appareils, procédez comme suit :

1. Dans la fenêtre des propriétés des tâches, sélectionnez la section **Programmation**.
2. Ouvrez la fenêtre destinée à la configuration des actions avec les appareils clients en cliquant sur le lien **Avancé**.
3. Dans la **Avancé** fenêtre qui s'ouvre, sélectionnez la case **Arrêter la tâche si elle prend plus de (min.)** et spécifiez l'intervalle de temps en minutes.

Finalement, Kaspersky Security Center arrêtera automatiquement l'exécution de la tâche si à l'issue du temps indiqué, l'exécution de la tâche ne se terminera pas sur l'appareil.

Exportation d'une tâche

Vous pouvez exporter les tâches de groupe et les tâches pour les ensembles d'appareils dans un fichier. Les tâches du Serveur d'administration ne sont pas disponibles à l'exportation.

Pour exporter une tâche, procédez comme suit :

1. Dans le menu contextuel de la tâche, choisissez l'option **Toutes les tâches → Exporter**.
2. Dans la fenêtre **Enregistrer sous** qui s'ouvre, indiquez le nom du fichier et le chemin d'accès pour l'enregistrement.
3. Cliquez sur **Enregistrer**.

Les privilèges des utilisateurs locaux ne sont pas exportés.

Importation d'une tâche

Vous pouvez importer les tâches de groupe et les tâches pour l'ensemble d'appareils. Les tâches du Serveur d'administration ne peuvent pas être importées.

Pour importer une tâche, procédez comme suit :

1. Sélectionnez la liste dans laquelle il faut importer la tâche :
   - Si vous voulez importer la tâche dans la liste des tâches de groupe, dans l'espace de travail du groupe d'administration concerné, sélectionnez l'onglet **Tâches**.
   - Si vous voulez importer une tâche dans la liste des tâches pour un ensemble d'appareils, sélectionnez le dossier **Tâches** dans l'arborescence de la console.
2. Sélectionnez un des moyens suivants d'importation de la tâche :
   - Dans le menu contextuel de la liste des tâches, sélectionnez **Toutes les tâches** → **Importer**.
   - Cliquez sur le lien **Importer une tâche à partir d'un fichier** dans le bloc de gestion de la liste des tâches.
3. Dans la fenêtre qui s'ouvre, indiquez le chemin d'accès au fichier depuis lequel vous souhaitez importer la tâche.
4. Cliquez sur **Ouvrir**.

   Suite à l'importation, la tâche s'affiche dans la liste des tâches.

Si la tâche importée porte le même nom qu'une tâche existante, le nom de la tâche importée est suivi de l'index **(<numéro de séquence suivant>)**, par exemple : **(1)**, **(2)**.

Conversion des tâches

Kaspersky Security Center permet de convertir les tâches des versions précédentes des applications Kaspersky en tâches des versions actuelles des applications.

La conversion est possible pour les tâches des applications suivantes :

- Kaspersky Anti-Virus 6.0 for Windows Workstations MP4
- Kaspersky Endpoint Security 8 for Windows
- Kaspersky Endpoint Security 10 for Windows

Pour convertir les tâches, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le Serveur d'administration pour lequel vous voulez convertir les tâches.
2. Dans le menu contextuel du Serveur d'administration, sélectionnez **Toutes les tâches** → **Assistant de conversion de masse des stratégies et des tâches**.

Ensuite, l'Assistant de conversion de masse des stratégies et des tâches démarre. Suivez les instructions de l'assistant.

Finalement l'Assistant forme des nouvelles tâches qui utilisent les paramètres des tâches des versions précédentes des applications.

Démarrage et arrêt manuels des tâches

Les tâches peuvent être lancées et arrêtées par deux moyens : à partir du menu contextuel de tâches et dans la fenêtre de propriétés de l'appareil client auquel la tâche est affectée.

Seuls les **utilisateurs qui appartiennent au groupe KLAdmins** peuvent lancer des tâches de groupe via le menu contextuel de l'appareil.

Pour lancer ou arrêter une tâche via le menu contextuel ou la fenêtre des propriétés, procédez comme suit :

1. Sélectionnez une tâche dans la liste des tâches.
2. Lancez ou arrêtez la tâche à l'aide d'un des moyens suivants :
   - En sélectionnant l'option **Début** ou **Arrêter** dans le menu contextuel de la tâche.
   - En cliquant sur **Début** ou sur **Arrêter** dans la section **Général** de la fenêtre des propriétés de la tâche.

Pour lancer ou arrêter une tâche via le menu contextuel ou la fenêtre des propriétés de l'appareil client, procédez comme suit :

1. Sélectionnez l'appareil dans la liste des appareils.
2. Lancez ou arrêtez la tâche à l'aide d'un des moyens suivants :
   - Sélectionnez l'option **Toutes les tâches** → **Lancer la tâche** dans le menu contextuel de l'appareil. Sélectionnez la tâche pertinente dans la liste.

     La liste des appareils auxquels la tâche a été affectée se trouvera dans l'appareil sélectionné. La tâche sera lancée.
   - En cliquant sur le bouton de démarrage ( ) ou sur le bouton d'arrêt ( ) dans la section **Tâches** de la fenêtre des propriétés de l'appareil.

Suspension et reprise manuelles d'une tâche

Pour suspendre ou reprendre l'exécution de la tâche lancée, procédez comme suit :

1. Sélectionnez une tâche dans la liste des tâches.
2. Suspendez ou reprenez l'exécution de la tâche à l'aide d'un des moyens suivants :
   - En sélectionnant, l'option **Pause** ou **Reprendre** dans le menu contextuel de la tâche.
   - En sélectionnant la section **Général** de la fenêtre des propriétés de la tâche, et en cliquant sur **Pause** ou sur **Reprendre**.

Suivi et affichage des comptes rendus d'activité des tâches

Pour surveiller l'exécution des tâches,

Dans la fenêtre des propriétés des tâches, sélectionnez la section **Général**.

L'état de la tâche actuelle est affiché dans la partie intermédiaire de la section **Général**.

Affichage de l'historique des tâches entreposé sur le Serveur d'administration

Kaspersky Security Center permet de consulter les résultats d'exécution des tâches de groupe, des tâches pour des ensembles d'appareils et des tâches du Serveur d'administration.

Pour consulter les résultats de l'exécution de la tâche, procédez comme suit :

1. Dans la fenêtre des propriétés de la tâche, sélectionnez la section **Général**.
2. Cliquez sur le lien **Résultats** pour ouvrir la fenêtre **Résultats de la tâche**.

Pour consulter les résultats des tâches d'un Serveur d'administration secondaire, procédez comme suit :

1. Dans la fenêtre des propriétés de la tâche, sélectionnez la section **Général**.
2. Cliquez sur le lien **Résultats** pour ouvrir la fenêtre **Résultats de la tâche**.
3. Cliquez sur **Statistiques des Serveurs secondaires**.
4. Sélectionnez le Serveur secondaire pour lequel vous souhaitez afficher la fenêtre **Résultats de la tâche**.

Configuration du filtre d'informations sur les résultats de l'exécution de la tâche

Kaspersky Security Center permet de filtrer les informations sur les résultats d'exécution des tâches de groupe, des tâches pour un ensemble d'appareils et des tâches du Serveur d'administration. Le filtrage n'est pas disponible pour les tâches locales.

Pour configurer le filtrage pour les informations sur les résultats de la tâche, procédez comme suit :

1. Dans la fenêtre des propriétés de la tâche, sélectionnez la section **Général**.
2. Cliquez sur le lien **Résultats** pour ouvrir la fenêtre **Résultats de la tâche**.

   Le tableau dans la partie supérieure de la fenêtre contient la liste de tous les appareils pour lesquels la tâche a été désignée. Le tableau de la partie inférieure de la fenêtre contient les résultats de l'exécution des tâches sur l'appareil sélectionné.
3. Dans le tableau qui vous intéresse, cliquez avec le bouton droit de la souris pour ouvrir le menu contextuel, puis sélectionnez **Filtre**.
4. Dans la fenêtre **Appliquer le filtre** qui s'ouvre, configurez les paramètres du filtre dans les sections **Événements**, **Appareils** et **Heure**. Cliquez sur le bouton **OK**.

Après cela, les informations qui vérifient les paramètres indiqués dans le filtre seront affichées dans la fenêtre **Résultats de la tâche**.

Modification d'une tâche. Restauration des modifications

Pour modifier une tâche, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le dossier **Tâches**.
2. Dans l'espace de travail du dossier **Tâches**, sélectionnez une tâche et ouvrez la fenêtre des propriétés de la tâche à l'aide du menu contextuel.
3. Apportez les modifications nécessaires.

   Dans la section **Exclusions de la zone d'action de la tâche**, il est possible de configurer la liste à laquelle la tâche n'est pas appliquée.
4. Cliquez sur le bouton **Appliquer**.

Les modifications apportées à la tâche seront enregistrées dans la fenêtre des propriétés de la tâche, dans la section **Historique des révisions**.

En cas de besoin, vous pouvez restaurer les modifications de la tâche.

Pour restaurer les modifications d'une tâche, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le dossier **Tâches**.
2. Sélectionnez la tâche dont il faut restaurer les modifications et ouvrez la fenêtre des propriétés de la stratégie à l'aide du menu contextuel.
3. Dans la fenêtre des propriétés des tâches, sélectionnez la section **Historique des révisions**.
4. Dans la liste des révisions de la tâche, sélectionnez le numéro de la révision pour laquelle il faut restaurer les modifications.
5. Cliquez sur le bouton **Avancé** et dans la liste déroulante, sélectionnez la valeur **Restaurer**.

Comparaison des tâches

Vous pouvez comparer les tâches d'un type, par exemple deux tâches Analyse des logiciels malveillants, mais il est impossible de comparer une tâche d'analyse des logiciels malveillants et une tâche d'installation de mises à jour. A l'issue de la comparaison des tâches, vous obtenez un rapport qui indique les équivalences et les différences entre les paramètres. Vous pouvez imprimer le rapport de comparaison des tâches ou l'enregistrer dans un fichier. La comparaison des tâches peut être utile quand il existe plusieurs tâches d'un même type dans différents départements d'une entreprise. Par exemple, il peut exister une tâche d'analyse des logiciels malveillants uniquement sur les disques locaux dans le service Comptabilité tandis que dans le service Commercial, qui communique avec les clients, la tâche peut porter non seulement sur les disques locaux, mais aussi sur l'email. Afin d'identifier rapidement les différences, il n'est pas nécessaire d'analyser tous les paramètres de la tâche. Il suffit de comparer les tâches.

La comparaison peut uniquement porter sur des tâches d'un même type.

Les tâches peuvent être comparées deux à la fois uniquement.

La comparaison de tâches peut s'opérer de deux manières : sélection d'une tâche et comparaison avec une autre ou comparaison de deux tâches d'une liste de tâches.

Pour choisir une tâche et la comparer à une autre, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le dossier **Tâches**.
2. Dans l'espace de travail du dossier **Tâches**, sélectionnez la tâche à comparer à une autre tâche.
3. Dans le menu contextuel de la tâche, stratégie, sélectionnez **Toutes les tâches → Comparer à une autre tâche**.
4. Dans la fenêtre **Sélection de la tâche**, sélectionnez la tâche à comparer.
5. Cliquez sur le bouton **OK**.

Le rapport sur la comparaison des deux tâches s'affiche au format HTML.

Pour comparer deux tâches de la liste des tâches, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le dossier **Tâches**.
2. Dans le dossier **Tâches**, dans la liste des tâches, appuyez sur la touche **SHIFT** ou **CTRL** pour sélectionner deux tâches de même type.
3. Dans le menu contextuel, sélectionnez l'option **Comparer**.

Le rapport sur la comparaison des tâches sélectionnées s'affiche au format HTML.

Lors de la comparaison des tâches, si les mots de passe utilisés se distinguent, les symboles ****** s'affichent dans le rapport de comparaison des tâches.

Si le mot de passe a été modifié dans les propriétés de la tâche, les symboles ****** s'affichent dans le rapport de comparaison de révision des tâches.

Comptes utilisateur pour le lancement des tâches

Vous pouvez indiquer le compte utilisateur sous lequel la tâche doit être lancée.

Par exemple, pour une tâche d'analyse à la demande, il faut avoir un droit d'accès à l'objet analysé, tandis que pour une tâche de mise à jour, il faut des droits d'utilisateur autorisé sur serveur proxy. Ceci permet d'éviter des erreurs lors de l'exécution de tâches d'analyse à la demande ou de mise à jour si l'utilisateur lance une tâche sans jouir des privilèges nécessaires.

Dans les tâches d'installation et de désinstallation à distance de l'application, le compte utilisateur est utilisé pour télécharger sur les appareils clients des fichiers nécessaires pour l'installation (la suppression) si l'Agent d'administration n'est pas installé ou n'est pas accessible sur l'appareil. Si l'Agent d'administration est installé ou accessible, le compte utilisateur est utilisé si, selon les paramètres d'une tâche, la remise des fichiers s'effectue uniquement par les moyens de Microsoft Windows du dossier partagé. Dans ce cas le compte utilisateur doit posséder les droits sur l'appareil suivant :

- Le droit sur le lancement des applications à distance.
- Les droits sur une ressource Admin$.
- Le droit *Connexion en tant que service*.

Si l'Agent d'administration effectue la remise des fichiers sur les appareils, le compte utilisateur ne sera pas utilisé. L'Agent d'administration effectuera toutes les opérations de copie et d'installation des fichiers sous le compte utilisateur **Agent d'administration** (**compte LocalSystem**).

Exporter l'historique d'exécution des tâches

Si vous rencontrez des problèmes avec une tâche, vous devrez peut-être rechercher les raisons sous-jacentes. Pour ce faire, vous pouvez exporter et analyser plus en détail l'historique d'exécution des tâches.

Pour exporter l'historique d'exécution des tâches :

1. Créez un fichier TXT vide dans un répertoire de votre appareil.

   L'historique d'exécution des tâches sera exporté dans ce fichier.

2. Ouvrez la fenêtre des résultats de la tâche.

3. Dans la partie supérieure de la fenêtre des résultats de la tâche, sélectionnez l'appareil qui présente des problèmes.

4. Dans la partie inférieure de la fenêtre des résultats de la tâche, où s'affiche l'historique de l'exécution pour l'appareil sélectionné, sélectionnez un ou plusieurs événements.

   Pour sélectionner plusieurs événements, utilisez la touche **Shift** ou **Ctrl**.

5. Faites un clic droit sur le ou les événements sélectionnés pour ouvrir le menu contextuel et sélectionnez **Exporter**.

   L'Assistant d'exportation des événements démarre.

6. À l'étape **Fichier d'exportation** de l'assistant, cliquez sur le bouton **Parcourir**, puis sélectionnez le fichier TXT que vous avez créé pour exporter l'historique d'exécution des tâches.

   Si vous souhaitez exporter uniquement les événements sélectionnés, activez l'option **Exporter uniquement les événements sélectionnés**.

   Si vous souhaitez exporter l'intégralité de l'historique d'exécution des tâches (tous les événements), l'option **Exporter uniquement les événements sélectionnés** doit être désactivé.

7. Cliquez sur le bouton **Suivant**.

8. À l'étape **Type d'exportation** de l'assistant, activez l'une des options suivantes :

   - **Exporter au format UNICODE séparé par des tabulations**

     Activez cette option si les données exportées comprennent des caractères spéciaux et des symboles de plusieurs langues et que vous devez vous assurer que tous les caractères sont préservés avec précision lorsque le fichier TXT contenant les données exportées est ouvert dans différentes applications.

   - **Exporter au format texte séparé par des tabulations**

     Activez cette option si vous souhaitez maintenir la compatibilité avec des systèmes ou des applications plus anciens qui peuvent ne pas prendre en charge le standard Unicode.

9. Cliquez sur le bouton **Suivant** pour fermer l'Assistant.

L'historique d'exécution des tâches est exporté vers le fichier TXT sélectionné.

Assistant de modification du mot de passe des tâches

Pour une tâche non locale, vous pouvez spécifier un compte sous lequel la tâche doit être exécutée. Vous pouvez spécifier le compte lors de la création de la tâche ou dans les propriétés d'une tâche existante. Si le compte spécifié est utilisé conformément aux instructions de sécurité de l'organisation, ces instructions peuvent nécessiter périodiquement le changement du mot de passe du compte. Lorsque le mot de passe du compte expire et que vous en définissez un nouveau, les tâches ne démarrent pas tant que vous n'avez pas spécifié le nouveau mot de passe valide dans les propriétés de la tâche.

L'Assistant de modification du mot de passe des tâches vous permet de remplacer automatiquement l'ancien mot de passe par le nouveau dans toutes les tâches dans lesquelles le compte est spécifié. Vous pouvez également le modifier manuellement dans les propriétés de chaque tâche.

Pour démarrer l'Assistant de modification du mot de passe des tâches :

1. Dans l'arborescence de la console, sélectionnez le nœud **Tâches**.
2. Dans le menu contextuel du nœud, sélectionnez l'option **Assistant de modification du mot de passe des tâches**.

Suivez les instructions de l'assistant.

Étape 1. Spécification des informations d'identification

Dans les champs **Compte utilisateur** et **Mot de passe**, spécifiez les nouvelles informations d'identification valides dans votre système (par exemple, dans Active Directory). Lorsque vous passez à l'étape suivante de l'assistant, Kaspersky Security Center vérifie si le nom de compte spécifié correspond au nom de compte dans les propriétés de chaque tâche non locale. Si les noms de compte correspondent, le mot de passe dans les propriétés de la tâche sera automatiquement remplacé par le nouveau.

Si vous remplissez le champ **Ancien mot de passe (facultatif)**, Kaspersky Security Center remplace uniquement le mot de passe pour les tâches dans lesquelles se trouvent le nom de compte et l'ancien mot de passe. Le remplacement est effectué automatiquement. Dans tous les autres cas, vous devez choisir une action à entreprendre à l'étape suivante de l'assistant.

Étape 2. Sélection d'une action à entreprendre

Si vous n'avez pas indiqué l'ancien mot de passe à la première étape de l'Assistant ou si l'ancien mot de passe indiqué ne correspond pas aux mots de passe dans les tâches, vous devez choisir une action à entreprendre pour les tâches trouvées.

Pour chaque tâche ayant un état de *Approbation exigée*, décidez si vous souhaitez supprimer le mot de passe dans les propriétés de la tâche ou le remplacer par le nouveau. Si vous choisissez de supprimer le mot de passe, la tâche est indiquée comme devant s'exécuter sous le compte par défaut.

Étape 3. Affichage des résultats

À la dernière étape de l'assistant, consultez les résultats pour chacune des tâches trouvées. Cliquez sur **Terminer** pour terminer le travail de l'Assistant.

Création d'une hiérarchie des groupes d'administration soumis au Serveur d'administration virtuel

Après la création du Serveur d'administration virtuel, il contient, par défaut, un groupe d'administration **Appareils administrés**.

La procédure de création de la hiérarchie des groupes d'administration, soumis au Serveur d'administration virtuel, coïncide avec la procédure de création de la hiérarchie des groupes d'administration, soumis au Serveur d'administration physique.

Il est impossible d'ajouter les Serveurs d'administration virtuels et secondaires aux groupes d'administration soumis à un Serveur d'administration virtuel. Ceci est dû aux restrictions des Serveurs d'administration virtuels.

Stratégies et profils de stratégie

Kaspersky Security Center Web Console permet de créer des stratégies pour des applications de Kaspersky. Cette section décrit les stratégies et les profils de stratégie et explique comment les créer et les modifier.

Hiérarchie des stratégies, utilisation des profils de stratégie

Cette section contient des informations sur les particularités de l'application de stratégies aux appareils dans les groupes d'administration. Cette section fournit également des informations sur les profils de stratégie.

Hiérarchie des stratégies

Dans Kaspersky Security Center, les stratégies servent à appliquer un ensemble de valeurs de paramètres identiques à plusieurs appareils. Par exemple, la zone d'action de la stratégie de l'application A définie pour le groupe G reprend les appareils administrés dotés de l'application A et situés dans le groupe d'administration G et l'ensemble de ses sous-groupes, à l'exception des sous-groupes dans les propriétés desquels la case **Hériter du groupe parent** est décochée.

La stratégie se distingue des paramètres locaux par la présence de cadenas (🔒) en regard des paramètres qu'elle contient. Un cadenas fermé dans les propriétés de la stratégie signifie que le paramètre (ou le groupe de paramètres) correspondant doit, premièrement, être utilisé dans la composition des paramètres effectifs et, deuxièmement, être inscrit dans la stratégie de niveau inférieur.

La définition des paramètres actifs sur l'appareil peut être représentée de la manière suivante : les valeurs des paramètres sans " cadenas " sont tirées de la stratégie, elles sont écrasées par les valeurs des paramètres locaux, puis les valeurs récupérées sont écrasées par les valeurs des paramètres avec cadenas extraites de la stratégie.

Les stratégies d'une même application agissent les unes sur les autres en fonction de la hiérarchie des groupes d'administration : les paramètres avec cadenas fermé de la stratégie supérieure sont appliqués aux paramètres du même nom de la stratégie inférieure.

Il existe un type particulier de stratégie : la stratégie pour les utilisateurs itinérants. Cette stratégie entre en vigueur sur l'appareil quand celui-ci passe au mode de l'utilisateur autonome. Les stratégies pour les utilisateurs autonomes n'agissent pas sur les autres stratégies selon la hiérarchie des groupes d'administration.

Profils de stratégie

Dans de nombreux cas, l'application de stratégies à des appareils sur la seule base de la hiérarchie des groupes d'administration n'est pas pratique. La nécessité de créer plusieurs copies de stratégies, qui se distinguent par un ou deux paramètres, dans différents groupes d'administration peut se présenter, avec la synchronisation manuelle ultérieure du contenu de ces stratégies.

Pour éviter ce type de problèmes, Kaspersky Security Center prend en charge les *profils de stratégie*. Un profil de stratégie est un sous-ensemble nommé de paramètres de stratégie. Ce sous-ensemble est diffusé sur les appareils avec la stratégie et vient compléter la stratégie quand une condition définie, la *condition d'activation du profil*, est remplie. Les profils contiennent uniquement les paramètres qui se distinguent de la stratégie " de base " en vigueur sur l'appareil client (ordinateur, appareil mobile). Quand le profil est activé, les paramètres de la stratégie en vigueur sur l'appareil avant l'activation du profil sont modifiés. Ces paramètres prennent alors les valeurs reprises dans le profil.

Les profils de stratégie possèdent maintenant les restrictions suivantes :

- Une stratégie ne peut pas compter plus de 100 profils.
- Un profil de stratégie ne peut pas contenir d'autres profils.
- Un profil de stratégie ne peut pas contenir des paramètres de notification.

Composition d'un profil

Un profil de stratégie contient les parties suivantes :

- Nom. Les profils qui portent le même nom agissent les uns sur les autres selon la hiérarchie des groupes d'administration avec des règles générales.
- Sous-ensemble de paramètres d'une stratégie. À la différence d'une stratégie qui contient tous les paramètres, un profil reprend uniquement les paramètres qui sont vraiment nécessaires (le cadenas est activé).
- La condition d'activation est une expression logique avec les propriétés de l'appareil. Le profil est actif (complète la stratégie) uniquement quand la condition d'activation du profil se vérifie. Dans les autres cas, le profil est inactif et est ignoré. Les propriétés suivantes de l'appareil peuvent intervenir dans l'expression logique :
  - état du mode de l'utilisateur autonome ;
  - propriétés de l'environnement réseau : nom de la règle active de connexion de l'Agent d'administration ;
  - présence ou absence sur l'appareil des tags indiqués ;
  - emplacement de l'appareil dans les sous-divisions Active Directory : explicite (l'appareil se trouve directement dans la sous-division indiquée) ou implicite (l'appareil se trouve dans la sous-division qui se trouve à l'intérieur de la sous-division indiquée à n'importe quel niveau d'imbrication) ;
  - appartenance de l'appareil au groupe de sécurité Active Directory (explicite ou implicite) ;
  - appartenance du propriétaire de l'appareil au groupe de sécurité Active Directory (explicite ou implicite).

- Case de désactivation du profil. Les profils désactivés sont toujours ignorés, les conditions d'activation ne sont pas vérifiées.

- Priorité du profil. Les conditions d'activation des profils sont indépendantes, c'est pourquoi plusieurs profils peuvent s'activer simultanément. Si les profils actifs contiennent les ensembles de paramètres qui ne se recoupent pas, aucun problème ne se présente. Mais si deux profils actifs contiennent des valeurs différentes pour un même paramètre, il y a une ambiguïté. L'ambiguïté se résout à l'aide des priorités des profils : la valeur adoptée dans ce cas est celle du profil qui affiche la priorité supérieure (le profil qui se trouve plus haut dans la liste des profils).

Comportement des profils dans le cadre de l'action des stratégies les unes sur les autres selon la hiérarchie

Les profils homonymes sont rassemblés selon les règles du groupement de stratégies. Les profils de stratégie supérieure ont une priorité supérieure à celle des profils de la stratégie inférieure. Si la modification des paramètres est interdite (cadenas activé) dans la stratégie supérieure, la stratégie inférieure utilise les conditions d'activation de la stratégie supérieure. Si la modification des paramètres est autorisée dans la stratégie supérieure, ce sont les conditions d'activation du profil de stratégie inférieure qui sont utilisées.

Puisque le profil de stratégie peut contenir la propriété **Appareil en mode déconnecté** dans la condition de l'activation, les profils remplacent complètement la fonction des stratégies pour les utilisateurs itinérants qui ne va plus être prise en charge à l'avenir.

La stratégie pour les utilisateurs itinérants peut contenir des profils, mais l'activation de ses profils ne peut pas se produire avant que l'appareil ne passe au mode de l'utilisateur autonome.

Héritage des paramètres d'une stratégie

Une stratégie est définie pour un groupe d'administration. Les paramètres d'une stratégie peuvent être *hérités*, à savoir appliqués aux sous-groupes (groupes enfant) du groupe d'administration pour lequel elle a été créée. Par la suite, une stratégie pour un groupe parent est également désignée par l'expression *stratégie parent*.

Vous pouvez activer ou désactiver deux options d'héritage : **Hériter des paramètres de la stratégie parent** et **Imposer l'héritage des paramètres aux stratégies enfants** :

- Si vous activez l'option **Hériter des paramètres de la stratégie parent** pour une stratégie enfant et verrouillez certains paramètres dans la stratégie parent, vous ne pourrez alors pas modifier ces paramètres pour le groupe enfant. Toutefois, vous pouvez modifier les valeurs pour les paramètres qui ne sont pas verrouillés dans la politique parent.

- Si vous désactivez l'option **Hériter des paramètres de la stratégie parent** pour une stratégie enfant, vous pouvez modifier tous les paramètres dans le groupe enfant, même si certains paramètres sont verrouillés dans la stratégie parent.

- Si vous activez l'option **Imposer l'héritage des paramètres aux stratégies enfants** dans le groupe parent, cela active **l'héritage des paramètres de la stratégie parent** pour chaque stratégie enfant. Dans ce cas, vous ne pouvez désactiver cette option pour aucune stratégie enfant. Tous les paramètres verrouillés dans la stratégie parent sont hérités par force dans les groupes enfants et ne sont plus modifiables.

- Dans les stratégies du groupe **Appareils administrés**, **l'héritage des paramètres de la stratégie parent** n'affecte aucun paramètre, car le groupe **Appareils administrés** ne comporte aucun groupe en amont et n'hérite donc d'aucune stratégie.

Par défaut, l'option **Hériter des paramètres de la stratégie parent** est activée pour une nouvelle stratégie.

Si une stratégie possède des profils, toutes les stratégies enfants héritent de ces profils.

Administration des stratégies

La configuration centralisée des paramètres des applications installées sur les appareils clients s'opère à l'aide de la définition de stratégies.

Les stratégies créées pour les applications dans le groupe d'administration s'affichent dans l'espace de travail, sur l'onglet **Stratégies**. Une icône figure devant le nom de chaque stratégie et caractérise son état.

Après la suppression d'une stratégie ou la fin de ses effets, l'application continue à fonctionner selon les paramètres définis dans la stratégie. Par la suite, il est possible de modifier ces paramètres à la main.

L'application d'une stratégie se déroule de la manière suivante : si des tâches résidentes (tâches de protection en temps réel) sont exécutées sur l'appareil, leur exécution est poursuivie avec les nouvelles valeurs des paramètres. Les tâches lancées périodiquement (analyse à la demande, mise à jour des bases de données de l'application) sont exécutées avec les valeurs non modifiées. Le nouveau lancement des tâches périodiques est exécuté avec les valeurs modifiées des paramètres.

Les stratégies pour les applications qui prennent en charge l'architecture mutualisée sont transmises par héritage aux groupes d'administration de niveau inférieur ainsi qu'aux groupes d'administration de niveau supérieur : la stratégie est diffusée sur tous les appareils clients sur lesquels l'application est installée.

Dans le cas d'utilisation de la structure hiérarchique des Serveurs d'administration, les Serveurs secondaires récupèrent les stratégies du Serveur d'administration principal et les diffusent vers les appareils clients. Quand le mode d'héritage est activé, les paramètres de la stratégie peuvent être modifiés sur le Serveur d'administration principal. Après cela, les modifications apportées dans les paramètres d'une stratégie se diffusent sur les stratégies héritées des Serveurs d'administration secondaires.

En cas de perte de la connexion entre les Serveurs d'administration principal et secondaire, la stratégie sur le Serveur secondaire continue de fonctionner selon les paramètres précédents. Les paramètres modifiés dans la stratégie sur le Serveur d'administration principal sont propagés vers le Serveur d'administration secondaire une fois que la connexion a été rétablie.

Lorsque le mode d'héritage est désactivé, les paramètres de la stratégie peuvent être modifiés sur le Serveur d'administration secondaire indépendamment du Serveur d'administration principal.

En cas de déconnexion entre le Serveur d'administration et l'appareil client, la stratégie pour les utilisateurs autonomes (si elle a été définie) entre en vigueur sur l'appareil, ou la stratégie continue de fonctionner selon les paramètres précédents jusqu'au rétablissement de la connexion.

Les résultats de la diffusion de la stratégie sur les Serveurs d'administration secondaires figurent dans la fenêtre des propriétés de la stratégie sur le Serveur d'administration principal.

Les résultats de diffusion de la stratégie sur les appareils clients s'affichent dans la fenêtre des propriétés de la stratégie du Serveur d'administration auquel ils sont connectés.

N'utilisez pas de données confidentielles dans les paramètres d'une stratégie. Par exemple, le mot de passe de l'administrateur de domaine.

Création d'une stratégie

Dans la Console d'administration, il est possible de créer des stratégies directement dans le dossier du groupe d'administration pour lequel la stratégie est créée et dans l'espace de travail du dossier **Stratégies**.

Pour créer une stratégie dans le dossier du groupe d'administration, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le groupe d'administration pour lequel il faut créer une stratégie.
2. Dans l'espace de travail du groupe, sélectionnez l'onglet **Stratégies**.
3. Lancez l'Assistant de création de la stratégie en cliquant sur le bouton **Nouvelle stratégie**.

   L'Assistant de création de la stratégie démarre. Suivez les instructions de l'assistant.

*Pour créer une stratégie dans l'espace de travail du dossier **Stratégies**, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le dossier **Stratégies**.
2. Lancez l'Assistant de création de la stratégie en cliquant sur le bouton **Nouvelle stratégie**.

   L'Assistant de création de la stratégie démarre. Suivez les instructions de l'assistant.

Il est possible de créer de nombreuses stratégies pour une application, mais une seule d'entre elles peut être celle active. Lors de la création d'une nouvelle stratégie effective, la stratégie active précédente devient inactive.

Lors de la création de la stratégie, il est possible de configurer un ensemble minimal des paramètres sans lesquels l'application ne fonctionnera pas. Tous les autres paramètres prendront les valeurs par défaut correspondantes à celles définies lors de l'installation locale de l'application. Vous pouvez modifier la stratégie après sa création.

N'utilisez pas de données confidentielles dans les paramètres d'une stratégie. Par exemple, le mot de passe de l'administrateur de domaine.

Les paramètres des applications Kaspersky, qui se modifient après l'application des stratégies, sont décrits en détails dans les documentations correspondantes.

Après la création de la stratégie, les paramètres verrouillés (avec un cadenas (🔒)) commencent à agir sur les appareils clients quels que soient les paramètres définis auparavant pour l'application.

Affichage des stratégies héritées dans le groupe imbriqué

Pour activer l'affichage des stratégies héritées pour le groupe d'administration imbriqué, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le groupe d'administration pour lequel il faut afficher les stratégies héritées.
2. Dans l'espace de travail du groupe sélectionné, ouvrez l'onglet **Stratégies**.
3. Dans le menu contextuel de la liste des stratégies, sélectionnez l'option **Affichage → Stratégies héritées**.

Ainsi, les stratégies héritées s'affichent dans la liste des stratégies avec l'icône :

- : si elles ont été héritées du groupe créé sur le Serveur d'administration primaire.
- : si elles ont été héritées d'un groupe de niveau supérieur.

Lorsque le mode d'héritage des paramètres est activé, la modification des stratégies héritées n'est possible que dans les groupes où elles ont été créées. La modification de stratégies héritées n'est pas disponible dans le groupe qui hérite les stratégies.

Activation d'une stratégie

Pour activer une stratégie pour le groupe sélectionné, procédez comme suit :

1. Dans l'espace de travail du groupe, sous l'onglet **Stratégies**, sélectionnez la stratégie à activer.
2. Pour activer une stratégie, exécutez une des actions suivantes :
   - Dans le menu contextuel de la stratégie, sélectionnez l'option **Stratégie active**.
   - Dans la fenêtre des propriétés de la stratégie, ouvrez la section **Général**, puis sélectionnez l'option **Stratégie active** dans le groupe des paramètres **État de la stratégie**.

Finalement, la stratégie devient active pour le groupe d'administration sélectionné.

Tout changement de stratégie réalisé simultanément sur un grand nombre d'appareils clients augmente considérablement la charge du Serveur d'administration ainsi que le volume du trafic réseau.

Activation automatique d'une stratégie lors d'un événement " Propagation de virus "

Pour que la stratégie soit automatiquement activée lors d'un événement " Attaque de virus ", procédez comme suit :

1. Dans la fenêtre des propriétés du Serveur d'administration, ouvrez la section **Attaque de virus**.
2. Ouvrez la fenêtre **Activation des stratégies** en cliquant sur le lien **Configurer l'activation des stratégies dans le cas d'un événement Attaque de virus**, puis ajoutez la stratégie à la liste sélectionnée de stratégies activées en cas d'attaque de virus.

Si vous désactivez la stratégie en fonction de l'événement *Attaque de virus*, vous ne pouvez rétablir la stratégie précédente que manuellement.

Application des stratégies pour les utilisateurs autonomes

La stratégie pour les utilisateurs autonomes entre en vigueur sur l'appareil dans le cas de déconnexion du réseau d'entreprise.

Pour appliquer une stratégie pour les utilisateurs autonomes, procédez comme suit :

Dans la fenêtre des propriétés de la stratégie, ouvrez la section **Général** et, dans le groupe de paramètres **État de la stratégie**, sélectionnez **Stratégie pour les utilisateurs autonomes**.

La stratégie pour les utilisateurs autonomes commence à agir sur les appareils dans le cas de leur déconnexion du réseau d'entreprise.

Modification d'une stratégie. Restauration des modifications

Pour modifier une stratégie, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le dossier **Stratégies**.
2. Dans l'espace de travail du dossier **Stratégies**, sélectionnez une stratégie et accédez à la fenêtre des propriétés de la stratégie à l'aide du menu contextuel.
3. Apportez les modifications nécessaires.
4. Cliquez sur le bouton **Appliquer**.

Les modifications de la stratégie seront enregistrées dans les propriétés de la stratégie, dans la section **Historique des révisions**.

En cas de besoin, vous pouvez restaurer les modifications de la stratégie.

Pour restaurer les modifications de la stratégie, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le dossier **Stratégies**.
2. Sélectionnez la stratégie dont vous souhaitez restaurer les modifications et ouvrez la fenêtre des propriétés de la stratégie à l'aide du menu contextuel.
3. Dans la fenêtre des propriétés de la stratégie, sélectionnez la section **Historique des révisions**.
4. Dans la liste des révisions de la stratégie, sélectionnez le numéro de révision dont il faut restaurer les modifications.
5. Cliquez sur le bouton **Avancé** et dans la liste déroulante, sélectionnez la valeur **Restaurer**.

Comparaison des stratégies

Vous pouvez comparer deux stratégies pour une seule application administrée. A l'issue de la comparaison des stratégies, vous obtenez un rapport qui indique les équivalences et les différences entre les paramètres. La comparaison de stratégie peut s'imposer quand, par exemple, différents administrateurs ont créé localement plusieurs stratégies pour une application administrée ou quand une stratégie parent a été héritée et modifiée pour chaque bureau local. La comparaison de stratégies peut s'opérer de deux manières : sélection d'une stratégie et comparaison avec une autre ou comparaison de deux stratégies d'une liste de stratégies.

Vous pouvez uniquement comparer des stratégies dont les révisions sont en cours dans l'historique des révisions.

Pour comparer une stratégie à une autre, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le dossier **Stratégies**.
2. Dans l'espace de travail du dossier **Stratégies**, sélectionnez la stratégie à comparer à une autre stratégie.
3. Dans le menu contextuel de la stratégie, sélectionnez l'option **Comparer la stratégie à une autre stratégie**.
4. Dans la fenêtre **Sélection de stratégie**, sélectionnez la stratégie avec laquelle la comparaison doit être effectuée.
5. Cliquez sur le bouton **OK**.

Le rapport sur la comparaison des deux stratégies pour l'application s'affiche au format HTML.

Pour comparer deux stratégies de la liste des stratégies, procédez comme suit :

1. Dans le dossier **Stratégies**, dans la liste des stratégies, utilisez les touches **SHIFT** ou **CTRL** pour sélectionner deux stratégies pour une seule application administrée.
2. Dans le menu contextuel, sélectionnez l'option **Comparer**.

Le rapport sur la comparaison des deux stratégies pour l'application s'affiche au format HTML.

Le rapport de la comparaison des paramètres de stratégies pour l'application Kaspersky Endpoint Security for Windows contient aussi une comparaison des profils de stratégie. Il est possible de réduire l'affichage des résultats de la comparaison des paramètres des profils de stratégie. Pour cela, cliquez sur l'icône flèche ( ) en regard du nom du groupe.

Affichage du graphique de l'état de la distribution des stratégies

Kaspersky Security Center vous permet de consulter les résultats de l'application des stratégies sur chaque appareil.

Pour afficher l'état de la distribution des stratégies sur chaque appareil, procédez comme suit :

1. Dans l'espace de travail du groupe, sous l'onglet **Stratégies**, sélectionnez la stratégie dont vous souhaitez consulter l'état de distribution.

   Le graphique dans le volet droit affiche une vue d'ensemble de l'application des stratégies.

2. Cliquez sur **En savoir plus**.

   La fenêtre **Résultats de l'application de la stratégie** s'ouvre.

   Vous pouvez exporter les résultats de l'application de la stratégie dans un fichier CSV ou TXT.

Suppression d'une stratégie

Pour supprimer une stratégie, procédez comme suit :

1. Dans l'espace de travail du groupe d'administration, sous l'onglet **Stratégies**, sélectionnez la stratégie que vous souhaitez supprimer.

2. Supprimez la stratégie à l'aide d'un des moyens suivants :

   - En sélectionnant **Supprimer** dans le menu contextuel de la stratégie.
   - En cliquant sur le lien **Supprimer la stratégie** dans la zone d'informations correspondant à la stratégie sélectionnée.

Copie d'une stratégie

Pour copier une stratégie, procédez comme suit :

1. Dans l'espace de travail du groupe requis, sous l'onglet **Stratégies**, sélectionnez une stratégie.

2. Dans le menu contextuel de la stratégie, sélectionnez l'option **Copier**.

3. Sélectionnez dans l'arborescence de la console le groupe à ajouter une stratégie.

   La stratégie peut être ajoutée dans le groupe depuis lequel elle a été copiée.

4. Dans le menu contextuel de la liste des stratégies pour le groupe sélectionné, sous l'onglet **Stratégies**, sélectionnez l'option **Coller**.

La stratégie est copiée avec tous les paramètres et elle est diffusée sur tous les appareils du groupe où elle a été déplacée. Si vous insérez la stratégie dans le groupe depuis lequel elle a été copiée, le suffixe de type **(<next sequence number>)** s'ajoute automatiquement au nom de la stratégie, par exemple : **(1)**, **(2)**.

Une stratégie active devient inactive lors de la copie. Le cas échéant, vous pouvez en faire une stratégie active.

Exportation d'une stratégie

Pour exporter une stratégie, procédez comme suit :

1. Exportez la stratégie à l'aide d'un des moyens suivants :
   - En sélectionnant l'option **Toutes les tâches** → **Exporter** dans le menu contextuel de la stratégie.
   - A l'aide du lien **Exporter la stratégie dans le fichier** dans la zone d'informations de la stratégie sélectionnée.
2. Dans la fenêtre **Enregistrer sous** qui s'ouvre, indiquez le nom du fichier de la stratégie et le chemin d'accès pour son enregistrement. Cliquez sur **Enregistrer**.

Importation d'une stratégie

Pour importer une stratégie, procédez comme suit :

1. Dans l'espace de travail du groupe pertinent, sous l'onglet **Stratégies**, sélectionnez un des moyens d'importation de la stratégie suivants :
   - Dans le menu contextuel de la liste des stratégies, sélectionnez l'option **Toutes les tâches** → **Importer**.
   - En cliquant sur le lien **Importer une stratégie à partir d'un fichier** dans le bloc d'administration de la liste de stratégie.
2. Dans la fenêtre qui s'ouvre, indiquez le chemin d'accès au fichier depuis lequel vous souhaitez importer la stratégie. Cliquez sur **Ouvrir**.

La stratégie importée s'affiche dans la liste des stratégies. Les paramètres et les profils de la stratégie sont également importés. Quel que soit l'état de la stratégie sélectionné lors de l'exportation, la stratégie importée est inactive. Vous pouvez modifier l'état de la stratégie dans les propriétés de la stratégie.

Si la stratégie importée porte le même nom que la stratégie existante, le nom de la stratégie importée est suivi de l'index **(<numéro de séquence suivant>)**, par exemple : **(1)**, **(2)**.

Conversion des stratégies

Kaspersky Security Center peut convertir les stratégies des versions antérieures des applications Kaspersky administrées en versions à jour des mêmes applications. Les stratégies converties conservent les paramètres actuels de l'administrateur définis avant la mise à jour et incluent les nouveaux paramètres des versions à jour des applications. Si une stratégie est convertie vers une version à jour d'une application Kaspersky administrée, vous ne pouvez pas ouvrir la stratégie sur un Serveur d'administration sur lequel une version antérieure du plug-in de l'application est installée. Les plug-ins d'administration pour les applications de Kaspersky déterminent si la conversion est disponible pour les stratégies de ces applications. Pour plus d'informations sur la conversion des stratégies pour chaque application Kaspersky prise en charge, consultez l'aide correspondante dans la liste suivante :

- **Applications Kaspersky pour postes de travail :**
  - Kaspersky Endpoint Security for Windows
  - Kaspersky Endpoint Security for Linux
  - Kaspersky Endpoint Security for Linux Elbrus Edition
  - Kaspersky Endpoint Security for Mac
  - Kaspersky Endpoint Agent
  - Kaspersky Embedded Systems Security for Windows
- **Kaspersky Industrial CyberSecurity :**
  - Kaspersky Industrial CyberSecurity for Nodes
  - Kaspersky Industrial CyberSecurity for Linux Nodes
  - Kaspersky Industrial CyberSecurity for Networks (le déploiement centralisé n'est pas pris en charge)
- **Applications Kaspersky pour appareils mobiles :**
  - Kaspersky Endpoint Security for Android
  - Kaspersky Security for iOS
- **Applications Kaspersky pour serveurs de fichiers :**
  - Kaspersky Security for Windows Server
  - Kaspersky Endpoint Security for Windows
  - Kaspersky Endpoint Security for Linux
- **Applications Kaspersky pour machines virtuelles :**
  - Kaspersky Security for Virtualization Light Agent
  - Kaspersky Security for Virtualization Agentless

- **Applications Kaspersky pour les systèmes de messagerie et les serveurs SharePoint/de collaboration :**
  - Kaspersky Security for Linux Mail Server
  - Kaspersky Security for Microsoft Exchange Servers
- **Applications Kaspersky pour la détection des attaques ciblées :**
  - Kaspersky Sandbox
  - Kaspersky Endpoint Detection and Response Optimum
  - Kaspersky Managed Detection and Response
- **Applications Kaspersky pour appareils KasperskyOS :**
  - Kaspersky IoT Secure Gateway
  - Kaspersky Security Management Suite (plug-in pour Kaspersky Thin Client)

Pour convertir les stratégies, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le Serveur d'administration pour lequel vous voulez convertir les stratégies.
2. Dans le menu contextuel du Serveur d'administration, sélectionnez **Toutes les tâches** → **Assistant de conversion de masse des stratégies et des tâches**.

   Ensuite, l'Assistant de conversion de masse des stratégies et des tâches démarre. Suivez les instructions de l'assistant.

Une fois que l'Assistant a terminé, de nouvelles stratégies sont créées qui utilisent les paramètres des stratégies de l'administrateur actuel et les nouveaux paramètres des versions à jour des applications de Kaspersky.

Administration des profils de stratégies

Un profil de stratégie est un ensemble de paramètres nominatif d'une stratégie qui est activé sur un appareil client (ordinateur ou appareil mobile) si l'appareil répond aux règles d'activation définies. Quand le profil est activé, les paramètres de la stratégie en vigueur sur l'appareil avant l'activation du profil sont modifiés. Ces paramètres prennent alors les valeurs reprises dans le profil.

Les profils de stratégie sont nécessaires pour que les appareils à l'intérieur d'un groupe d'administration puissent avoir différents paramètres de stratégie. Par exemple, lorsque quand dans le groupe d'administration de certains appareils, les paramètres de la stratégie doivent être modifiés. Dans ce cas, pour cette stratégie, il est possible de configurer des profils de stratégie dont l'utilisation permet de modifier les paramètres de la stratégie seulement pour certains appareils du groupe d'administration. Par exemple, la stratégie interdit le applications des programmes de navigation urbaine pour tous les appareils du groupe d'administration « Utilisateurs ». Les applications de navigation urbaine sont seulement nécessaires au fonctionnement d'un appareil de l'utilisateur jouant le rôle de livreur, dans le groupe d'administration « Utilisateurs ». Sur cet appareil, il est possible de définir le tag « Livreur » et de configurer à nouveau le profil de stratégie pour autoriser le lancement des applications de navigation urbaine seulement sur l'appareil contenant le tag « Livreur », tout en conservant tous les autres paramètres de la stratégie. Dans ce cas, si dans le groupe d'administration « Utilisateurs », un appareil contient le tag « Livreur », le lancement des programmes de navigation urbaine y est autorisé. Le lancement des programmes de navigation urbaine sur d'autres appareils dans le groupe d'administration « Utilisateurs » qui ne contiennent pas le tag « Livreur » sera interdit.

Les profils sont pris en charge uniquement pour les stratégies suivantes :

- Stratégies de Kaspersky Endpoint Security for Windows
- Stratégies de Kaspersky Endpoint Security for Mac
- stratégies du plug-in d'administration des appareils mobiles de Kaspersky des versions 10 Service Pack 1 à 10 Service Pack 3 Maintenance Release 1
- stratégies du plug-in Kaspersky Device Management for iOS
- politiques de Kaspersky Security for Virtualization 5.1 Light Agent pour Windows
- politiques de Kaspersky Security for Virtualization 5.1 Light Agent pour Linux

Les profils de stratégie simplifient l'administration des appareils clients sur lesquels sont appliquées les stratégies :

- Les paramètres du profil de stratégie peuvent être différents des paramètres de la stratégie elle-même.
- Il n'est pas nécessaire de maintenir et d'appliquer manuellement plusieurs copies d'une stratégie qui se distinguent uniquement par un faible nombre de paramètres.
- Il n'est pas nécessaire de prévoir une stratégie distincte pour des utilisateurs autonomes.
- Vous pouvez exporter et importer des profils de stratégie, ainsi que créer de nouveaux profils sur la base de ceux existants.
- Pour une seule stratégie, plusieurs profils de stratégie peuvent être actifs. Seront appliqués à l'appareil les profils qui satisfont aux règles d'activation sur cet appareil.
- Les profils sont soumis à la hiérarchie des stratégies. La stratégie héritée contient tous les profils de stratégie du niveau supérieur.

Priorités des profils

Les profils créés pour une stratégie sont classés par ordre de priorité décroissante. Par exemple, si le profil X se trouve plus haut que le profil Y dans la liste des profils, le profil X a une priorité plus élevée que le profil Y. Il est possible d'appliquer simultanément plusieurs profils à un seul appareil. Si la valeur d'un paramètre est différente dans les profils, la valeur du paramètre du profil ayant la priorité la plus élevée est appliquée à l'appareil.

Règles d'activation d'un profil

Le profil de stratégie s'active sur l'appareil client quand une règle d'activation est remplie. *Les règles d'activation* sont un ensemble de conditions qui si elles sont remplies déclenchent le profil de stratégie sur l'appareil. Une règle d'activation peut contenir les conditions suivantes :

- L'Agent d'administration sur l'appareil client se connecte au Serveur d'administration selon une sélection de paramètres de connexion définis (adresse du Serveur d'administration, numéro de port, etc.).
- L'appareil client se trouve en mode déconnecté.
- Des tags déterminés ont été attribués à l'appareil client.

- L'appareil client est situé dans une subdivision définie d'Active Directory® de manière évidente (l'appareil se trouve directement dans la subdivision indiquée) ou de manière non évidente (l'appareil se trouve dans une subdivision à l'intérieur de la subdivision indiquée, à n'importe quel niveau d'imbrication), l'appareil ou son propriétaire se trouvent dans le groupe de sécurité d'Active Directory.

- L'appareil client appartient à un propriétaire défini ou son propriétaire se trouve dans le groupe de sécurité interne Kaspersky Security Center.

- Le propriétaire de l'appareil client a reçu un rôle défini.

Stratégies dans la hiérarchie des groupes d'administration

Si vous créez une stratégie dans un groupe d'administration de niveau inférieur, la nouvelle stratégie hérite des profils de la stratégie active pour le groupe de niveau supérieur. Les profils dont les noms sont identiques sont réunis. Les profils de stratégie pour un groupe de niveau plus élevé ont une priorité plus élevée. Ainsi, la stratégie *P(A)* du groupe d'administration *A* contient les profils *X1*, *X2* et *X3* par ordre de priorité descendante. Dans le groupe d'administration *B*, qui est un sous-groupe du groupe *A*, la stratégie *P(B)* est créée avec les profils *X2*, *X4* et *X5*. Alors la stratégie *P(B)* sera remplacée par la stratégie *P(A)* de sorte que dans la stratégie *P(B)*, la liste des profils par ordre de priorité décroissante sera *X1*, *X2*, *X3*, *X4*, *X5*. La priorité du profil *X2* dépendra de l'état d'origine de *X2* de la stratégie *P(B)* et *X2* de la stratégie *P(A)*. Une fois la stratégie *P(B)* créée, la stratégie *P(A)* s'affichera dans le sous-groupe *B*.

La stratégie active est recalculée à chaque fois au lancement de l'Agent d'administration, lors de l'activation ou de la désactivation du mode déconnecté ou en cas de modification de la liste des tags attribués à l'appareil client. Par exemple, si le volume de mémoire vive a été augmenté sur l'appareil, le profil de stratégie a été activé et est appliqué aux appareils ayant un volume de mémoire vive important.

Propriétés et restrictions d'un profil de stratégie

Les profils possèdent les propriétés suivantes :

- Les profils d'une stratégie inactive n'ont aucun impact sur les appareils client.

- Si une stratégie est définie sur l'état **Stratégie pour les utilisateurs autonomes**, les profils de cette stratégie seront également appliqués uniquement lorsqu'un appareil est déconnecté du réseau d'entreprise.

- Les profils ne prennent pas en charge l'analyse statistique de l'accès aux fichiers exécutables.

- Un profil de stratégie ne peut pas contenir des paramètres des notifications sur les événements.

- En cas de connexion de l'appareil au Serveur d'administration via le port UDP 15000, le profil de stratégie correspondant est activé dans la minute lors de l'attribution d'un tag à l'appareil.

- Vous pouvez utiliser les règles de la connexion de l'Agent d'administration au Serveur d'administration lorsque vous créez les règles d'activation du profil de stratégie.

Création d'un profil de stratégie

La création du profil est disponible uniquement pour les stratégies des applications suivantes :

- Kaspersky Endpoint Security 10 Service Pack 1 for Windows et versions supérieures

- Kaspersky Endpoint Security 10 Service Pack 1 for Mac

- Plug-in d'administration des appareils mobiles de Kaspersky des versions 10 Service Pack 1 à 10 Service Pack 3 Maintenance Release 1
- Plug-in Kaspersky Device Management for iOS
- Kaspersky Security for Virtualization 5.1 Light Agent pour Windows et Linux

Pour créer un profil de stratégie, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le groupe d'administration dont la stratégie requiert la création d'un profil de stratégie.
2. Dans l'espace de travail du groupe d'administration, ouvrez l'onglet **Stratégies**.
3. Sélectionnez la stratégie et ouvrez la fenêtre des propriétés de la stratégie à l'aide du menu contextuel.
4. Ouvrez la section **Profils de stratégie** dans la fenêtre des propriétés de la stratégie, puis cliquez sur le bouton **Ajouter**.

   L'Assistant de création d'un profil de stratégie démarre.
5. Dans la fenêtre **Nom du profil de stratégie** de l'Assistant, définissez ce qui suit :

   a. Nom d'un profil de stratégie.

      Le nom du profil ne peut pas contenir plus de 100 caractères.

   b. L'état du profil de stratégie (*Active*, *désactive*).

      Il est conseillé de créer des profils inactifs de stratégie et de les activer uniquement après la fin de la configuration des paramètres et des conditions d'activation des profils de stratégie.
6. Cochez la case **&Après la fermeture de l'Assistant de création de profil de stratégie terminé, passer à la configuration de la règle d'activation du profil de stratégie** pour démarrer l'Assistant de création d'une règle d'activation du profil de stratégie. Suivez les étapes de l'assistant.
7. Modifiez les paramètres du profil de stratégie dans la fenêtre des propriétés du profil de stratégie comme vous le voulez.
8. Enregistrez les modifications en cliquant sur le bouton **OK**.

   Le profil est enregistré. Le profil est activé sur les appareils qui répondent aux règles d'activation.

Plusieurs profils de stratégie peuvent être créer pour une stratégie. Les profils créés pour une stratégie apparaissent dans les propriétés de la stratégie, dans la section **Profils de stratégie**. Vous pouvez modifier un profil de stratégie et modifier la priorité du profil ainsi que supprimer le profil.

Modification du profil de stratégie

Modification des paramètres du profil de stratégie

La modification d'un profil de stratégie est uniquement possible pour les stratégies de Kaspersky Endpoint Security for Windows.

Pour modifier un profil de stratégie, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le groupe d'administration pour lequel il faut modifier le profil de stratégie.
2. Dans l'espace de travail du groupe, sélectionnez l'onglet **Stratégies**.
3. Sélectionnez la stratégie et ouvrez la fenêtre des propriétés de la stratégie à l'aide du menu contextuel.
4. Ouvrez la section **Profils de stratégie** dans les propriétés de la stratégie.

   La section contient la liste des profils créés pour la stratégie. Les profils de la liste sont affichés conformément à leur priorité.
5. Sélectionnez le profil de stratégie, puis cliquez sur le bouton **Propriétés**.
6. Configurez les paramètres du profil dans la fenêtre des propriétés :
   - Le cas échéant, dans la section **Général**, modifiez le nom du profil et activez ou désactivez le profil en utilisant la case à cocher **Activer le profil**.
   - Dans la section **Règles d'activation**, modifiez les règles d'activation du profil.
   - Modifiez les paramètres de la stratégie dans les sections correspondantes.
7. Cliquez sur le bouton **OK**.

Les paramètres modifiés entrent en vigueur après la synchronisation de l'appareil avec le Serveur d'administration (si le profil de stratégie est actif), ou après l'exécution de la règle d'activation (si le profil de stratégie est inactif).

Modification de la priorité du profil de stratégie

La priorité des profils de stratégie détermine l'ordre d'activation de ces profils sur l'appareil client. La priorité intervient si différents profils de stratégie sont soumis aux mêmes règles d'activation.

Imaginons deux profils de stratégie : *Profil 1* et *Profil 2* qui se distinguent uniquement par les valeurs d'un paramètre (*Valeur 1* et *Valeur 2*). La priorité du *Profil 1* est supérieure à celle du *Profil 2*. De plus, il existe d'autres profils dont la priorité est inférieure à celle de *Profil 2*. Les règles d'activation des profils correspondent.

En cas d'exécution des règles d'activation, s'est le *Profil 1* qui sera activé. Le paramètre sur l'appareil prend la *Valeur 1*. Si le *Profil 1* est supprimé, c'est le *Profil 2* qui aura la priorité la plus haute et le paramètre prendra la *Valeur 2*.

La liste des profils de stratégie affiche les profils selon leur priorité. La tête de la liste revient au profil possédant la priorité la plus élevée. Vous pouvez modifier la priorité d'un profil à l'aide des boutons en flèche vers le haut et vers le bas .

Suppression d'un profil de stratégie

Pour supprimer un profil de stratégie, procédez comme suit :

1. Sélectionnez dans l'arborescence de la console le groupe d'administration dans lequel vous voulez supprimer le profil de stratégie.
2. Dans l'espace de travail du groupe d'administration, ouvrez l'onglet **Stratégies**.
3. Sélectionnez la stratégie et ouvrez la fenêtre des propriétés de la stratégie à l'aide du menu contextuel.
4. Ouvrez la section **Profils de stratégie** dans les propriétés de la stratégie de Kaspersky Endpoint Security.
5. Sélectionnez le profil de stratégie que vous souhaitez supprimer, puis cliquez sur le bouton **Supprimer**.

Le profil de stratégie sera Supprimé. Il sera remplacé par un autre profil de stratégie dont les règles d'activation sont exécutées sur l'appareil ou par une stratégie.

Création d'une règle d'activation du profil de stratégie

Pour créer une règle d'activation du profil de stratégie, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le groupe d'administration pour lequel il faut créer une règle d'activation du profil de stratégie.
2. Dans l'espace de travail du groupe, sélectionnez l'onglet **Stratégies**.
3. Sélectionnez la stratégie et ouvrez la fenêtre des propriétés de la stratégie à l'aide du menu contextuel.
4. Sélectionnez la section **Profils de stratégie** dans la fenêtre des propriétés de la stratégie.
5. Choisissez le profil de stratégie, pour lequel vous devez créer la règle d'activation, puis cliquez sur le bouton **Propriétés**.

   Cette action entraîne l'ouverture de la fenêtre des propriétés du profil de stratégie.

   Si la liste des profils de stratégie est vide, vous pouvez créer le profil de stratégie.
6. Sélectionnez la section **Règles d'activation**, puis cliquez sur le bouton **Ajouter**.

   L'Assistant de création d'une règle d'activation du profil de stratégie démarre.

7. Dans la fenêtre **Règles d'activation du profil de stratégie**, cochez les cases en regard des conditions qui doivent affecter l'activation du profil de stratégie créé :

- **&Règles générales d'activation du profil de stratégie**

  Cochez la case pour configurer les règles de l'activation du profil de stratégie sur l'appareil en fonction de l'état du mode déconnecté de l'appareil, de la règle de connexion de l'appareil au Serveur d'administration et des tags attribués à l'appareil.

- **Règles d'utilisation d'&Active Directory**

  Cochez la case pour configurer les règles d'activation du profil de stratégie sur l'appareil en fonction du placement de l'appareil dans une division Active Directory ou de l'appartenance de l'appareil ou du propriétaire de l'appareil au groupe de sécurité Active Directory.

- **Règles d'un &propriétaire particulier de l'appareil**

  Cochez la case pour configurer les règles d'activation du profil de stratégie sur l'appareil en fonction de son propriétaire.

- **Règles pour les spécifications matérielles**

  Cochez la case pour configurer les règles d'activation du profil de stratégie sur l'appareil en fonction du volume de la mémoire et du nombre de processeurs logiques de l'appareil.

Le nombre de pages supplémentaires de l'Assistant dépend des paramètres que vous sélectionnez à la première étape. Vous pouvez modifier les règles d'activation du profil de stratégie plus tard.

8. Dans la fenêtre **Conditions générales**, configurez les paramètres suivants :

- Dans la liste déroulante du champ **Appareil en mode déconnecté**, spécifiez la condition de présence de l'appareil sur le réseau :

  - **Oui**

    L'appareil se trouve dans un réseau extérieur, c'est-à-dire que le Serveur d'administration n'est pas accessible.

  - **Non**

    L'appareil se trouve sur le réseau, le Serveur d'administration est donc accessible.

  - **La valeur n'est pas sélectionnée**

    Les critères ne sont pas appliqués.

- Dans le champ **L'appareil se trouve à l'emplacement réseau indiqué**, utilisez les listes déroulantes pour configurer l'activation du profil de stratégie si la règle de connexion du Serveur d'administration est exécutée ou non exécutée sur cet appareil :

  - **Est exécuté / N'est pas exécuté**

    Condition d'activation du profil de stratégie (la règle est appliquée ou non).

  - **Nom de la règle**

    La description de l'emplacement réseau de l'appareil pour la connexion au Serveur d'administration dont la vérification ou non de la condition détermine l'activation du profil de stratégie.

    La description de l'emplacement réseau de l'appareil pour la connexion au Serveur d'administration peut être créée ou configurée dans la règle de permutation de l'Agent d'administration.

La fenêtre **Conditions générales** s'affiche si vous avez coché la case **Règles générales d'activation du profil de stratégie**.

9. Dans la fenêtre **Conditions utilisant les tags**, configurez les paramètres suivants :

   - **Liste des tags**

     Définissez dans la liste des tags la règle d'inclusion des appareils dans le profil de stratégie en cochant la case des tags souhaités.

     Vous pouvez ajouter à la liste de nouveaux tags en les saisissant dans le champ sur la liste et en cliquant sur le bouton **Ajouter**.

     Le profil de stratégie reprendra les appareils dont la description reprend tous les tags sélectionnés. Si les cases sont décochées, les critères ne sont pas appliqués. Les cases sont décochées par défaut.

   - **Appliquer aux appareils sans les tags sélectionnés**

     Activez cette option s'il est nécessaire d'intervertir la sélection de tags.

     Si cette option est activée, les appareils sans tags sélectionnés seront inclus dans le profil de stratégie. Si l'option est désactivée, les critères ne sont pas appliqués.

     Cette option est Inactif par défaut.

   La fenêtre **Conditions utilisant les tags** est affichée si la case **&Règles générales d'activation du profil de stratégie** est cochée.

10. Dans la fenêtre **Conditions utilisant Active Directory**, configurez les paramètres suivants :

    - **Appartenance du propriétaire de l'appareil au groupe de &sécurité Active Directory**

      Si l'option est activée, le profil de stratégie est activé sur l'appareil dont le propriétaire est membre du groupe de sécurité indiqué. Si l'option est désactivée, les critères d'activation du profil ne sont pas appliqués. Cette option est Inactif par défaut.

    - **Appartenance de l'appareil au groupe de sécurité Active Directory**

      Si cette option est activée, le profil de stratégie est activé sur l'appareil. Si l'option est désactivée, les critères d'activation du profil ne sont pas appliqués. Cette option est Inactif par défaut.

    - **Placement de l'appareil dans &une unité organisationnelle Active Directory**

      Si cette option est activée, le profil de stratégie est activé sur l'appareil figurant dans la sous-division Active Directory indiquée. Si l'option est désactivée, les critères d'activation du profil ne sont pas appliqués.

      Cette option est Inactif par défaut.

    La fenêtre **Conditions utilisant Active Directory** s'affiche, si vous avez coché la case **Règles d'utilisation d'&Active Directory**.

11. Configurez les paramètres suivants dans la fenêtre **Conditions utilisant le propriétaire de l'appareil** :

- **&Propriétaire de l'appareil**

  Activez l'option pour configurer et activer une règle d'activation de profil sur l'appareil en fonction de son propriétaire. La liste déroulante située sous la case permet de sélectionner les critères d'activation du profil :

  - L'appareil appartient au propriétaire indiqué (le symbole "=").
  - L'appareil n'appartient pas au propriétaire indiqué (le symbole "#").

    Si cette option est activée, le profil est activé sur l'appareil en fonction du critère configuré. Vous pouvez indiquer le propriétaire de l'appareil lorsque l'option est activée. Si l'option est désactivée, les critères d'activation du profil ne sont pas appliqués. Cette option est Inactif par défaut.

- **&Le propriétaire de l'appareil fait partie d'un groupe de sécurité interne**

  Activez l'option pour configurer et activer la règle d'activation du profil sur l'appareil en fonction de l'appartenance de son propriétaire au groupe de sécurité interne de Kaspersky Security Center. La liste déroulante située sous la case permet de sélectionner les critères d'activation du profil :

  - Le propriétaire de l'appareil appartient au groupe de sécurité indiqué (le symbole "=").
  - Le propriétaire de l'appareil n'appartient pas au groupe de sécurité indiqué (le symbole "#").

    Si cette option est activée, le profil est activé sur l'appareil en fonction du critère configuré. Vous pouvez spécifier un groupe de sécurité de Kaspersky Security Center. Si l'option est désactivée, les critères d'activation du profil ne sont pas appliqués. Cette option est Inactif par défaut.

- **Activer le profil de stratégie en présence d'un &rôle pour le propriétaire de l'appareil**

  Sélectionnez cette option pour configurer et activer la règle d'activation du profil sur l'appareil en fonction du rôle du propriétaire. Ajoutez le rôle manuellement depuis la liste des rôles existants.

  Si cette option est activée, le profil est activé sur l'appareil en fonction du critère configuré.

La fenêtre **Conditions utilisant le propriétaire de l'appareil** s'ouvre si la case **Règles d'un &propriétaire particulier de l'appareil** est cochée.

12. Configurez les paramètres suivants dans la fenêtre **Conditions utilisant les caractéristiques de l'équipement** :

- **Taille de la mémoire RAM (Mo)**

  Activez cette option pour configurer et activer une règle d'activation du profil sur l'appareil en fonction du volume de mémoire vive de l'appareil. La liste déroulante située sous la case permet de sélectionner les critères d'activation du profil :

  - Le volume de mémoire vive de l'appareil est inférieur à la valeur indiquée (le symbole " < ").
  - Le volume de mémoire vive de l'appareil est supérieur à la valeur indiquée (le symbole " > ").

  Si cette option est activée, le profil est activé sur l'appareil en fonction du critère configuré. Vous pouvez indiquer le volume de mémoire vive de l'appareil. Si l'option est désactivée, les critères d'activation du profil ne sont pas appliqués. Cette option est Inactif par défaut.

- **Nombre de processeurs logiques**

  Activez cette option pour configurer et activer une règle d'activation du profil sur l'appareil en fonction de son nombre de processeurs logiques. La liste déroulante située sous la case permet de sélectionner les critères d'activation du profil :

  - Le nombre de processeurs logiques de l'appareil est inférieur ou égal à la valeur indiquée (le symbole " < ").
  - Le nombre de processeurs logiques de l'appareil est supérieur ou égal à la valeur indiquée (le symbole " > ").

  Si cette option est activée, le profil est activé sur l'appareil en fonction du critère configuré. Vous pouvez indiquer le nombre de processeurs logiques de l'appareil. Si l'option est désactivée, les critères d'activation du profil ne sont pas appliqués. Cette option est Inactif par défaut.

La fenêtre **Conditions utilisant les caractéristiques de l'équipement** s'affiche si la case **Règles pour les spécifications matérielles** a été cochée.

13. Dans la fenêtre **Nom de la règle d'activation du profil de stratégie**, dans le champ **Nom de la règle**, spécifiez un nom pour la règle.

Le profil est enregistré. Le profil sera activé sur l'appareil lors de l'application des règles d'activation.

Les règles d'activation du profil de stratégie créées pour le profil s'affichent dans les propriétés du profil de stratégie dans la section **Règles d'activation**. Vous pouvez modifier ou supprimer la règle de l'activation du profil de stratégie.

Il est possible d'exécuter simultanément plusieurs règles d'activation.

Règles de déplacement des appareils

Nous vous conseillons d'automatiser l'organisation des appareils en groupes d'administration à l'aide des *règles de déplacement des appareils*. Une règle de déplacement de l'appareil contient trois parties principales : un nom, une condition d'exécution (l'expression logique sur les attributs de l'appareil) et un groupe d'administration cible. La règle déplace l'appareil dans le groupe d'administration cible si les attributs de l'appareils répondent à la condition d'exécution de la règle.

Les règles de déplacement des appareils ont des priorités. Le Serveur d'administration vérifie si les attributs de l'appareil sont conformes à la condition d'exécution de chaque règle, selon la priorité croissante des règles. Si les attributs de l'appareil satisfont à la condition d'exécution de la règle, l'appareil est déplacé vers le groupe cible et le traitement des règles pour cet appareil cesse. Si les attributs de l'appareil satisfont directement à plusieurs règles, l'appareil est placé dans le groupe cible de la règle qui affiche la priorité la plus élevée (la règle qui figure plus haut dans la liste).

Les règles de déplacement des appareils peuvent être créées de manière implicite. Par exemple, les propriétés d'un paquet ou d'une tâche d'installation à distance peuvent contenir un groupe d'administration qui va accueillir un appareil après l'installation sur celui-ci d'un Agent d'administration. De même, l'administrateur de Kaspersky Security Center peut créer des règles de déplacement de manière explicite dans la liste des règles de déplacement. La liste se trouve dans la Console d'administration, dans les propriétés du groupe **Appareils non définis**.

La règle de déplacement par défaut est prévue pour le déplacement initial et ponctuel des appareils dans les groupes d'administration. La règle déplace une seule fois les appareils qui se trouvent dans le groupe **Appareils non définis**. Si l'appareil a déjà été déplacé une fois par cette règle, celle-ci ne le déplacera pas à nouveau, même si l'appareil est replacé manuellement dans le groupe **Appareils non définis**. C'est le moyen recommandé pour l'utilisation des règles de déplacement.

Il est possible de déplacer des appareils qui se trouvent déjà dans des groupes d'administration. Pour ce faire, dans les propriétés d'une règle, décochez la case **Déplacer &uniquement les appareils non inclus dans un groupe d'administration**.

La présence de règles de déplacement qui agissent sur des appareils qui figurent déjà dans des groupes d'administration augmente sensiblement la charge sur le Serveur d'administration.

La case **Déplacer &uniquement les appareils non inclus dans un groupe d'administration** est verrouillée dans les propriétés des règles de déplacement créées automatiquement. Ces règles sont créées lorsque vous ajoutez la tâche *Installation de l'application à distance* ou créez le paquet d'installation autonome.

Il est possible de créer une règle de déplacement qui peut agir à plusieurs reprises sur le même appareil.

Il est vivement conseillé d'éviter d'adopter une démarche de manipulation des appareils administrés dans le cadre de laquelle le même appareil est déplacé à plusieurs reprises d'un groupe vers un autre, par exemple pour appliquer une stratégie particulière à l'appareil, pour lancer une tâche de groupe spéciale ou réaliser une mise à jour depuis un point de distribution défini.

Ces scénarios ne sont pas pris en charge car ils ne sont pas efficaces en termes de charge sur le Serveur d'administration et de trafic réseau. De plus, ils sont en contradiction avec les modèles de fonctionnement de Kaspersky Security Center (surtout au niveau des privilèges d'accès, des événements et des rapports). Il faut trouver une autre solution, par exemple utiliser des profils de stratégies, des tâches pour des sélections d'appareils, désigner des agents de mises à Réseau conformément à la méthode.

Clonage Règles de déplacement des appareils

Lorsque vous devez créer plusieurs règles de déplacement d'appareils avec des paramètres similaires, vous pouvez cloner une règle en vigueur, puis modifiez les paramètres dans les règles clonées. Cette fonction est utile lorsqu'il vous faut plusieurs règles de déplacement d'appareils avec différentes plages IP et groupes cible.

Pour cloner une règle de déplacement d'appareil

1. Ouvrez la fenêtre principale de l'application.
2. Dans le dossier **Appareils non définis**, cliquez sur **Configurer les règles**.

   La fenêtre **Propriétés : appareils non définis** s'ouvre.
3. Dans la section **Déplacer les appareils**, sélectionnez la règle de déplacement de l'appareil que vous voulez cloner.
4. Cliquez sur **Cloner la règle**.

Le clone de la règle de déplacement d'appareil sélectionnée est ajouté en fin de liste.

La règle créée possède l'état désactivé. Vous pouvez modifier et activer la règle à tout moment.

Catégorisation du logiciel

La méthode principale pour contrôler le lancement des applications repose sur les *catégories de Kaspersky* (ci-après, les *catégories KL*). Les catégories KL simplifient la tâche de l'administrateur de Kaspersky Security Center au niveau de la maintenance des catégories d'applications et réduisent le volume de trafic transmis aux appareils administrés.

Créez des catégories utilisateur uniquement pour les applications qui ne correspondent à aucune des catégories KL (par exemple une application développée sur mesure). Les catégories utilisateur sont créées sur la base d'un paquet d'installation (MSI) ou sur la base du dossier contenant les paquets d'installation.

S'il existe une grande collection à enrichir de logiciels qui ne sont pas classés selon les catégories KL, il peut être utile de créer une catégorie mise à jour automatiquement. Cette catégorie s'enrichit automatiquement des sommes de contrôle des fichiers exécutable lors de la modification du dossier contenant les distributions.

Ne créez pas des catégories d'applications mises à jour automatiquement pour les dossiers Mes documents, %windir%, %ProgramFiles% et %ProgramFiles(x86)%. Les fichiers dans ces dossiers changent souvent, ce qui augmente la charge sur le Serveur d'administration et le trafic dans le réseau. Il faut créer un dossier séparé contenant la collection de logiciels et l'enrichir de temps à autre.

Conditions indispensables pour l'installation des applications sur les appareils de l'entreprise cliente

Le processus d'installation à distance des applications sur les appareils de l'entreprise cliente correspond au processus d'installation à distance des applications à l'intérieur de la société.

Pour installer des applications sur les appareils de l'entreprise cliente, les conditions suivantes doivent être remplies :

- Avant la première installation des applications sur les appareils de l'entreprise cliente, il faut installer sur ceux-ci l'Agent d'administration.

  Lors de la configuration du paquet d'installation de l'Agent d'administration par le fournisseur de services dans l'application Kaspersky Security Center, il faut configurer les paramètres suivants dans la fenêtre des propriétés du paquet d'installation :

  - Dans la section **Connexion**, dans la chaîne **Serveur d'administration**, indiquez l'adresse du Serveur d'administration virtuel spécifié lors de l'installation locale de l'Agent d'administration sur le point de distribution.

  - Dans la section **Avancé**, cochez la case **Se connecter au Serveur d'administration au moyen d'une passerelle de connexion**. Dans la chaîne **Adresse de la passerelle**, indiquez l'adresse du point de distribution. Pour l'adresse de l'appareil, vous pouvez utiliser l'adresse IP ou le nom de l'appareil sur le réseau Windows.

- Pour télécharger le paquet d'installation de l'Agent d'administration, sélectionnez **En utilisant les ressources du système d'exploitation via les points de distribution**. La sélection du mode de téléchargement s'effectue d'une manière suivante :

  - Lors de l'installation des applications à l'aide des tâches d'installation à distance, le mode de téléchargement peut être sélectionné par deux moyens :

    - Lors de la création de la tâche d'installation à distance dans la fenêtre **Paramètres**.

    - Dans la fenêtre des propriétés de la tâche d'installation à distance dans la section **Paramètres**.

  - Lors de l'installation des applications à l'aide de l'Assistant de l'installation à distance, le mode de téléchargement peut être sélectionné dans la fenêtre **Paramètres** de l'Assistant.

- Le compte utilisateur sous lequel fonctionne le point de distribution doit avoir accès à la ressource Admin$ sur les appareils clients.

Consultation et modification des paramètres locaux de l'application

Le système d'administration Kaspersky Security Center permet d'administrer à distance les paramètres locaux des applications sur les appareils via la Console d'administration.

Les *Paramètres locaux des applications* sont les paramètres de l'application propres à un appareil. A l'aide de Kaspersky Security Center, vous pouvez installer les paramètres locaux des applications pour les appareils inclus dans le groupe d'administration.

Les descriptions détaillées des paramètres des applications Kaspersky sont présentées dans les documentations respectives.

Pour consulter ou modifier les paramètres locaux de l'application, procédez comme suit :

1. Dans l'espace de travail du groupe dans lequel se trouve l'appareil concerné, sélectionnez l'onglet **Appareils**.
2. Dans la fenêtre des propriétés de l'appareil, dans la section **Applications**, sélectionnez l'application concernée.
3. Ouvrez la fenêtre des propriétés de l'application en double-cliquant sur le nom de l'application ou en cliquant sur le bouton **Propriétés**.

La fenêtre des paramètres locaux de l'application sélectionnée s'ouvre. Il est possible de consulter et de modifier ces paramètres.

Vous pouvez modifier les valeurs des paramètres dont la modification n'est pas interdite par la stratégie de groupe (le paramètre n'est pas verrouillé (🔓) dans la stratégie).

Mise à jour de Kaspersky Security Center et des applications administrées

Cette section décrit les étapes à suivre pour mettre à jour Kaspersky Security Center et les applications administrées.

Scénario : Mise à jour régulière des bases de données et des applications Kaspersky

Cette section fournit un scénario de mise à jour régulière des bases de données, des modules logiciels et des applications Kaspersky. Après avoir terminé le scénario de configuration de la protection du réseau, vous devez conserver la fiabilité du système de protection pour vous assurer que les Serveurs d'administration et les appareils administrés sont protégés contre plusieurs menaces, y compris des virus, des attaques réseau et des attaques par phishing.

La protection du réseau reste à jour pour assurer les mises à jour régulières des éléments suivants :

- Bases de données et modules logiciels de Kaspersky
- Applications de Kaspersky installées, y compris les modules et les applications de sécurité de Kaspersky Security Center

Lorsque vous terminez ce scénario, vous pouvez être sûr que :

- Votre réseau est protégé par le dernier logiciel de Kaspersky, y compris les modules et les applications de sécurité de Kaspersky Security Center.
- Les bases antivirus et les autres bases de données de Kaspersky critiques pour la sécurité du réseau sont toujours à jour.

Prérequis

Les appareils administrés doivent disposer d'une connexion au Serveur d'administration. Si ce n'est pas un cas, pensez à mettre à jour manuellement les bases de données, les modules logiciels et les applications de Kaspersky ou directement à partir des serveurs de mise à jour de Kaspersky.

Le Serveur d'administration doit avoir une connexion à Internet.

Avant de démarrer, assurez-vous que vous avez :

1. Déployé les applications de sécurité de Kaspersky sur les appareils administrés selon le scénario de déploiement des applications de Kaspersky par Kaspersky Security Center Web Console.
2. Créé et configuré l'ensemble des stratégies, profils de stratégie et tâches obligatoire selon le scénario de configuration de la protection du réseau.
3. Désigné une quantité appropriée de points de distribution en fonction du nombre d'appareils administrés et de la topologie du réseau.

Étapes de la mise à jour des bases de données et des applications Kaspersky :

1. **Choix d'un schéma de mise à jour**

   Vous pouvez utiliser plusieurs schémas pour installer les mises à jour des modules et des applications de sécurité de Kaspersky Security Center. Choisissez le schéma ou plusieurs schémas qui répondent le mieux aux exigences de votre réseau.

2. **Création de la tâche de téléchargement des mises à jour dans le stockage du Serveur d'administration**

   Cette tâche est créée automatiquement par l'Assistant de configuration initiale de l'application Kaspersky Security Center. Si vous n'aviez pas exécuté l'Assistant, créez la tâche maintenant.

   Cette tâche est requise pour télécharger les mises à jour des serveurs de mise à jour de Kaspersky dans le stockage du Serveur d'administration, ainsi que pour mettre à jour les bases de données et les modules logiciels de Kaspersky pour Kaspersky Security Center. Une fois téléchargées, les mises à jour peuvent être propagées vers les appareils administrés.

   Si votre réseau comporte des points de distribution désignés, les mises à jour sont automatiquement téléchargées du stockage du Serveur d'administration aux stockages des points de distribution. Dans ce cas, les appareils administrés inclus dans la zone d'action d'un point de distribution téléchargent les mises à jour du stockage du point de distribution au lieu du stockage du Serveur d'administration.

   Instructions pour :

   - Console d'administration : Création de la tâche de téléchargement des mises à jour dans le stockage du Serveur d'administration
   - Kaspersky Security Center Web Console : Création de la tâche de téléchargement des mises à jour dans le stockage du Serveur d'administration

3. **Création de la tâche de téléchargement des mises à jour dans les stockages des points de distribution (facultatif)**

   Par défaut, les mises à jour sont téléchargées sur les points de distribution à partir du Serveur d'administration. Vous pouvez configurer Kaspersky Security Center pour télécharger les mises à jour sur les points de distribution directement à partir des serveurs de mise à jour de Kaspersky. Le téléchargement vers les stockages des points de distribution est préférable si le trafic entre le Serveur d'administration et les points de distribution est plus cher que le trafic entre les points de distribution et les serveurs de mise à jour de Kaspersky ou si votre Serveur d'administration n'a pas d'accès Internet.

Lorsque votre réseau comporte des points de distribution désignés et que la tâche *Téléchargement des mises à jour sur les stockages des points de distribution* est créée, les points de distribution téléchargent les mises à jour à partir des serveurs de mises à jour de Kaspersky, et non à partir du stockage du Serveur d'administration.

Instructions pour :

- Console d'administration : Création de la tâche de téléchargement des mises à jour sur les stockages des points de distribution
- Kaspersky Security Center Web Console : Création de la tâche de téléchargement des mises à jour sur les stockages des points de distribution

4. **Configuration des points de distribution**

Lorsque votre réseau comporte des points de distribution désignés, assurez-vous que l'option **Déployer les mises à jour** est activée dans les propriétés de tous les points de distribution nécessaires. Lorsque cette option est désactivée pour un point de distribution, les appareils inclus dans la zone d'action du point de distribution téléchargent les mises à jour à partir du stockage du Serveur d'administration.

Si vous souhaitez que les appareils administrés reçoivent des mises à jour uniquement à partir des points de distribution, activez l'option **Distribuer les fichiers uniquement via les points de distribution** dans la stratégie de l'Agent d'administration.

5. **Optimisation du processus de mise à jour à l'aide du modèle déconnecté de téléchargement de mise à jour ou des fichiers diff (facultatif)**

Vous pouvez optimiser le processus de mise à jour à l'aide du modèle déconnecté de téléchargement de mise à jour (activé par défaut) ou à l'aide de fichiers diff. Pour chaque segment du réseau, vous devez choisir laquelle de ces deux fonctions activer car elles ne peuvent pas s'exécuter simultanément.

Lorsque le modèle déconnecté de téléchargement de mise à jour est activé, l'Agent d'administration télécharge les mises à jour nécessaires dans l'appareil administré une fois qu'elles sont téléchargées dans le stockage du Serveur d'administration, avant que l'application de sécurité les demande. Cela améliore la fiabilité du processus de mise à jour. Pour utiliser cette fonctionnalité, activez l'option **Télécharger au préalable les mises à jour et les bases antivirus depuis le Serveur d'administration (recommandé)** dans la stratégie de l'Agent d'administration.

Si vous n'utilisez pas le modèle déconnecté de téléchargement de mise à jour, vous pouvez optimiser le trafic entre le Serveur d'administration et les appareils administrés avec des fichiers diff. Lorsque cette fonction est activée, le Serveur d'administration ou un point de distribution télécharge des fichiers diff au lieu de fichiers entiers de bases de données ou de modules logiciels de Kaspersky. Un fichier diff décrit les différences entre deux version d'un fichier d'une base de données ou d'un module logiciel. Par conséquent, un fichier diff occupe moins d'espace qu'un fichier entier. Cela entraîne une baisse du trafic entre le Serveur d'administration ou les points de distribution et les appareils administrés. Pour utiliser cette fonctionnalité, activez l'option **Télécharger les fichiers diff** dans les propriétés de la tâche *Téléchargement des mises à jour sur le stockage du Serveur d'administration* et/ou de la tâche *Téléchargement des mises à jour sur les stockages des points de distribution*.

Instructions pour :

- Utilisation de fichiers diff pour la mise à jour des bases de données et des modules logiciels Kaspersky
- Console d'administration : Activation et désactivation du modèle déconnecté de téléchargement de mise à jour
- Kaspersky Security Center Web Console : Activation et désactivation du modèle déconnecté de téléchargement de mise à jour

6. **Vérification des mises à jour téléchargées (facultatif)**

Avant d'installer les mises à jour téléchargées, vous pouvez les vérifier via la tâche d'*analyse des mises à jour*. Cette tâche exécute de manière séquentielle les tâches de mise à jour des appareils et les tâches d'analyse des logiciels malveillants pour la collecte spécifiée d'appareils de test. Dès l'obtention des résultats de la tâche, le Serveur d'administration démarre ou bloque la propagation des mises à jour sur les appareils restants.

Dans le cadre de l'exécution de la tâche *Télécharger les mises à jour dans le stockage du Serveur d'administration*, la tâche d'*analyse des mises à jour* peut être exécutée. Dans les propriétés de la tâche de *Télécharger les mises à jour dans le stockage du Serveur d'administration*, activez l'option **Vérifier les mises à jour avant de les déployer** dans la Console d'administration ou l'option **Exécuter la vérification de mise à jour** dans Kaspersky Security Center Web Console.

Instructions pour :

- Console d'administration : Vérification des mises à jour téléchargées
- Kaspersky Security Center Web Console : Vérification des mises à jour téléchargées

7. **Approbation et refus des mises à jour logicielles**

   Par défaut, les mises à jour logicielles téléchargées sont à l'état *Non défini*. Vous pouvez modifier l'état en *Approuvée* ou *Rejetée*. Les mises à jour confirmées sont toujours installées. Si une mise à jour nécessite une révision et l'acceptation des termes du Contrat de licence utilisateur final, vous devez d'abord les accepter. Ensuite, la mise à jour peut être propagée sur les appareils administrés. Les mises à jour non définies peuvent uniquement être installées sur l'Agent d'administration et sur les autres modules de Kaspersky Security Center conformément aux paramètres de stratégie de l'Agent d'administration. Les mises à jour auxquelles vous avez attribué l'état *Rejetée* ne seront pas installées sur les appareils. Si une mise à jour rejetée pour une application de sécurité a été installée précédemment, Kaspersky Security Center essaiera de la désinstaller de tous les appareils.

   L'approbation et le refus de mises à jour est disponible uniquement pour l'Agent d'administration et les applications Kaspersky administrées installées sur les appareils clients Windows et Linux. La mise à jour transparente du Serveur d'administration, de Kaspersky Security Center Web Console et des plug-ins Web d'administration n'est pas prise en charge.

   Instructions pour :

   - Console d'administration : Approbation et refus des mises à jour logicielles
   - Kaspersky Security Center Web Console : Approbation et refus des mises à jour logicielles

8. **Configuration de l'installation automatique des mises à jour et des correctifs des composants de Kaspersky Security Center**

   Les mises à jour et les correctifs téléchargés pour l'Agent d'administration et les autres composants de Kaspersky Security Center sont installés automatiquement. Si vous n'avez pas laissé l'option **Installer automatiquement les mises à jour et les correctifs nécessaires pour les modules dont l'état est Non défini** activée dans les propriétés de l'Agent d'administration, toutes les mises à jour seront installées automatiquement après leur téléchargement dans le stockage (ou plusieurs stockages). Si l'option est désactivée, les correctifs de Kaspersky chargés avec l'état *Non défini* sont installés après que l'administrateur a modifié leur état pour qu'il soit *Approuvé*.

   Instructions pour :

   - Console d'administration : Activation et désactivation de la mise à jour automatique et de l'installation automatique des correctifs pour les modules de Kaspersky Security Center
   - Kaspersky Security Center Web Console : Activation et désactivation de l'installation automatique des mises à jour et des correctifs pour les modules de Kaspersky Security Center

9. **Installation des mises à jour du Serveur d'administration.**

   Les mises à jour logicielles du Serveur d'administration ne dépendent pas des états de la mise à jour. Elles ne sont pas installées automatiquement et doivent être préalablement approuvées par l'administrateur dans l'onglet **Surveillance** de la Console d'administration (**Serveur d'administration** `<nom du serveur>` → **Surveillance**) ou dans la section **Notifications** de Kaspersky Security Center Web Console (**Surveillance et rapports** → **Notifications**). Ensuite, l'administrateur doit exécuter explicitement l'installation des mises à jour.

10. **Configuration de l'installation automatique des mises à jour des applications de sécurité**

    Créez les tâches de *mise à jour* pour les applications administrées afin de fournir des mises à jour rapides des applications, des modules logiciels et des bases de données Kaspersky, et notamment des bases antivirus. Pour assurer des mises à jour en temps opportun, nous vous recommandons de sélectionner l'option **Lors du téléchargement des mises à jour dans le stockage** lors de la configuration de la planification des tâches.

    Si votre réseau comprend des appareils IPv6 uniquement et que vous souhaitez mettre à jour régulièrement les applications de sécurité installées sur ces appareils, assurez-vous que le Serveur d'administration (version non inférieure à 13.2) et l'Agent d'administration (version non inférieure à 13.2) sont installés sur les appareils administrés.

    Par défaut, les mises à jour de Kaspersky Endpoint Security for Windows et de Kaspersky Endpoint Security for Linux sont installées uniquement après que vous avez redéfini l'état de la mise à jour sur *Approuvée*. Vous pouvez modifier les paramètres des mises à jour dans la tâche de *mise à jour*.

    Si une mise à jour nécessite une révision et l'acceptation des termes du Contrat de licence utilisateur final, vous devez d'abord les accepter. Ensuite, la mise à jour peut être propagée sur les appareils administrés.

    Instructions pour :

    - Console d'administration : Installation automatique des mises à jour pour Kaspersky Endpoint Security sur les appareils
    - Kaspersky Security Center Web Console : Installation automatique des mises à jour pour Kaspersky Endpoint Security sur les appareils

Résultats

Lorsque le scénario est terminé, Kaspersky Security Center est configuré pour mettre à jour les bases de données de Kaspersky et les applications de Kaspersky installées après que les mises à jour sont téléchargées dans le stockage du Serveur d'administration ou dans les stockages des points de distribution. Vous pouvez ensuite passer à la surveillance de l'état du réseau.

À propos de la mise à jour des bases de données, des modules logiciels et des applications de Kaspersky

Pour vous assurer que la protection de vos Serveurs d'administration et des appareils administrés est à jour, vous devez fournir des mises à jour opportunes des éléments suivants :

- Bases de données et modules logiciels de Kaspersky

  Avant de télécharger les bases de données et les modules logiciels de Kaspersky, Kaspersky Security Center vérifie si les serveurs de Kaspersky sont accessibles. Si l'accès aux serveurs via le DNS système n'est pas possible, l'application utilise les serveurs DNS publics. Cela est nécessaire pour s'assurer que les bases de données antivirus sont mises à jour et que le niveau de sécurité est maintenu pour les appareils administrés.

- Applications de Kaspersky installées, y compris les modules et les applications de sécurité de Kaspersky Security Center

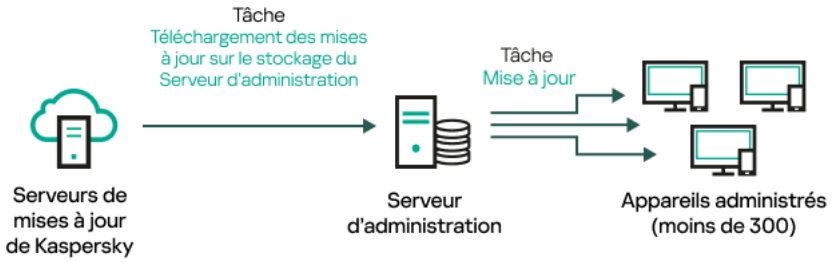
  Kaspersky Security Center permet de mettre à jour automatiquement l'Agent d'administration et les applications Kaspersky installées sur les appareils clients Windows et Linux. La mise à jour transparente du Serveur d'administration, de Kaspersky Security Center Web Console et des plug-ins Web d'administration n'est pas prise en charge. Pour mettre à jour ces modules, vous devez télécharger les dernières versions à partir du site Internet de Kaspersky, puis les installer manuellement.

En fonction de la configuration de votre réseau, vous pouvez utiliser les schémas suivants de téléchargement et de distribution des mises à jour requises sur les appareils administrés :

- En utilisant une seule tâche : *Téléchargement des mises à jour sur le stockage du Serveur d'administration*
- En utilisant deux tâches :
  - *Téléchargement des mises à jour sur le stockage du Serveur d'administration*
  - Tâche de *Téléchargement des mises à jour sur les stockages des points de distribution*
- Manuellement via un dossier local, un dossier partagé ou un serveur FTP
- Directement à partir des serveurs de mise à jour de Kaspersky vers Kaspersky Endpoint Security sur les appareils administrés
- Via un dossier local ou réseau si le Serveur d'administration n'a pas de connexion Internet

Cliquez sur la tâche de Téléchargement des mises à jour sur le stockage du Serveur d'administration

Dans ce schéma, Kaspersky Security Center télécharge les mises à jour via la tâche *Téléchargement des mises à jour sur le stockage du Serveur d'administration*. Dans les petits réseaux qui contiennent moins de 300 appareils administrés dans un segment de réseau unique ou moins de 10 appareils administrés dans chaque segment de réseau, les mises à jour sont distribuées aux appareils administrés directement à partir du stockage du Serveur d'administration (voir figure ci-dessous).

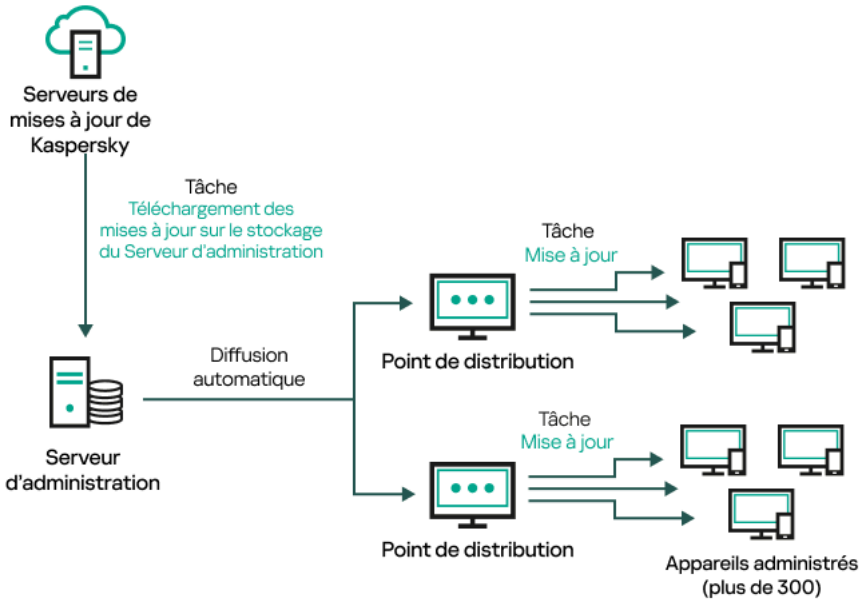


Mise à jour à l'aide de la tâche Téléchargement des mises à jour sur le stockage du Serveur d'administration sans points de distribution

Par défaut, le Serveur d'administration communique avec les serveurs de mise à jour de Kaspersky et télécharge les mises à jour au moyen du protocole HTTPS. Vous pouvez configurer le Serveur d'administration pour qu'il utilise le protocole HTTP au lieu du protocole HTTPS.

Si votre réseau contient plus de 300 appareils administrés ou si votre réseau comprend plusieurs segments de réseau avec plus de 9 appareils administrés dans chacun d'entre eux, nous vous recommandons d'utiliser des points de distribution pour propager les mises à jour vers les appareils administrés (voir figure ci-dessous). Les points de distribution réduisent la charge sur le Serveur d'administration et optimisent le trafic entre le Serveur d'administration et les appareils administrés. Vous pouvez calculer le nombre et la configuration de points de distribution nécessaires pour votre réseau.

Dans ce schéma, les mises à jour sont automatiquement téléchargées du stockage du Serveur d'administration vers les stockages des points de distribution. Les appareils administrés inclus dans la zone d'action d'un point de distribution téléchargent les mises à jour du stockage du point de distribution au lieu du stockage du Serveur d'administration.



Mise à jour à l'aide de la tâche Téléchargement des mises à jour sur le stockage du Serveur d'administration avec points de distribution

Lorsque la tâche *Téléchargement des mises à jour sur le stockage du Serveur d'administration* est terminée, les mises à jour suivantes sont téléchargées dans le stockage du Serveur d'administration :

- Bases de données et modules logiciels de Kaspersky pour Kaspersky Security Center

  Ces mises à jour sont installées automatiquement.

- Bases de données et modules logiciels de Kaspersky pour les applications de sécurité sur les appareils administrés

  Ces mises à jour sont installées via la tâche de mise à jour pour Kaspersky Endpoint Security for Windows.

- Mises à jour du Serveur d'administration

  Ces mises à jour ne sont pas installées automatiquement. L'administrateur doit approuver et exécuter explicitement l'installation des mises à jour.

  > L'installation de correctifs sur le Serveur d'administration requiert des privilèges d'administrateur.

- Mises à jour des modules de Kaspersky Security Center

  Par défaut, ces mises à jour sont installées automatiquement. Vous pouvez modifier les paramètres dans la stratégie de l'Agent d'administration.

- Mises à jour des programmes de protection

  Par défaut, Kaspersky Endpoint Security for Windows installe uniquement les mises à jour que vous approuvez. (Vous pouvez approuver les mises à jour via la Console d'administration ou via Kaspersky Security Center Web Console). Les mises à jour sont installées via la tâche de *mise à jour* et peuvent être configurées dans les propriétés de cette tâche.

> La tâche *Télécharger les mises à jour dans le stockage de la tâche du Serveur d'administration* n'est pas disponible sur les Serveurs d'administration virtuels. Les mises à jour téléchargées sur le Serveur d'administration principal s'affichent dans le stockage du Serveur d'administration virtuel.

Vous pouvez configurer l'analyse des mises à jour reçues sur la productivité et sur la présence des erreurs sur un ensemble d'appareils de test. Si la vérification réussit, les mises à jour sont distribuées à d'autres appareils administrés.

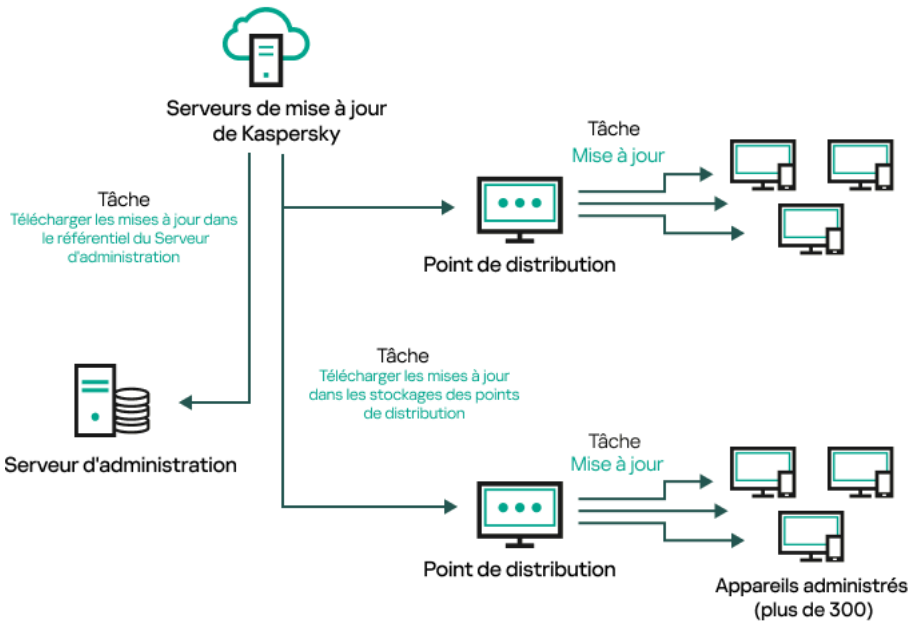
Chaque application de Kaspersky sollicite les mises à jour requises au serveur d'administration. Le Serveur d'administration accumule ces requêtes et télécharge uniquement les mises à jour requises par n'importe quelle application. Cela évite de télécharger les mêmes mises à jour plusieurs fois, voire de télécharger les mises à jour inutiles. Lors de l'exécution de la tâche *Téléchargement des mises à jour sur le stockage du Serveur d'administration*, le Serveur d'administration envoie automatiquement les informations suivantes aux serveurs de mise à jour de Kaspersky afin de garantir le téléchargement des versions appropriées des bases de données et des modules logiciels de Kaspersky :

- ID et version de l'application
- Identifiant d'installation de l'application
- ID de la clé active
- ID d'exécution de la tâche *Télécharger les mises à jour dans le stockage du Serveur d'administration*

Aucune des informations transmises ne contient des données personnelles ou confidentielles. AO Kaspersky Lab protège les informations obtenues conformément aux exigences définies par la loi.

En utilisant deux tâches : la tâche Téléchargement des mises à jour sur le stockage du Serveur d'administration et la tâche Téléchargement des mises à jour sur les stockages des points de distribution

Vous pouvez télécharger des mises à jour vers les stockages des points de distribution directement à partir des serveurs de mise à jour de Kaspersky au lieu du stockage du Serveur d'administration, puis distribuer les mises à jours sur les appareils administrés (voir figure ci-après). Le téléchargement vers les stockages des points de distribution est préférable si le trafic entre le Serveur d'administration et les points de distribution est plus cher que le trafic entre les points de distribution et les serveurs de mise à jour de Kaspersky ou si votre Serveur d'administration n'a pas d'accès Internet.



Mise à jour à l'aide de la tâche Téléchargement des mises à jour sur le stockage du Serveur d'administration et de la tâche Téléchargement des mises à jour sur les stockages des points de distribution

Par défaut, le Serveur d'administration et les points de distribution communiquent avec les serveurs de mise à jour de Kaspersky et télécharge les mises à jour au moyen du protocole HTTPS. Vous pouvez configurer le Serveur d'administration et/ou les points de distribution pour utiliser le protocole HTTP au lieu de HTTPS.

Pour implémenter ce schéma, créez la tâche *Téléchargement des mises à jour sur les stockages des points de distribution* en plus de la tâche *Téléchargement des mises à jour sur le stockage du Serveur d'administration*. Ensuite, les points de distribution téléchargent les mises à jour à partir des serveurs de mise à jour de Kaspersky, et non à partir du stockage du Serveur d'administration.

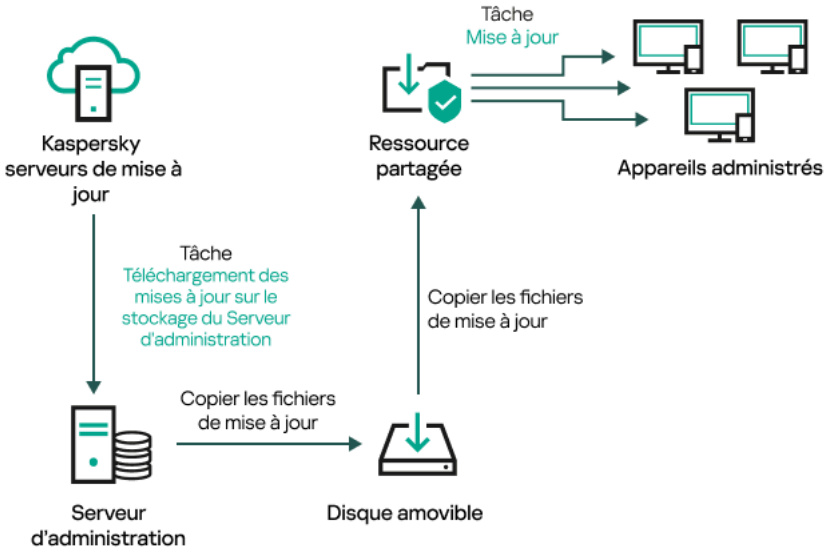
Les appareils de points de distribution exécutant macOS ne peuvent pas télécharger les mises à jour à partir des serveurs de mises à jour de Kaspersky.

Si un ou plusieurs appareils exécutant macOS sont inclus dans la zone d'action de la tâche *Télécharger les mises à jour sur les stockages des points de distribution*, la tâche reçoit l'état *Échec*, même si elle s'est terminée avec succès sur tous les appareils Windows.

La tâche *Téléchargement des mises à jour sur le stockage du Serveur d'administration* est également nécessaire pour ce schéma, car cette tâche sert à télécharger les bases de données et les modules logiciels de Kaspersky pour Kaspersky Security Center.

Manuellement via un dossier local, un dossier partagé ou un serveur FTP

Si les appareils client ne disposent pas d'une connexion au Serveur d'administration, vous pouvez utiliser un dossier local ou une ressource partagée comme source de mise à jour des bases de données, des modules logiciels et des applications de Kaspersky. Dans ce schéma, vous devez copier les mises à jour nécessaires du stockage du Serveur d'administration sur un disque amovible, puis copier les mises à jour dans le dossier local ou dans la ressource spécifiée comme source des mise à jour dans les paramètres de Kaspersky Endpoint Security (voir figure ci-dessous).



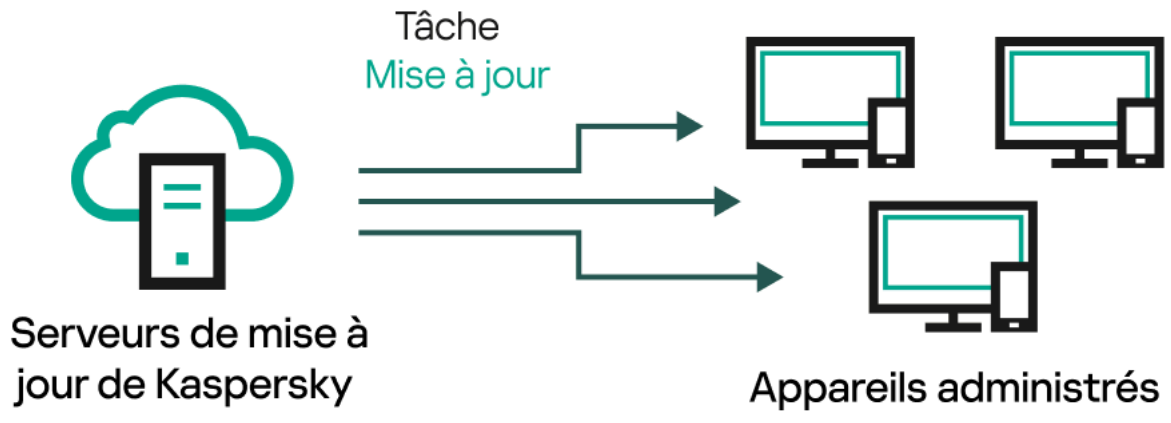
Mise à jour via un dossier local, un dossier partagé ou un serveur FTP

Pour en savoir plus sur les sources des mises à jour dans Kaspersky Endpoint Security, consultez les aides suivantes :

- Aide de Kaspersky Endpoint Security for Windows
- Aide de Kaspersky Endpoint Security for Linux

Directement à partir des serveurs de mise à jour de Kaspersky vers Kaspersky Endpoint Security sur les appareils administrés

Sur les appareils administrés, vous pouvez configurer Kaspersky Endpoint Security pour recevoir directement les mises à jour à partir des serveurs de mise à jour de Kaspersky (voir figure ci-dessous).



Mise à jour des applications de sécurité directement à partir des serveurs de mise à jour de Kaspersky

Dans ce schéma, l'application de sécurité n'utilise pas les stockages fournis par Kaspersky Security Center. Pour recevoir directement les mises à jour à partir des serveurs de mise à jour de Kaspersky, spécifiez ces derniers comme source de mises à jour dans l'interface de l'application de sécurité. Pour plus d'informations sur ces paramètres, consultez les aides suivantes :

- Aide de Kaspersky Endpoint Security for Windows
- Aide de Kaspersky Endpoint Security for Linux

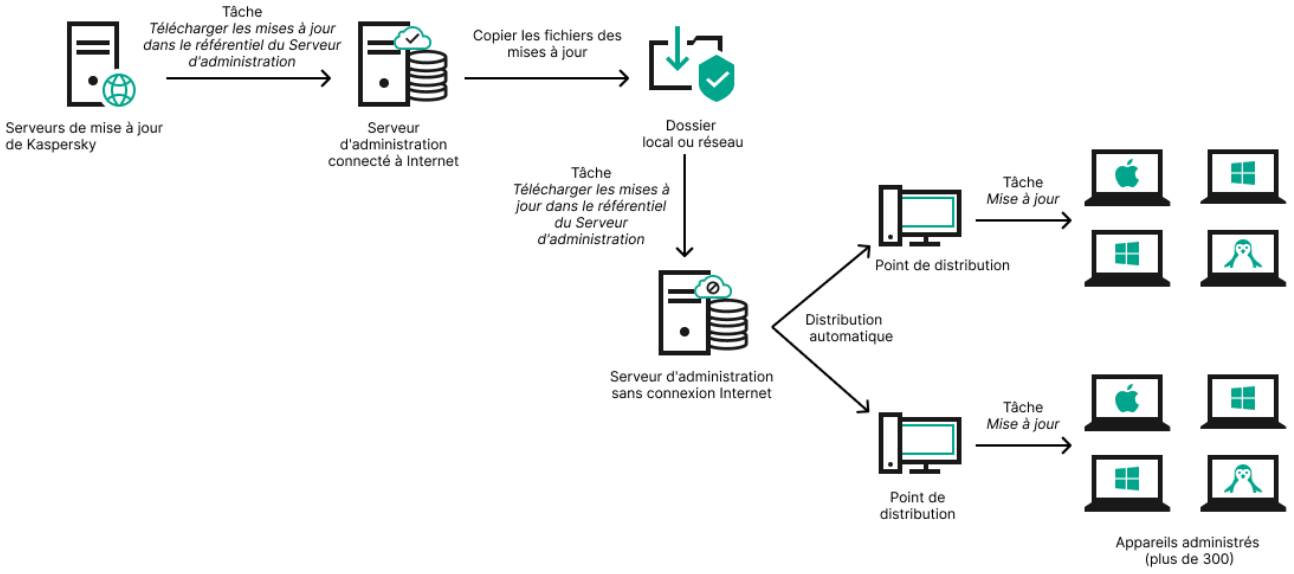
Via un dossier local ou réseau si le Serveur d'administration n'a pas de connexion Internet

Si le Serveur d'administration n'a pas de connexion Internet, vous pouvez configurer la tâche *Téléchargement des mises à jour sur le stockage du Serveur d'administration* pour télécharger les mises à jour à partir d'un dossier local ou réseau. Dans ce cas, vous devez copier les fichiers de mise à jour requis dans le dossier indiqué de temps en temps. Par exemple, vous pouvez copier les fichiers de mise à jour requis à partir de l'une des sources suivantes :

- Serveur d'administration doté d'une connexion Internet (voir la figure ci-dessous)

  Étant donné qu'un Serveur d'administration télécharge uniquement les mises à jour demandées par les applications de sécurité, les ensembles d'applications de sécurité administrés par les Serveurs d'administration (celui qui dispose d'une connexion Internet et celui qui n'en a pas) doivent correspondre.

  Si le Serveur d'administration que vous utilisez pour télécharger les mises à jour a la version 13.2 ou une version antérieure, ouvrez les propriétés de la tâche *Téléchargement des mises à jour sur le stockage du Serveur d'administration*, puis activez l'option **Télécharger les mises à jour en utilisant l'&ancien système**.



Mise à jour via un dossier local ou réseau si le Serveur d'administration n'a pas de connexion Internet

- Kaspersky Update Utility

  Étant donné que cet utilitaire utilise l'ancien schéma pour télécharger les mises à jour, ouvrez les propriétés de la tâche *Téléchargement des mises à jour sur le stockage du Serveur d'administration*, puis activez l'option **Télécharger les mises à jour en utilisant l'&ancien système**.

À propos de l'utilisation de fichiers diff pour la mise à jour des bases de données et des modules logiciels Kaspersky

Quand Kaspersky Security Center télécharge les mises à jour depuis les serveurs de mise à jour de Kaspersky, il optimise le trafic en utilisant les fichiers diff. Vous pouvez également activer l'utilisation des fichiers diff par les appareils (Serveurs d'administration, points de distribution et appareils clients) qui récupèrent les mises à jour auprès d'autres appareils sur le réseau.

À propos de la fonction de Téléchargement des fichiers diff

Un fichier diff décrit les différences entre deux version d'un fichier d'une base de données ou d'un module logiciel. Le recours aux fichiers diff économise le trafic au sein du réseau de votre entreprise car les fichiers diff occupent moins d'espace que les fichiers complets des bases de données et des modules de l'application. Si la fonction de *Téléchargement des fichiers diff* est activée sur le Serveur d'administration ou sur un point de distribution, les fichiers diff sont enregistrés sur ce Serveur d'administration ou ce point de distribution. Par conséquent, les appareils qui récupèrent les mises à jour depuis ce Serveur d'administration ou point de distribution peuvent utiliser les fichiers diff pour mettre à jour leurs bases de données et les modules de l'application.

Pour optimiser l'utilisation des fichiers diff, nous vous conseillons de synchroniser la planification des mises à jour avec la planification des mises à jour du Serveur d'administration ou du Point de distribution sur lesquels les appareils récupèrent les mises à jour. Toutefois, il est possible d'économiser du trafic même si les appareils sont mis à jour bien moins souvent que le Serveur d'administration ou le Point de distribution sur lesquels les appareils récupèrent les mises à jour.

La fonction de Téléchargement des fichiers diff peut être activée uniquement sur les Serveurs d'administration et les points de distribution à partir de la version 11. Pour enregistrer les fichiers diff sur des Serveurs d'administration et des points de distribution de versions antérieures, procédez à une mise à jour vers la version 11 ou suivante.

Le téléchargement des fichiers diff n'est pas compatible avec le modèle hors ligne de téléchargement des mises à jour. Cela signifie que les Agent d'administration qui utilisent un modèle hors ligne de téléchargement des mises à jour ne téléchargent pas les fichiers diff, même si la fonction de téléchargement des fichiers diff est activée sur le Serveur d'administration ou le point de distribution qui remet les mises hors ligne pour ces Agents d'administration.

Les points de distribution n'utilisent pas la multidiffusion IP pour distribuer automatiquement les fichiers diff.

Activation de la fonction de téléchargement des fichiers diff

Prérequis

Voici les prérequis pour ce scénario :

- Les Serveurs d'administration et les points de distribution sont mis à niveau vers la version 11 ou ultérieure.
- Le mode hors ligne de téléchargement des mises à jour est désactivé dans les paramètres de la stratégie de l'Agent d'administration.

Étapes

1. **Activation de la fonction sur le Serveur d'administration.**

   Activation de la fonction dans les paramètres de la tâche Télécharger les mises à jour dans le stockage du Serveur d'administration.

2. **Activation de la fonctionnalité pour un point de distribution**

   Activez la fonction pour un point de distribution qui reçoit les mises à jour par une tâche de Téléchargement des mises à jour sur les stockages des points de distribution.

   Activez ensuite la fonction pour un point de distribution qui récupère les mises à jour auprès d'un Serveur d'administration.

   La fonction est activée dans les paramètres de l'Agent d'administration et (si les points de distribution sont affectés manuellement et si vous souhaitez écraser les paramètres de la stratégie), dans la section **Points de distribution** des propriétés du Serveur d'administration.

Pour confirmer que la fonction de Téléchargement des fichiers diff a bien été activée, vous pouvez mesurer le trafic interne avant et après l'exécution du scénario.

Création de la tâche de téléchargement des mises à jour dans le stockage du Serveur d'administration

La tâche *Télécharger les mises à jour dans le stockage du Serveur d'administration* du Serveur d'administration est créée automatiquement lors du fonctionnement de l'Assistant de configuration initiale de l'application de Kaspersky Security Center. La tâche *Télécharger les mises à jour dans le stockage du Serveur d'administration* peut être créée en un seul exemplaire. Par conséquent, vous pouvez créer une tâche *Télécharger les mises à jour dans le stockage du Serveur d'administration* uniquement dans le cas où elle a été supprimée de la liste des tâches du Serveur d'administration.

Lancement en cours la tâche Télécharger les mises à jour dans le stockage du Serveur d'administration :

1. Dans l'arborescence de la console, sélectionnez le dossier **Tâches**.
2. Lancez le processus de création de la tâche par un des moyens suivants :

   - Dans l'arborescence de la console, dans le menu contextuel du dossier **Tâches** sélectionnez l'option **Nouveau → Tâche**.
   - Dans l'espace de travail du dossier **Tâches**, cliquez sur le bouton **Créer une tâche**.

   Ceci permet de lancer l'Assistant de création d'une tâche. Suivez les étapes de l'assistant.
3. Sur la page **Sélection du type de tâche** de l'Assistant, sélectionnez **Téléchargement des mises à jour dans le référentiel du Serveur d'administration**.

4. Sur la page **Paramètres** de l'Assistant, définissez les paramètres de la tâche comme suit :

- Sources des mises à jour

  Les ressources suivantes peuvent faire office de source des mises à jour pour le Serveur d'administration :

  - Serveurs de mises à jour de Kaspersky

    Serveurs HTTP(S) Kaspersky sur lesquels les applications de Kaspersky récupèrent les mises à jour des bases de données et des modules de l'application. Par défaut, le Serveur d'administration communique avec les serveurs de mise à jour de Kaspersky et télécharge les mises à jour au moyen du protocole HTTPS. Vous pouvez configurer le Serveur d'administration pour qu'il utilise le protocole HTTP au lieu du protocole HTTPS.

    Sélectionné par défaut.

  - Serveur d'administration principal

    Cette ressource s'applique aux tâches créées pour un Serveur d'administration virtuel ou secondaire.

  - Dossier local ou réseau

    Un dossier local ou de réseau qui contient les mises à jour les plus récentes. Un dossier de réseau peut être un serveur FTP ou HTTP ou un dossier partagé SMB. Si un dossier réseau nécessite une authentification, seul le protocole SMB est pris en charge. Lors de la sélection du dossier local, il faut indiquer le dossier sur l'appareil avec le Serveur d'administration installé.

    > Un serveur FTP ou http ou un dossier de réseau utilisé par une source des mises à jour doit contenir une structure de dossiers (avec les mises à jour) qui correspond à la structure créée lors de l'utilisation des serveurs de mise à jour de Kaspersky.

- **Autres paramètres** :

  - Forcer la mise à jour des Serveurs d'administration secondaires

    Si cette option est activée, le Serveur d'administration lance les tâches de mise à jour sur les Serveurs d'administration secondaires dès que de nouvelles mises à jour sont téléchargées. Les tâches de mise à jour sont lancées en utilisant la source de mise à jour configurée dans les propriétés de la tâche sur les Serveurs d'administration secondaires.

    Si cette option est désactivée, les tâches de mise à jour sur les Serveurs d'administration secondaires sont lancées conformément à leur programmation.

    Cette option est Inactif par défaut.

  - Copier les mises à jour récupérées dans des dossiers complémentaires

Après que le Serveur d'administration reçoit les mises à jour, il les copie dans les dossiers indiqués. Utilisez cette option si vous voulez administrer manuellement la distribution des mises à jour sur votre réseau.

Par exemple, vous pourriez vouloir utiliser cette option dans la situation suivante : le réseau de votre organisation comprend plusieurs sous-réseaux indépendants et les appareils sur chacun de ces sous-réseaux n'ont pas accès aux autres sous-réseaux. Toutefois, les appareils dans tous les sous-réseaux ont accès à un dossier partagé central. Dans ce cas, vous installez le Serveur d'administration dans un des sous-réseaux pour télécharger les mises à jour depuis les serveurs de mise à jour de Kaspersky, vous activez cette option, puis vous définissez ce dossier partagé réseau. Dans les tâches de téléchargement des mises à jour dans le stockage pour les autres Serveurs d'administration, définissez le nom du dossier réseau partagé en tant que source des mises à jour.

Cette option est Inactif par défaut.

- **Ne pas forcer la mise à jour des appareils et des Serveurs d'administration secondaires avant la fin de la copie**

  Les tâches de téléchargement des mises à jour sur les appareils clients et les Serveurs d'administration secondaires démarrent uniquement après la copie de ces mises à jour depuis le dossier de mise à jour principal vers les dossiers de mise à jour complémentaires.

  Cette option doit être activée si les appareils clients et les Serveurs d'administration secondaires téléchargent les mises à jour depuis des dossiers réseau complémentaires.

  Cette option est Inactif par défaut.

- **Télécharger les mises à jour en utilisant l'&ancien système**

  Depuis la version 14, Kaspersky Security Center télécharge les mises à jour des bases de données et des modules logiciels en utilisant le nouveau schéma. Pour que l'application télécharge les mises à jour à l'aide du nouveau schéma, la source de mise à jour doit contenir des fichiers de mise à jour avec des métadonnées compatibles avec le nouveau schéma. Si la source de mise à jour contient des fichiers de mise à jour avec des métadonnées compatibles avec l'ancien schéma uniquement, activez l'option **Télécharger les mises à jour en utilisant l'&ancien système**. Sinon, la tâche de téléchargement de la mise à jour échouera.

  Par exemple, vous devez activer cette option lorsqu'un dossier local ou réseau est spécifié comme source de mise à jour et que les fichiers de mise à jour de ce dossier ont été téléchargés par l'une des applications suivantes :

  - Kaspersky Update Utility

    Cet utilitaire télécharge les mises à jour en utilisant l'ancien schéma.

  - Kaspersky Security Center 13.2 ou version antérieure

    Par exemple, votre Serveur d'administration 1 n'a pas de connexion Internet. Dans ce cas, vous pouvez télécharger les mises à jour à l'aide d'un Serveur d'administration 2 doté d'une connexion Internet, puis placer les mises à jour dans un dossier local ou réseau pour l'utiliser comme source de mise à jour pour le Serveur d'administration 1. Si le Serveur d'administration 2 dispose de la version 13.2 ou antérieure, activez l'option **Télécharger les mises à jour en utilisant l'&ancien système** dans la tâche du Serveur d'administration 1.

  Cette option est Inactif par défaut.

5. La page **Planifier la tâche** de l'Assistant vous permet de programmer le lancement de la tâche. Le cas échéant, configurez les paramètres suivants :

- **Lancement planifié :**

  Sélectionnez la programmation de l'exécution de la tâche, puis configurez la programmation sélectionnée.

  - **Toutes les N heures**

    La tâche s'exécute régulièrement, selon l'intervalle défini en heures, à partir de la date et heure définis.

    La tâche s'exécute par défaut toutes les six heures à partir de la date et de l'heure actuelles du système.

  - **Tous les N jours**

    La tâche s'exécute régulièrement, selon l'intervalle défini en jours. En outre, vous pouvez spécifier la date et l'heure de la première exécution de la tâche. Ces options supplémentaires deviennent disponibles si elles sont prises en charge par l'application pour laquelle vous créez la tâche.

    La tâche s'exécute par défaut chaque jour, à partir de la date et de l'heure actuelle du système.

  - **Toutes les N semaines**

    La tâche s'exécute régulièrement, selon l'intervalle défini en semaines, le jour indiqué de la semaine et à l'heure indiquée.

    La tâche s'exécute par défaut chaque lundi à l'heure système actuelle.

  - **Toutes les N minutes**

    La tâche s'exécute régulièrement, à l'intervalle défini en minutes, à partir de l'heure indiquée le jour de la création de la tâche.

    La tâche s'exécute par défaut toutes les 30 minutes, à partir de l'heure actuelle du système.

  - **Chaque jour (passage à l'heure d'été non pris en charge)**

    La tâche s'exécute régulièrement, selon l'intervalle défini en jours. Cette programmation ne tient pas compte du passage à l'heure d'été. Cela signifie que lorsque les horloges sont avancées ou reculées d'une heure au début ou à la fin de l'été, l'heure de lancement réelle de la tâche ne change pas.

    Nous déconseillons d'adopter cette programmation. Elle est requise pour la rétrocompatibilité avec Kaspersky Security Center.

    La tâche démarre par défaut chaque jour à l'heure système actuelle.

  - **Chaque semaine**

    La tâche s'exécute chaque semaine, le jour défini et à l'heure indiquée.

- **Par jours de la semaine**

  La tâche s'exécute régulièrement les jours définis de la semaine, à l'heure indiquée.

  Par défaut, la tâche s'exécute chaque vendredi à 18h00.

- **Chaque mois**

  La tâche s'exécute régulièrement le jour du mois défini, à l'heure indiquée.

  Si le jour en question ne figure pas dans le mois, la tâche s'exécute le dernier jour.

  La tâche s'exécute par défaut le premier jour de chaque mois, à l'heure système actuelle.

- **Manuel**

  La tâche ne s'exécute pas automatiquement. Vous pouvez uniquement la lancer manuellement.

  Cette option est sélectionnée par défaut.

- **Chaque mois, les jours indiqués des semaines sélectionnées**

  La tâche s'exécute régulièrement les jours du mois définis, à l'heure indiquée.

  Par défaut, aucun jour du mois n'est sélectionné. L'heure de début par défaut est 18:00.

- **Lors de la détection d'une attaque de virus**

  La tâche s'exécute après un événement *Attaque de virus* de virus. Sélectionnez les types d'application qui vont surveiller les propagations de virus. Les types suivants de Application sont présent :

  - Antivirus pour postes de travail et serveurs de fichiers
  - Antivirus de protection du périmètre
  - Antivirus pour systèmes de messagerie

  Tous les types d'application sont cochés par défaut.

  Il se peut que vous souhaitiez exécuter différentes tâches en fonction du type d'application de sécurité qui signale une propagation de virus. Dans ce cas, supprimez la sélection des types d'application dont vous n'avez pas besoin.

- **Après l'exécution d'une autre tâche**

La tâche actuelle démarre à la fin d'une autre tâche. Cette option ne fonctionne que si les deux tâches sont affectées aux mêmes appareils. Par exemple, vous pouvez exécuter la tâche *Administration des appareils* avec l'option **&Activer l'appareil** et, une fois celle-ci terminée, exécuter la tâche de *recherche de virus* comme tâche de déclenchement.

Il faut sélectionner la tâche de déclenchement dans le tableau et l'état avec lequel cette tâche doit se terminer (**Terminée avec succès** ou **Échec**).

Si nécessaire, vous pouvez rechercher, trier et filtrer les tâches dans le tableau comme suit :

- Saisissez le nom de la tâche dans le champ de recherche pour rechercher une tâche par son nom.
- Cliquez sur l'icône de tri pour trier les tâches par nom.

  Par défaut, les tâches sont triées par ordre alphabétique croissant.
- Cliquez sur l'icône du filtre, et dans la fenêtre qui s'ouvre, filtrez les tâches par groupe, puis cliquez sur le bouton **Appliquer**.

- **Lancer les tâches non exécutées**

  Cette option détermine le comportement d'une tâche si un appareil client n'est pas visible sur le réseau quand la tâche est sur le point de démarrer.

  Si la case est Activé, lors du lancement suivant de l'application de Kaspersky sur cet appareil client, une tentative de lancement de la tâche sera faite. Si la programmation de la tâche est **Manuel**, **Une fois** ou **Immédiatement**, la tâche est immédiatement lancée dès que l'appareil apparaît sur le réseau ou immédiatement après l'inclusion de l'appareil dans la zone d'action de la tâche.

  Si cette option est désactivée, seules les tâches planifiées s'exécutent sur les appareils clients. Pour les planifications **Manuel**, **Une fois** et **Immédiatement**, les tâches s'exécutent uniquement sur les appareils clients qui sont visibles sur le réseau. Par exemple, vous pouvez désactiver cette option pour une tâche qui consomme des ressources que vous voulez exécuter uniquement en dehors des heures de bureau.

  Cette option est Inactif par défaut.

- **Adopter un décalage aléatoire automatique pour les lancements de tâche**

  Si cette option est activée, la tâche est lancée sur les appareils clients de manière aléatoire au cours d'un intervalle défini. C'est ce qu'on appelle un *lancement échelonné d'une tâche*. Un lancement échelonné de tâche permet d'éviter la communication simultanée d'un nombre important d'appareils clients avec le Serveur d'administration lors du lancement de la tâche programmée.

  Le temps du lancement aléatoire est automatiquement calculée lors de la création d'une tâche selon le nombre d'appareils clients sur lesquels la tâche est diffusée. Par la suite, la tâche démarre toujours à l'heure de lancement calculée. Toutefois, quand les paramètres de la tâche sont modifiés ou si la tâche est lancée manuellement, la valeur calculée de l'heure de lancement de la tâche est modifiée.

  Si la case n'est pas cochée, le lancement de la tâche sur les appareils clients s'opère selon la planification.

- **Décaler aléatoirement le lancement de la tâche dans un intervalle de (min.)**

Si cette option est activée, la tâche est lancée sur les appareils clients de manière aléatoire au cours de l'intervalle défini. Un lancement échelonné de tâche permet d'éviter la communication simultanée d'un nombre important d'appareils clients avec le Serveur d'administration lors du lancement de la tâche programmée.

Si la case n'est pas cochée, le lancement de la tâche sur les appareils clients s'opère selon la planification.

Cette option est Inactif par défaut. Par défaut, la valeur de cet intervalle est de une minute.

6. La page **Définition du nom de la tâche** de l'Assistant permet de renseigner le nom de la tâche en cours de création. Le nom de la tâche ne peut pas contenir plus de 100 symboles et contenir de symboles spéciaux ("*<>?\:|).

7. Sur la page **Fin de la création de la tâche** de l'Assistant, cliquez sur le bouton **Terminer** pour quitter l'Assistant.

   Si vous souhaitez que la tâche démarre directement à la fin de l'Assistant, cochez la case **&Lancer la tâche à la fin de l'Assistant**.

Quand l'Assistant a terminé, la tâche **Téléchargement des mises à jour dans le stockage du Serveur d'administration** apparaît dans la liste des tâches du Serveur d'administration dans l'espace de travail.

En plus des paramètres que vous définissez lors de la création de la tâche, vous pouvez modifier d'autres propriétés de la tâche créée.

Quand le Serveur d'administration exécute la tâche *Télécharger les mises à jour dans le stockage du Serveur d'administration*, les mises à jour des bases de données et des modules des applications sont copiées depuis la source de mise à jour définie vers le dossier partagé du Serveur d'administration. Si une tâche est créée pour un groupe d'administration, elle est diffusée uniquement aux Agents d'administration inclus dans le groupe d'administration indiqué.

Les mises à jour du dossier partagé sur le Serveur d'administration sont diffusées sur les appareils clients et les Serveurs d'administration secondaires.

Création de la tâche de téléchargement des mises à jour sur les stockages des points de distribution

Les appareils de points de distribution exécutant macOS ne peuvent pas télécharger les mises à jour à partir des serveurs de mises à jour de Kaspersky.

Si un ou plusieurs appareils exécutant macOS sont inclus dans la zone d'action de la tâche *Télécharger les mises à jour sur les stockages des points de distribution*, la tâche reçoit l'état *Échec*, même si elle s'est terminée avec succès sur tous les appareils Windows.

Vous pouvez créer la tâche *Télécharger les mises à jour sur les stockages des points de distribution* pour un groupe d'administration. Cette tâche est exécutée pour les points de distribution inclus dans le groupe d'administration indiqué.

Vous pouvez utiliser cette tâche par exemple si le trafic entre le Serveur d'administration et le ou les point(s) de distribution est plus cher que le trafic entre le ou les point(s) de distribution et les serveurs de mise à jour de Kaspersky ou si votre Serveur d'administration n'a pas d'accès Internet. Si le point de distribution se connecte à Internet en utilisant un serveur proxy, vous devez définir les paramètres correspondants dans la stratégie de l'Agent d'administration.

Pour créer la tâche Téléchargement des mises à jour sur les stockages des points de distribution, pour un groupe d'administration sélectionné :

1. Dans l'arborescence de la console, sélectionnez le dossier **Tâches**.

2. Dans l'espace de travail de ce dossier, cliquez sur le bouton **Nouvelle tâche**.

   Ceci permet de lancer l'Assistant de création d'une tâche. Suivez les étapes de l'assistant.

3. À la page **Sélection du type de tâche** de l'Assistant, sélectionnez le nœud **Serveur d'administration de Kaspersky Security Center**, développez le dossier **Avancé**, puis sélectionnez la tâche **Téléchargement des mises à jour sur les stockages des points de distribution**.

4. Sur la page **Paramètres** de l'Assistant, définissez les paramètres de la tâche comme suit :

- **Sources des mises à jour**

  Les ressources suivantes peuvent faire office de source des mises à jour pour le point de distribution :

  - Serveurs de mise à jour de Kaspersky

    Serveurs HTTP(S) Kaspersky sur lesquels les applications de Kaspersky récupèrent les mises à jour des bases de données et des modules de l'application.

    Par défaut, cette option est sélectionnée.

  - Dossier local ou réseau

    Un dossier local ou de réseau qui contient les mises à jour les plus récentes. Un dossier de réseau peut être un serveur FTP ou HTTP ou un dossier partagé SMB. Si un dossier réseau nécessite une authentification, seul le protocole SMB est pris en charge. Lors de la sélection du dossier local, il faut indiquer le dossier sur l'appareil avec le Serveur d'administration installé.

    > Un serveur FTP ou http ou un dossier de réseau utilisé par une source des mises à jour doit contenir une structure de dossiers (avec les mises à jour) qui correspond à la structure créée lors de l'utilisation des serveurs de mise à jour de Kaspersky.

- **Dossier de stockage des mises à jour**

  Le chemin d'accès au dossier spécifié pour stocker les mises à jour enregistrées. Vous pouvez copier le chemin du dossier spécifié dans un presse-papiers. Vous ne pouvez pas modifier le chemin d'accès à un dossier spécifié pour une tâche de groupe.

- **Télécharger les mises à jour en utilisant l'&ancien système**

  Depuis la version 14, Kaspersky Security Center télécharge les mises à jour des bases de données et des modules logiciels en utilisant le nouveau schéma. Pour que l'application télécharge les mises à jour à l'aide du nouveau schéma, la source de mise à jour doit contenir les fichiers de mise à jour avec les métadonnées compatibles avec le nouveau schéma. Si la source de mise à jour contient les fichiers de mise à jour avec les métadonnées compatibles avec l'ancien schéma uniquement, activez l'option **Télécharger les mises à jour en utilisant l'&ancien système**. Sinon, la tâche de téléchargement de la mise à jour échouera.

  Par exemple, vous devez activer cette option lorsqu'un dossier local ou réseau est spécifié comme source de mise à jour et que les fichiers de mise à jour de ce dossier ont été téléchargés par l'une des applications suivantes :

  - Kaspersky Update Utility

    Cet utilitaire télécharge les mises à jour en utilisant l'ancien schéma.

  - Kaspersky Security Center 13.2 ou version antérieure

    Par exemple, un point de distribution est configuré pour prendre les mises à jour d'un dossier local ou réseau. Dans ce cas, vous pouvez télécharger les mises à jour à l'aide d'un Serveur d'administration doté d'une connexion Internet, puis placer les mises à jour dans le dossier local du point de distribution. Si le Serveur d'administration dispose de la version 13.2 ou antérieure, activez l'option **Télécharger les mises à jour en utilisant l'&ancien système** dans la tâche *Télécharger les mises à jour dans les stockages des points de distribution*.

  Cette option est Inactif par défaut.

5. Sur la page **Sélectionnez un Groupe d'administration**, cliquez sur **Parcourir** et sélectionnez le groupe d'administration auquel la tâche s'applique.

6. La page **Planifier la tâche** de l'Assistant vous permet de programmer le lancement de la tâche. Le cas échéant, configurez les paramètres suivants :

- **Programmation :**

  Sélectionnez la programmation de l'exécution de la tâche, puis configurez la programmation sélectionnée.

  - **Toutes les N heures**

    La tâche s'exécute régulièrement, selon l'intervalle défini en heures, à partir de la date et heure définis.

    La tâche s'exécute par défaut toutes les six heures à partir de la date et de l'heure actuelles du système.

  - **Tous les N jours**

    La tâche s'exécute régulièrement, selon l'intervalle défini en jours. En outre, vous pouvez spécifier la date et l'heure de la première exécution de la tâche. Ces options supplémentaires deviennent disponibles si elles sont prises en charge par l'application pour laquelle vous créez la tâche.

    La tâche s'exécute par défaut chaque jour, à partir de la date et de l'heure actuelle du système.

  - **Toutes les N semaines**

    La tâche s'exécute régulièrement, selon l'intervalle défini en semaines, le jour indiqué de la semaine et à l'heure indiquée.

    La tâche s'exécute par défaut chaque lundi à l'heure système actuelle.

  - **Toutes les N minutes**

    La tâche s'exécute régulièrement, à l'intervalle défini en minutes, à partir de l'heure indiquée le jour de la création de la tâche.

    La tâche s'exécute par défaut toutes les 30 minutes, à partir de l'heure actuelle du système.

  - **Chaque jour (passage à l'heure d'été non pris en charge)**

    La tâche s'exécute régulièrement, selon l'intervalle défini en jours. Cette programmation ne tient pas compte du passage à l'heure d'été. Cela signifie que lorsque les horloges sont avancées ou reculées d'une heure au début ou à la fin de l'été, l'heure de lancement réelle de la tâche ne change pas.

    Nous déconseillons d'adopter cette programmation. Elle est requise pour la rétrocompatibilité avec Kaspersky Security Center.

    La tâche démarre par défaut chaque jour à l'heure système actuelle.

  - **Chaque semaine**

    La tâche s'exécute chaque semaine, le jour défini et à l'heure indiquée.

- **Par jours de la semaine**

  La tâche s'exécute régulièrement les jours définis de la semaine, à l'heure indiquée.

  Par défaut, la tâche s'exécute chaque vendredi à 18h00.

- **Chaque mois**

  La tâche s'exécute régulièrement le jour du mois défini, à l'heure indiquée.

  Si le jour en question ne figure pas dans le mois, la tâche s'exécute le dernier jour.

  La tâche s'exécute par défaut le premier jour de chaque mois, à l'heure système actuelle.

- **Manuel**

  La tâche ne s'exécute pas automatiquement. Vous pouvez uniquement la lancer manuellement.

  Cette option est sélectionnée par défaut.

- **Chaque mois, les jours indiqués des semaines sélectionnées**

  La tâche s'exécute régulièrement les jours du mois définis, à l'heure indiquée.

  Par défaut, aucun jour du mois n'est sélectionné. L'heure de début par défaut est 18:00.

- **Lors de la détection d'une attaque de virus**

  La tâche s'exécute après un événement *Attaque de virus* de virus. Sélectionnez les types d'application qui vont surveiller les propagations de virus. Les types suivants de Application sont présent :

  - Antivirus pour postes de travail et serveurs de fichiers
  - Antivirus de protection du périmètre
  - Antivirus pour systèmes de messagerie

  Tous les types d'application sont cochés par défaut.

  Il se peut que vous souhaitiez exécuter différentes tâches en fonction du type d'application de sécurité qui signale une propagation de virus. Dans ce cas, supprimez la sélection des types d'application dont vous n'avez pas besoin.

- **Après l'exécution d'une autre tâche**

La tâche actuelle démarre à la fin d'une autre tâche. Cette option ne fonctionne que si les deux tâches sont affectées aux mêmes appareils. Par exemple, vous pouvez exécuter la tâche *Administration des appareils* avec l'option **&Activer l'appareil** et, une fois celle-ci terminée, exécuter la tâche de *recherche de virus* comme tâche de déclenchement.

Il faut sélectionner la tâche de déclenchement dans le tableau et l'état avec lequel cette tâche doit se terminer (**Terminée avec succès** ou **Échec**).

Si nécessaire, vous pouvez rechercher, trier et filtrer les tâches dans le tableau comme suit :

- Saisissez le nom de la tâche dans le champ de recherche pour rechercher une tâche par son nom.
- Cliquez sur l'icône de tri pour trier les tâches par nom.

  Par défaut, les tâches sont triées par ordre alphabétique croissant.
- Cliquez sur l'icône du filtre, et dans la fenêtre qui s'ouvre, filtrez les tâches par groupe, puis cliquez sur le bouton **Appliquer**.

- **Lancer les tâches non exécutées**

  Cette option détermine le comportement d'une tâche si un appareil client n'est pas visible sur le réseau quand la tâche est sur le point de démarrer.

  Si la case est Activé, lors du lancement suivant de l'application de Kaspersky sur cet appareil client, une tentative de lancement de la tâche sera faite. Si la programmation de la tâche est **Manuel**, **Une fois** ou **Immédiatement**, la tâche est immédiatement lancée dès que l'appareil apparaît sur le réseau ou immédiatement après l'inclusion de l'appareil dans la zone d'action de la tâche.

  Si cette option est désactivée, seules les tâches planifiées s'exécutent sur les appareils clients. Pour les planifications **Manuel**, **Une fois** et **Immédiatement**, les tâches s'exécutent uniquement sur les appareils clients qui sont visibles sur le réseau. Par exemple, vous pouvez désactiver cette option pour une tâche qui consomme des ressources que vous voulez exécuter uniquement en dehors des heures de bureau.

  Cette option est Inactif par défaut.

- **Adopter un décalage aléatoire automatique pour les lancements de tâche**

  Si cette option est activée, la tâche est lancée sur les appareils clients de manière aléatoire au cours d'un intervalle défini. C'est ce qu'on appelle un *lancement échelonné d'une tâche*. Un lancement échelonné de tâche permet d'éviter la communication simultanée d'un nombre important d'appareils clients avec le Serveur d'administration lors du lancement de la tâche programmée.

  Le temps du lancement aléatoire est automatiquement calculée lors de la création d'une tâche selon le nombre d'appareils clients sur lesquels la tâche est diffusée. Par la suite, la tâche démarre toujours à l'heure de lancement calculée. Toutefois, quand les paramètres de la tâche sont modifiés ou si la tâche est lancée manuellement, la valeur calculée de l'heure de lancement de la tâche est modifiée.

  Si la case n'est pas cochée, le lancement de la tâche sur les appareils clients s'opère selon la planification.

- **Décaler aléatoirement le lancement de la tâche dans un intervalle de (min.)**

Si cette option est activée, la tâche est lancée sur les appareils clients de manière aléatoire au cours de l'intervalle défini. Un lancement échelonné de tâche permet d'éviter la communication simultanée d'un nombre important d'appareils clients avec le Serveur d'administration lors du lancement de la tâche programmée.

Si la case n'est pas cochée, le lancement de la tâche sur les appareils clients s'opère selon la planification.

Cette option est Inactif par défaut. Par défaut, la valeur de cet intervalle est de une minute.

7. La page **Définition du nom de la tâche** de l'Assistant permet de renseigner le nom de la tâche en cours de création. Le nom de la tâche ne peut pas contenir plus de 100 symboles et contenir de symboles spéciaux ("*<>?\:|).

8. Sur la page **Fin de la création de la tâche** de l'Assistant, cliquez sur le bouton **Terminer** pour quitter l'Assistant.

   Si vous souhaitez que la tâche démarre directement à la fin de l'Assistant, cochez la case **&Lancer la tâche à la fin de l'Assistant**.

Une fois que l'Assistant a terminé **Téléchargement des mises à jour sur les stockages des points de distribution** apparaît dans la liste des tâches de l'Agent d'administration dans le groupe d'administration correspondant et dans l'espace de travail **Tâches** de la console.

En plus des paramètres que vous définissez lors de la création de la tâche, vous pouvez modifier d'autres propriétés de la tâche créée.

Suite à l'exécution de la tâche de *Téléchargement des mises à jour sur les stockages des points de distribution*, les mises à jour des bases de données et des modules des applications sont copiées depuis la source des mises à jour et placées dans le dossier partagé. Les mises à jour chargées sont utilisées uniquement par les points de distribution qui appartiennent au groupe d'administration indiqué et pour lesquels il n'existe aucune tâche de téléchargement des mises à jour clairement définie.

Dans la fenêtre des propriétés du Serveur d'administration, dans le volet **Sections**, sélectionnez **Points de distribution**. Dans les propriétés de chaque point de distribution, dans la section **Source des mises à jour**, vous pouvez indiquer la source des mises à jour (**&Récupérer depuis le Serveur d'administration** ou **Utiliser la tâche de téléchargement forcé des mises à jour**). L'option choisie par défaut pour un point de distribution affecté manuellement ou automatiquement est **&Récupérer depuis le Serveur d'administration**. Ces points de distribution utiliseront les résultats de la tâche *Télécharger les mises à jour sur les stockages des points de distribution*.

Les propriétés de chaque point de distribution reprennent le dossier réseau configuré individuellement pour ce point de distribution. Les noms des dossiers peuvent différer pour différents points de distribution. C'est la raison pour laquelle il est déconseillé de modifier le dossier réseau des mises à jour dans les propriétés de la tâche quand la tâche est créée pour un groupe d'appareils.

Vous pouvez modifier le dossier réseau des mises à jour dans les propriétés de la tâche *Télécharger les mises à jour sur les stockages des points de distribution* si vous créez une tâche locale pour l'appareil.

Configuration de la tâche Télécharger les mises à jour dans le stockage du Serveur d'administration

Pour configurer la tâche Télécharger les mises à jour dans le stockage du Serveur d'administration, procédez comme suit :

1. Dans l'espace de travail du dossier de l'arborescence de la console **Tâches**, sélectionnez la tâche **Téléchargement des mises à jour dans le stockage du Serveur d'administration** dans la liste des tâches.

2. Ouvrez la fenêtre des propriétés de la tâche à l'aide d'un des moyens suivants :

   - En sélectionnant **Propriétés** dans le menu contextuel de la tâche.

   - En cliquant sur le lien **Configurer les paramètres de la tâche** dans la zone d'informations correspondant à la tâche sélectionnée.

   La fenêtre des propriétés de la tâche *Télécharger les mises à jour dans le stockage du Serveur d'administration* s'ouvre. Cette fenêtre permet de configurer les paramètres de téléchargement des mises à jour dans le stockage du Serveur d'administration.

Analyse des mises à jour récupérées

Avant l'installation des mises à jour sur les appareils administrés, vous pouvez d'abord vérifier l'efficacité des mises à jour et rechercher les erreurs via la tâche *Vérification de la mise à jour*. Au cours de la tâche de *Téléchargement des mises à jour sur le stockage du Serveur d'administration*, la tâche *Vérification de la mise à jour* est exécutée automatiquement. Le Serveur d'administration télécharge les mises à jour depuis la source, les enregistre dans le stockage temporaire et exécute la tâche *Vérification de la mise à jour*. Si la tâche réussit, les mises à jour sont copiées depuis le stockage temporaire vers le dossier partagé du Serveur d'administration (<Dossier d'installation de Kaspersky Security Center>\Share\Updates). Elles sont diffusées à l'ensemble des appareils clients pour lesquels le Serveur d'administration est la source des mises à jour.

Si, à la suite de la tâche *Vérification de la mise à jour*, les mises à jour situées dans le référentiel temporaire sont incorrectes ou si la tâche *Vérification de la mise à jour* se termine avec une erreur, ces mises à jour ne sont pas copiées dans le dossier partagé. La version précédente des mises à jour est conservée sur le Serveur d'administration. De plus, les tâches disposant du type de programmation **Lors du téléchargement des mises à jour dans le stockage** n'ont pas encore été lancées. Ces opérations sont réalisées à la prochaine exécution de la tâche *Téléchargement des mises à jour sur le stockage du Serveur d'administration*, si l'analyse des nouvelles mises à jour réussit.

L'ensemble de mises à jour est considéré comme incorrect si une des conditions suivantes est remplie sur au moins un appareil d'essai :

- Une erreur s'est produite pendant l'exécution de la tâche de mise à jour.

- Après l'application des mises à jour, l'état de la protection en temps réel de l'application de sécurité est modifié.

- Un objet infecté a été identifié durant la tâche d'analyse à la demande.

- Une erreur de l'application de Kaspersky s'est produite.

Si aucune des conditions citées n'est remplie sur aucun des appareils d'essai, alors les mises à jour sont considérées comme correctes et la tâche *Vérification de la mise à jour* a réussi.

Avant de commencer à créer la tâche *Vérification de la mise à jour*, réalisez les prérequis :

1. Créez un groupe d'administration avec plusieurs appareils de test. Vous aurez besoin de ce groupe pour vérifier ses mises à jour.

   Nous recommandons d'utiliser des appareils bien protégés avec la configuration logicielle la plus répandue dans le réseau de l'entreprise. Cette approche augmente la qualité et la probabilité de détection des virus lors des analyses et minimise le risque de faux positifs. En cas de détection de virus sur les appareils d'essai, la tâche d'*analyse des mises à jour* échoue.

2. Créez les tâches *Mise à jour* et *Recherche d'applications malveillantes* pour une application prise en charge par Kaspersky Security Center, par exemple, Kaspersky Endpoint Security for Windows ou Kaspersky Security for Windows Server. Lors de la création des tâches *Mise à jour* et *Recherche d'applications malveillantes*, indiquez le groupe d'administration avec les appareils de test.

   La tâche *Vérification de la mise à jour* exécute séquentiellement les tâches *Mise à jour* et *Recherche d'applications malveillantes* sur les appareils de test pour vérifier que toutes les mises à jour sont valides. De plus, lors de la création de la tâche *Vérification de la mise à jour*, vous devez spécifier les tâches *Mise à jour* et *Recherche d'applications malveillantes*.

3. Créer la tâche *Téléchargement des mises à jour sur le stockage du Serveur d'administration*.

Pour que Kaspersky Security Center analyse les mises à jour reçues avant de les diffuser sur les appareils clients, procédez comme suit :

1. Dans l'espace de travail du dossier **Tâches**, sélectionnez la tâche *Téléchargement des mises à jour sur le stockage du Serveur d'administration* dans la liste des tâches.

2. Ouvrez la fenêtre des propriétés de la tâche à l'aide d'un des moyens suivants :

   - En sélectionnant **Propriétés** dans le menu contextuel de la tâche.
   - A l'aide du lien **Configurer les paramètres de la tâche** dans la zone d'informations de la tâche sélectionnée.

3. Si la tâche *Vérification de la mise à jour* existe, cliquez sur le bouton **Parcourir**. Dans la fenêtre qui s'ouvre, sélectionnez la tâche *Vérification de la mise à jour* dans le groupe d'administration avec les appareils de test.

4. Si vous n'avez pas créé la tâche *Vérification de la mise à jour* auparavant, cliquez sur le bouton **Créer**.

   L'Assistant de création de la tâche *Vérification de la mise à jour* démarre. Suivez les instructions de l'assistant.

5. Fermez la fenêtre des propriétés de la tâche de *Téléchargement des mises à jour sur le stockage du Serveur d'administration* en cliquant sur le bouton **OK**.

La vérification de la mise à jour automatique est activée. Vous pouvez maintenant exécuter la tâche *Téléchargement des mises à jour sur le stockage du Serveur d'administration* et elle démarrera à partir de la vérification des mises à jour.

Configuration des stratégies de vérification et des tâches auxiliaires

Lors de la création d'une tâche d'*analyse des mises à jour*, le Serveur d'administration crée des stratégies de vérification, ainsi que des tâches de groupe auxiliaires de mise à jour et d'analyse à la demande.

L'exécution des tâches de groupe auxiliaires de mise à jour et de l'analyse à la demande prend un certain temps. Ces tâches sont exécutées dans le cadre d'exécution de la tâche d'*analyse des mises à jour*. La tâche *Analyse des mises à jour* est exécutée dans le cadre d'exécution de la tâche *Télécharger les mises à jour dans le stockage*. Le temps d'exécution de la tâche *Télécharger les mises à jour dans le stockage* inclut le temps d'exécution des tâches de groupe auxiliaires de mise à jour et de l'analyse à la demande.

Vous pouvez modifier les paramètres des stratégies de test et des tâches auxiliaires.

Pour modifier les paramètres de la stratégie de test ou de la tâche auxiliaire, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le groupe pour lequel la tâche d'*analyse des mises à jour* sera formée.
2. L'espace de travail permet de sélectionner un des onglets suivants :
   - **Stratégies** si vous voulez modifier les paramètres de la stratégie de vérification.
   - **Tâches** si vous voulez modifier les paramètres de la tâche auxiliaire.
3. Dans l'espace de travail de l'onglet, sélectionnez la stratégie ou la tâche les paramètres de laquelle vous voulez modifier.
4. Ouvrez la fenêtre des propriétés de cette stratégie (tâche) à l'aide d'un des moyens suivants :
   - En sélectionnant **Propriétés** dans le menu contextuel de la stratégie (tâche).
   - En cliquant sur le lien **Configurer une stratégie** (**Configurer les paramètres de la tâche**) dans la zone d'informations correspondant à la stratégie (tâche) sélectionnée.

Pour que l'analyse des mises à jour soit exécutée correctement, il faut suivre les restrictions suivantes sur la modification des paramètres des stratégies de vérification et des tâches auxiliaires :

- Dans les paramètres des tâches auxiliaires :
  - Enregistrer sur le Serveur d'administration toutes les tâches correspondant aux niveaux d'importance **Événement critique** et **Erreur de fonctionnement**. Sur la base des événements de ce type, le Serveur d'administration analyse le fonctionnement des applications.
  - Utiliser le Serveur d'administration en tant que source des mises à jour.
  - Définir le type de programmation des tâches : **Manuel**.
- Dans les paramètres des stratégies de vérification :
  - Désactivez les technologies d'accélération d'analyse iChecker et iSwift (**Protection principale → Protection contre les fichiers malicieux → Paramètres → Supplémentaire → Technologies de numérisation**).
  - Sélectionnez des actions sur des objets infectés : **Désinfecter ; supprimer si la désinfection échoue** / **Désinfecter ; bloquer si la désinfection échoue** / **Bloquer**. (**Protection principale → Protection contre les fichiers malicieux → Action sur la détection des menaces**).
- Dans les paramètres des stratégies de vérification et des tâches auxiliaires :

  Si le redémarrage de l'appareil est requis après l'installation des mises à jour des modules logiciels, il faut l'exécuter sans attendre. Si l'appareil n'est pas redémarré, il sera impossible de vérifier ce type de mise à jour. Pour certaines applications, l'installation de mises à jour qui requièrent un redémarrage peut être interdites ou réalisées uniquement après confirmation de l'utilisateur. Ces restrictions doivent être désactivées dans les paramètres des stratégies de vérification et des tâches auxiliaires.

Affichage des mises à jour récupérées

Pour consulter la liste des mises à jour reçues,

Dans l'arborescence de la console du dossier **Stockages**, sélectionnez le sous-dossier **Mises à jour pour les bases de données de Kaspersky et modules logiciels**.

L'espace de travail du dossier **Mises à jour pour les bases de données de Kaspersky et modules logiciels** présente la liste des mises à jour enregistrées sur le Serveur d'administration.

Installation automatique des mises à jour pour Kaspersky Endpoint Security sur les appareils

Vous pouvez configurer automatiquement la mise à jour des bases de données et des modules de l'application Kaspersky Endpoint Security sur les appareils clients.

Pour configurer le téléchargement et l'installation automatique des mises à jour de Kaspersky Endpoint Security sur les appareils, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le dossier **Tâches**.
2. Créez une tâche de type **Mise à jour** selon l'un des procédés suivants :

   - En sélectionnant **Nouveau → Tâche** dans le menu contextuel du dossier **Tâches** dans l'arborescence de la console.
   - En cliquant sur le bouton **Nouvelle tâche** dans l'espace de travail du dossier **Tâches**.

   Ceci permet de lancer l'Assistant de création d'une tâche. Suivez les étapes de l'assistant.
3. Sur la page **Sélection du type de tâche** de l'Assistant, sélectionnez **Kaspersky Endpoint Security** en tant que type de tâche, puis **Mise à jour** en tant que sous-type de tâche.
4. Suivez les étapes ultérieures de l'assistant.

   Suite à l'exécution de l'assistant, une tâche de mise à jour est créée pour Kaspersky Endpoint Security. La tâche créée est affichée dans la liste de tâches de l'espace de travail du dossier **Tâches**.
5. Dans l'espace de travail du dossier **Tâches**, sélectionnez la tâche de mise à jour que vous avez créée.
6. Dans le menu contextuel de la tâche, choisissez l'option **Propriétés**.
7. Dans la fenêtre des propriétés de la tâche qui s'ouvre, dans le volet **Sections**, sélectionnez **Options**.

   La section **Options** permet de configurer les paramètres de la tâche de mise à jour en mode local ou mobile :

   - **Paramètres de mise à jour en mode local** : la connexion est établie entre l'appareil et le Serveur d'administration.
   - **Paramètres de mise à jour en mode mobile** : la communication n'est pas établie entre l'appareil et Kaspersky Security Center (par exemple, quand l'appareil n'est pas connecté à Internet).
8. Cliquez sur le bouton **Configuration** pour sélectionner la source des mises à jour.
9. Sélectionnez l'option **Télécharger les mises à jour des modules de l'application** pour télécharger et installer les mises à jour des modules de l'application avec les bases de l'application.

   Si la case est cochée, Kaspersky Endpoint Security notifie l'utilisateur de la présence de mises à jour disponibles pour les modules de l'application. En outre, au cours de l'exécution de la tâche, Kaspersky Endpoint Security inclut les mises à jour de l'application au paquet de mises à jour. Configurez l'application des modules de mises à jour :

   - **Installer les mises à jour critiques et approuvées**. En présence de mises à jour de modules de l'application, Kaspersky Endpoint Security installe automatiquement celles avec l'état *Critique* ; les autres mises à jour sont installées après votre approbation.
   - **Installer uniquement les mises à jour confirmées**. Si des mises à jours des modules de l'application sont disponibles, Kaspersky Endpoint Security les installe après approbation, en local via l'interface de l'application ou à l'aide de Kaspersky Security Center.

   Si la mise à jour des modules implique la lecture et l'acception des conditions du Contrat de licence et de la Politique de confidentialité, l'application installe les mises à jour après que l'utilisateur a accepté ces conditions.

10. Sélectionnez l'option **Copier les mises à jour dans un dossier** pour que l'application enregistre les mises à jour téléchargées dans un dossier, puis cliquez sur **Parcourir** pour définir le dossier.

11. Cliquez sur le bouton **OK**.

Lors de l'exécution de la tâche **Mise à jour**, l'application envoie des requêtes aux serveurs de mise à jour de Kaspersky.

Certaines mises à jour requièrent l'installation des versions les plus récentes des plug-ins d'administration.

Modèle hors ligne de téléchargement des mises à jour

L'Agent d'administration sur les appareils administrés ne peut pas toujours se connecter au Serveur d'administration pour la réception des mises à jour. Par exemple, l'Agent d'administration peut être installé sur un ordinateur portable qui, parfois, n'est pas connecté à Internet et au réseau local. L'administrateur peut également limiter la durée de connexion des appareils au réseau. Dans ces cas, l'Agent d'administration installé ne peut pas recevoir les mises à jour provenant du Serveur d'administration conformément à l'emploi du temps. Si la mise à jour des applications administrées est configurée (par exemple, Kaspersky Endpoint Security) à l'aide de l'Agent d'administration, chaque mise à jour nécessite une connexion au Serveur d'administration. Lorsque l'Agent d'administration et le Serveur d'administration ne sont pas connectés, la mise à jour est impossible. La connexion de l'Agent d'administration au Serveur d'administration peut être configurée de manière à s'effectuer seulement dans un délai défini. Au pire des cas, si les périodes de connexion configurées sont dépassées, lorsque la connexion est absente, les bases ne sont jamais mises à jour. Dans certaines situations, également, de nombreuses applications administrées s'adressent simultanément au Serveur d'administration pour des mises à jour. Dans ce cas, le Serveur d'administration peut arrêter de répondre aux requêtes (comme pendant une attaque DDoS).

Pour éviter les problèmes décrits, Kaspersky Security Center prévoit un modèle hors ligne de téléchargement de la mise à jour des bases de données et des modules des applications administrées. Ce modèle assure le mécanisme de diffusion des mises à jour quels que soient les problèmes temporaires d'indisponibilité des canaux de communication du Serveur d'administration et réduit la charge sur le Serveur d'administration. Le modèle réduit également la charge sur le Serveur d'administration.

Fonctionnement du modèle hors ligne de téléchargement des mises à jour

Quand le serveur d'administration reçoit des mises à jour, il signale à l'Agent d'administration (sur les appareils où il est installé) les mises à jour qui seront requises pour les applications administrées. Quand l'Agent d'administration reçoit des informations sur les mises à jour, il télécharge les fichiers nécessaires au préalable sur le Serveur d'administration. Lors de la première connexion à Agent d'administration, le Serveur d'administration initialise le téléchargement des mises à jour. Une fois que l'Agent d'administration sur l'appareil client a téléchargé toutes les mises à jour, celles-ci deviennent accessibles aux applications situées sur ce même appareil.

Lorsque l'application administrée sur l'appareil client s'adresse à l'Agent d'administration pour obtenir des mises à jour, l'Agent vérifie s'il a les mises à jour nécessaires. Si des mises à jour ont été reçues du Serveur d'administration au plus tôt 25 heures après la requête de l'application administrée, l'Agent d'administration ne se connecte pas au Serveur d'administration et fournit à l'application administrée des mises à jour du cache local. Il se peut que la connexion au Serveur d'administration ne soit pas établie lorsque l'Agent d'administration fournit les mises à jour aux applications sur les appareils client, mais la connexion n'est pas requise pour la mise à jour.

Pour répartir le téléchargement sur le Serveur d'administration, l'Agent d'administration commence à se connecter au serveur et à télécharger les mises à jour de manière aléatoire au cours du délai défini par le serveur. Ce délai dépend du nombre d'appareils dont l'Agent d'administration installé télécharge les mises à jour et de la taille de celles-ci. Pour réduire la charge du Serveur d'administration, vous pouvez utiliser l'Agent d'administration comme points de distribution.

Si le modèle hors ligne pour le téléchargement des mises à jour est désactivé, les mises à jour sont diffusées selon la programmation de la tâche de téléchargement des mises à jour

Par défaut, le modèle hors ligne de téléchargement des mises à jour est activé.

Le modèle hors ligne de téléchargement des mises à jour intervient uniquement pour les appareils administrés pour lesquels la planification de la tâche de récupération des mises à jour par les applications administrées a pour valeur **Lors du téléchargement des mises à jour dans le stockage**. Pour les autres appareils administrés, la récupération des mises à jour s'opère via le système traditionnel en temps réel de récupération depuis le Serveur d'administration.

Il est recommandé de désactiver le modèle hors ligne de téléchargement des mises à jour via les paramètres des stratégies de l'Agent d'administration des groupes d'administration correspondant dans les cas suivants : si, dans les applications administrées, le téléchargement des mises à jour est configurée pour avoir lieu non pas depuis le Serveur d'administration, mais depuis les serveurs de Kaspersky ou un dossier réseau et si la planification de cette tâche est définie sur **Lors du téléchargement des mises à jour dans le stockage**.

Activation et désactivation d'un modèle hors ligne de téléchargement des mises à jour

Il est déconseillé de désactiver le modèle hors ligne de téléchargement des mises à jour. La désactivation peut entraîner un échec dans la remise des mises à jour aux appareils. Dans certains cas, un expert du Support Technique de Kaspersky peut vous recommander de décocher la case **Télécharger au préalable les mises à jour et les bases antivirus depuis le Serveur d'administration**. Ensuite, vous devrez confirmer que la tâche de récupération des mises à jour pour les applications de Kaspersky a été configurée.

Pour activer ou désactiver le modèle hors ligne de téléchargement des mises à jour pour le groupe d'administration, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le groupe d'administration pour lequel il faut activer le modèle hors ligne de téléchargement des mises à jour.

2. Dans l'espace de travail du groupe, ouvrez l'onglet **Stratégies**.

3. Dans l'onglet **Stratégies**, choisissez la stratégie de l'Agent d'administration.

4. Dans le menu contextuel de la stratégie, sélectionnez l'option **Propriétés**.

   Ouvrez la fenêtre des propriétés de la stratégie de l'Agent d'administration.

5. Sélectionnez la section **Administration des correctifs et des mises à jour** dans la fenêtre des propriétés de la stratégie.

6. Sélectionnez ou désélectionnez la case à cocher **&Télécharger au préalable les mises à jour et les bases antivirus depuis le Serveur d'administration (recommandé)** pour activer ou désactiver, respectivement, le modèle hors ligne de téléchargement de mise à jour.

   Par défaut, le modèle hors ligne de téléchargement des mises à jour est activé.

Suite à cette action, le modèle hors ligne de téléchargement des mises à jour est activé ou désactivé.

Installation automatique des mises à jour et des correctifs pour les modules de Kaspersky Security Center

L'installation automatique des mises à jour et des correctifs téléchargés a lieu par défaut automatiquement pour les modules suivants de l'application :

- Agent d'administration pour Windows
- Console d'administration
- Serveur MDM iOS

L'installation automatique des mises à jour et des correctifs pour les modules de Kaspersky Security Center est uniquement disponible sur les appareils tournant sous Windows. Vous pouvez désactiver l'installation automatique des mises à jour et des correctifs pour ces modules. Dans ce cas, les mises à jour et les correctifs téléchargés sont installées seulement après que vous avez modifié leur état sur *Approuvée*. Les mises à jour et les correctifs avec l'état *Non défini* ne sont pas installés.

Activation et désactivation de l'installation automatique des mises à jour et des correctifs pour les modules de Kaspersky Security Center

L'installation automatique des mises à jour pour les modules de Kaspersky Security Center est activée par défaut lors de l'installation de l'Agent d'administration sur l'appareil. Vous pouvez la désactiver lors de l'installation de l'Agent d'administration ou plus tard, à l'aide d'une stratégie.

Pour désactiver l'installation automatique des mises à jour pour les modules de Kaspersky Security Center lors de l'installation locale de l'Agent d'administration sur l'appareil, procédez comme suit :

1. Lancez l'installation locale de l'Agent d'administration sur l'appareil.
2. À l'étape **Paramètres complémentaires**, décochez la case **Installer automatiquement les mises à jour et les correctifs applicables aux composants dont la case à cocher de statut est Non défini**.
3. Suivez les instructions de l'assistant.

L'Agent d'administration s'installe sur l'appareil sans l'option d'installé des mises à jour et des correctifs pour les modules de Kaspersky Security Center. Vous pouvez activer l'installation automatique plus tard à l'aide d'une stratégie.

Pour désactiver l'installation automatique des mises à jour pour les modules de Kaspersky Security Center lors de l'installation de l'Agent d'administration sur l'appareil à l'aide d'un paquet d'installation, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le dossier **Installation à distance → Paquets d'installation**.
2. Dans le menu contextuel du paquet **Agent d'administration de Kaspersky Security Center <version number>**, sélectionnez **Propriétés**.
3. Dans les propriétés du paquet d'installation, dans la section **Paramètres**, décochez la case **Installer automatiquement les mises à jour et les correctifs nécessaires pour les modules dont l'état est Non défini**.

L'Agent d'administration est installé depuis ce paquet avec l'option d'installation automatique des mises à jour et des correctifs pour les modules de Kaspersky Security Center désactivée. Vous pouvez activer l'installation automatique plus tard à l'aide d'une stratégie.

Si lors de l'installation de l'Agent d'administration sur un appareil la case a été cochée (décochée), vous pouvez ultérieurement désactiver (activer) l'installation automatique à l'aide d'une stratégie de l'Agent d'administration.

Pour activer ou désactiver l'installation automatique des mises à jour et les correctifs pour les modules de Kaspersky Security Center à l'aide d'une stratégie de l'Agent d'administration, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le groupe d'administration pour lequel il faut activer ou désactiver l'installation automatiquement des mises à jour et des correctifs.
2. Dans l'espace de travail du groupe, ouvrez l'onglet **Stratégies**.
3. Dans l'onglet **Stratégies**, choisissez la stratégie de l'Agent d'administration.
4. Dans le menu contextuel de la stratégie, sélectionnez l'option **Propriétés**.

   Ouvrez la fenêtre des propriétés de la stratégie de l'Agent d'administration.
5. Sélectionnez la section **Administration des correctifs et des mises à jour** dans la fenêtre des propriétés de la stratégie.
6. Cochez ou décochez la case **Installer automatiquement les mises à jour et les correctifs nécessaires pour les modules dont l'état est Non défini** pour activer ou désactiver, respectivement, la mise à jour automatique et l'application de correctifs.
7. Fermez le cadenas de ce paramètre.

La stratégie est appliquée aux appareils sélectionnés et l'installation automatique des mises à jour et des correctifs pour les modules de Kaspersky Security Center est activée (désactivée) sur ces appareils.

Déploiement de mises à jour automatique

Kaspersky Security Center permet de diffuser et d'installer automatiquement les mises à jour sur les appareils clients et sur les Serveurs d'administration secondaires.

Déploiement automatique des mises à jour sur les appareils clients

Pour que les mises à jour de l'application sélectionnée se diffusent automatiquement sur les appareils clients tout de suite après le téléchargement des mises à jour dans le stockage du Serveur d'administration, procédez comme suit :

1. Connectez-vous au Serveur d'administration qui administre les appareils clients.
2. Créez une tâche de déploiement des mises à jour pour les appareils clients sélectionnés par un des moyens suivants :

   - S'il faut diffuser les mises à jour sur les appareils clients qui font partie du groupe d'administration sélectionné, créer une tâche pour le groupe sélectionné.
   - S'il faut diffuser les mises à jour sur les appareils clients qui font partie ou non des différents groupes d'administration, créez une tâche pour un ensemble d'appareils.

   Ceci permet de lancer l'Assistant de création d'une tâche. Suivez ses instructions, exécutant les conditions suivantes :

   a. Dans la fenêtre de l'Assistant **Type de tâche** dans l'entrée de l'application nécessaire, sélectionnez la tâche de déploiement des mises à jour.

      Le nom de la tâche de déploiement des mises à jour, qui s'affiche dans la fenêtre **Type de tâche**, dépende de l'application pour lequel la tâche a été créée. Pour plus d'informations sur les noms des tâches de mise à jour pour les applications sélectionnées de Kaspersky, cf. Manuels pour ces applications.

   b. Dans la fenêtre de l'Assistant **Programmation** dans le champ **Programmation**, sélectionnez l'option de lancement **Lors du téléchargement des mises à jour dans le stockage**.

   Ainsi, la tâche de diffusion des mises à jour créée sera lancée pour les appareils sélectionnés chaque fois lors du téléchargement des mises à jour dans le stockage du Serveur d'administration.

Si la tâche de diffusion des mises à jour de l'application nécessaire a déjà été créée pour les appareils sélectionnés et que vous souhaitez une diffusion automatique des mises à jour sur les appareils clients, ouvrez la fenêtre des propriétés de la tâche et, dans la section **Programmation**, sélectionnez l'option de lancement **Lors du téléchargement des mises à jour dans le stockage** dans le champ **Programmation**.

Redistribution automatique des mises à jour sur les Serveurs d'administration secondaires

Pour que les mises à jour de l'application sélectionnée se diffusent automatiquement sur les Serveurs d'administration secondaires tout de suite après le téléchargement des mises à jour dans le stockage du Serveur d'administration principal, procédez comme suit :

1. Dans l'arborescence de la console dans l'entrée du Serveur d'administration principal, sélectionnez le dossier **Tâches**.
2. Dans la liste des tâches de l'espace de travail, sélectionnez la tâche Télécharger les mises à jour dans le stockage du Serveur d'administration du Serveur d'administration.
3. Ouvrez la section **Paramètres** de la fenêtre des propriétés de la tâche sélectionnée via l'un des moyens suivants :
   - Dans le menu contextuel de la tâche, sélectionnez l'option **Propriétés**.
   - A l'aide du lien **Modifier les paramètres** dans la zone d'informations de la tâche sélectionnée.
4. Dans la section **Paramètres** de la fenêtre de la tâche, ouvrez la fenêtre **Autres paramètres** à l'aide du lien **Personnaliser** dans la sous-section Autres paramètres.
5. Dans la fenêtre **Autres paramètres** qui s'ouvre, cochez la case **Forcer la mise à jour des Serveurs d'administration secondaires**.
6. Dans les paramètres de la tâche de mise à jour du Serveur d'administration, sous l'onglet **Paramètres** de la fenêtre des propriétés de la tâche, cochez la case **Forcer la mise à jour des Serveurs d'administration secondaires**.

Immédiatement après la réception des mises à jour par le Serveur d'administration principal, des tâches de téléchargement des mises à jour par les Serveurs d'administration secondaires seront automatiquement lancées, indépendamment de la programmation prévue dans la configuration de ces tâches.

Le Serveur d'administration principal effectue la mise à jour des bases de données antivirus, en fonction des applications installées sur les Serveurs d'administration secondaires. L'installation de plug-ins supplémentaires et la création de paquets d'installation sur le Serveur d'administration principal ne sont pas nécessaires.

Assignation automatique des points de distribution

Nous vous recommandons d'assigner les points de distribution automatiquement. Kaspersky Security Center choisira ainsi par lui-même les appareils à désigner comme points de distribution.

Pour assigner automatiquement des points de distribution :

1. Ouvrez la fenêtre principale de l'application.
2. Dans l'arborescence de la console, choisissez le nœud reprenant le nom du Serveur d'administration auquel vous souhaitez assigner automatiquement des points de distribution.
3. Dans le menu contextuel Serveur d'administration, cliquez sur **Propriétés**.

4. Dans la fenêtre des propriétés du Serveur d'administration, dans le volet **Sections**, sélectionnez **Points de distribution**.

5. Dans la partie droite de la fenêtre, sélectionnez l'option **Attribuer automatiquement les points de distribution**.

   Si l'assignation automatique d'appareils comme points de distribution est activée, vous ne pouvez pas configurer les points de distribution manuellement ni modifier la liste des points de distribution.

6. Cliquez sur le bouton **OK**.

Le Serveur d'administration assigne et configure automatiquement les points de distribution.

Assignation manuelle d'un point de distribution à un appareil

Kaspersky Security Center permet de désigner des appareils comme points de distribution.

Nous vous recommandons d'assigner les points de distribution automatiquement. Dans ce cas, Kaspersky Security Center choisira lui-même les appareils à désigner comme points de distribution. Cependant, si vous souhaitez, pour quelque raison que ce soit, refuser la désignation automatique des points de distribution (si vous souhaitez, par exemple, utiliser des serveurs prévus à cet effet), vous pouvez désigner les points de distribution manuellement, après avoir évalué leur quantité et leur configuration.

Les appareils fonctionnant comme points de distribution doivent être protégés, y compris physiquement contre tout accès non autorisé.

Pour désigner manuellement un appareil comme point de distribution :

1. Dans l'arborescence de la console, sélectionnez l'entrée **Serveur d'administration**.

2. Dans le menu contextuel Serveur d'administration, sélectionnez l'option **Propriétés**.

3. Dans la fenêtre des propriétés du Serveur d'administration, sélectionnez la section **Points de distribution** et cliquez sur le bouton **Ajouter**. Ce bouton est disponible si l'option **Attribuer manuellement les points de distribution** a été sélectionnée.

   La fenêtre **Ajouter un point de distribution** s'ouvre.

4. Dans la fenêtre **Ajouter un point de distribution**, exécutez les opérations suivantes :

   a. Sélectionnez l'appareil qui jouera le rôle de point de distribution (sélectionnez-le dans le groupe d'administration ou indiquez l'adresse IP de l'appareil). Lors de la sélection de l'appareil, prenez en compte les particularités de fonctionnement des points de distribution et les exigences pour l'appareil qui joue le rôle de point de distribution.

   b. Indiquez un ensemble d'appareils sur lesquels le point de distribution diffusera les mises à jour. Vous pouvez indiquer le groupe d'administration ou la description de l'emplacement réseau.

5. Cliquez sur le bouton **OK**.

   Le point de distribution que vous avez ajouté sera affiché dans la liste des points de distribution, dans la section **Points de distribution**.

6. Sélectionnez le point de distribution dans la liste et, via le bouton **Propriétés**, ouvrez la fenêtre de ses propriétés.

7. Configurez le point de distribution dans la fenêtre des propriétés :

   - La section **Général** contient les paramètres d'interaction entre le point de distribution et les appareils clients.

     - **Port SSL**

       Le numéro du port SSL utilisé pour la connexion sécurisée des appareils clients au point de distribution via le protocole SSL.

       Le numéro de port est de 13000 par défaut.

     - **Utiliser la multidiffusion**

       Si cette option est activée, la multidiffusion pour la diffusion automatique des paquets d'installation sur les appareils clients du groupe sera utilisée.

       La diffusion IP multidiffusion réduit le temps nécessaire à l'installation d'une application à partir d'un paquet d'installation sur un groupe d'appareils clients, mais prolonge le temps d'installation lorsque vous installez une application sur un seul appareil client.

     - **IP de multidiffusion**

       Adresse IP sur laquelle est exécuté l'envoi diffusion multiadresse. L'adresse IP peut être indiquée dans l'intervalle 224.0.0.0 – 239.255.255.255

       Par défaut, Kaspersky Security Center attribue automatiquement une adresse IP de multidiffusion unique dans la plage donnée.

     - **Numéro du port IP de multidiffusion**

       Numéro du port de diffusion multiadresse.

       Le numéro de port est de 15001 par défaut. Dans le cas où le point de distribution tourne sur un appareil sur lequel est également installé un Serveur d'administration, le numéro de port par défaut pour la connexion SSL est 13001.

     - **Déployer les mises à jour**

Les mises à jour sont distribuées aux appareils administrés à partir des sources suivantes :

- Ce point de distribution si cette option est activée.
- Autres points de distribution, Serveur d'administration ou serveurs de mise à jour Kaspersky si cette option est désactivée.

Si vous utilisez des points de distribution pour déployer des mises à jour, vous pouvez économiser du trafic parce que vous réduisez le nombre de téléchargements. Vous pouvez aussi alléger la charge sur le Serveur d'administration et répartir la charge entre les points de distribution. Vous pouvez calculer le nombre de points de distribution de votre réseau pour optimiser le trafic et la charge.

Si vous désactivez cette option, le nombre de téléchargements de mises à jour et de charges sur le Serveur d'administration peut augmenter. Cette option est activée par défaut.

- **Déployer les p&aquets d'installation**

Les paquets d'installation sont distribuées aux appareils administrés à partir des sources suivantes :

- Ce point de distribution si cette option est activée.
- Autres points de distribution, Serveur d'administration ou serveurs de mise à jour Kaspersky si cette option est désactivée.

Si vous utilisez des points de distribution pour déployer des paquets d'installation, vous pouvez économiser du trafic parce que vous réduisez le nombre de téléchargements. Vous pouvez aussi alléger la charge sur le Serveur d'administration et répartir la charge entre les points de distribution. Vous pouvez calculer le nombre de points de distribution de votre réseau pour optimiser le trafic et la charge.

Si vous désactivez cette option, le nombre de téléchargements de paquets d'installation et de charges sur le Serveur d'administration peut augmenter. Cette option est activée par défaut.

- **Utilisez ce point de distribution comme serveur push**

Dans Kaspersky Security Center, un point de distribution peut servir de serveur push pour les appareils administrés via le protocole mobile. Par exemple, un serveur push doit être activé si vous souhaitez pouvoir forcer la synchronisation des appareils KasperskyOS avec le Serveur d'administration. Un serveur push a la même portée d'appareils administrés que le point de distribution sur lequel le serveur push est activé. Si plusieurs points de distribution sont affectés au même groupe d'administration, vous pouvez activer le serveur push sur chacun des points de distribution. Dans ce cas, le Serveur d'administration équilibre la charge entre les points de distribution.

Si vous administrez des appareils avec un KasperskyOS installé, ou si vous prévoyez de le faire, vous devez utiliser un point de distribution comme serveur push. Vous pouvez également utiliser un point de distribution en tant que serveur push si vous souhaitez envoyer des notifications push aux appareils clients.

- **Port du serveur push**

Le port sur le point de distribution que les appareils clients utiliseront pour la connexion. Le numéro du port est de 13295 par défaut.

- Dans la section **Zone d'action**, indiquez la zone dans laquelle le point de distribution va distribuer des mises à jour (groupes d'administration et/ou emplacement réseau).

- Dans la section **Proxy KSN**, vous pouvez configurer l'application afin qu'elle utilise le point de distribution pour transmettre les requêtes KSN depuis les appareils administrés.

  - **Activer le proxy KSN du côté du point de distribution**

    Le service KSN proxy est exécuté sur l'appareil qui est utilisé en tant que points de distribution. Utilisez cette fonction pour rediffuser et optimiser le trafic sur le réseau.

    Le point de distribution envoie les statistiques KSN, lesquelles sont répertoriées dans la Déclaration de Kaspersky Security Network, à Kaspersky. Par défaut, la Déclaration KSN se trouve dans %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\ksneula.

    Cette option est Inactif par défaut. L'activation de cette option prend effet uniquement si les options **Utiliser le Serveur d'administration comme serveur proxy** et **J'accepte les termes du Kaspersky Security Network** sont activées dans la fenêtre Propriétés du Serveur d'administration.

    Vous pouvez affecter un nœud d'un cluster actif-passif à un point de distribution et activer le serveur proxy KSN sur ce nœud.

  - **Transférer les demandes KSN au Serveur d'administration**

    Le point de distribution transfère les requêtes KSN depuis les appareils administrés vers le Serveur d'administration.

    Cette option est activée par défaut.

  - **Accéder à KSN Cloud/KPSN directement via Internet**

    Le point de distribution transfère les requêtes KSN depuis les appareils administrés vers le Cloud KSN ou KPSN. Les requêtes KSN générées sur le point de distribution lui-même sont également envoyées directement à KSN Cloud ou à KPSN.

    Les points de distribution sur lesquels l'Agent d'administration version 11 (ou antérieure) est installé ne peuvent pas accéder directement à KPSN. Si vous souhaitez reconfigurer les points de distribution pour envoyer des demandes KSN à KPSN, activez l'option **&Transférer les demandes KSN au Serveur d'administration** pour chaque point de distribution.

    Les points de distribution sur lesquels l'Agent d'administration version 12 (ou version ultérieure) est installé peuvent accéder directement à KPSN.

  - **Ignorer les paramètres du serveur proxy lors de la connexion à KPSN**

    Activez cette option, si les paramètres du serveur proxy sont configurés dans les propriétés du point de distribution ou dans la stratégie de l'Agent d'administration, mais que votre architecture réseau exige que vous utilisiez directement un KPSN. Dans le cas contraire, les requêtes des applications administrées ne peuvent pas atteindre le KPSN.

    Cette option est disponible si vous sélectionnez l'option **Accéder à KSN Cloud/KPSN directement via Internet**.

  - **Port TCP**

    Le numéro du port TCP que les appareils administrés utilisent pour se connecter au serveur proxy KSN. Le numéro de port par défaut est 13111.

  - **Port UDP**

Si vous avez besoin que l'Agent d'administration se connecte au Serveur d'administration via un port UDP, activez l'option **Utiliser le port UDP** et indiquez le **Numéro de port UDP**. Cette option est activée par défaut. Par défaut, la connexion au Serveur d'administration est exécutée via le port UDP 15000.

- **Port HTTPS**

  Si vous souhaitez que les appareils administrés se connectent au serveur proxy KSN via un port HTTPS, activez l'option **Utiliser le protocole HTTPS** et spécifiez un numéro **HTTPS par port**. Par défaut, la connexion au serveur proxy KSN est exécutée via le port HTTPS 17111.

- Dans la section **Recherche d'appareils**, configurez les paramètres de sondage par le point de distribution des domaines Windows, Active Directory et des plages IP.

  - **Domaines Windows**

    Vous pouvez autoriser la recherche d'appareils pour les domaines Windows et programmer la recherche.

  - **Active Directory**

    Vous pouvez autoriser le sondage du réseau pour Active Directory et programmer le sondage.

    Si vous utilisez un point de distribution Windows, vous pouvez sélectionner une des options suivantes :

    - **Sonder le domaine actuel Active Directory**.
    - **Sonder la forêt de domaines Active Directory**.
    - **Sonder les domaines indiqués Active Directory**. Si vous choisissez cette option, ajoutez un ou plusieurs domaines Active Directory à la liste.

    Si vous utilisez un point de distribution Linux avec l'Agent d'administration version 15 installé, vous ne pouvez interroger que les domaines Active Directory dont vous spécifiez l'adresse et les informations d'identification de l'utilisateur. Les sondages du domaine Active Directory actuel et de la forêt de domaines Active Directory ne sont pas disponibles.

  - **Plages IP**

    Vous pouvez activer la recherche d'appareils pour les plages IPv4 et les réseaux IPv6.

    Si vous activez l'option **Autoriser le sondage de la plage**, vous pouvez ajouter des plages d'analyse et définir les programmations pour celles-ci. Vous pouvez ajouter des plages IP à la liste des plages analysées.

    Si vous activez l'option **Utiliser Zeroconf pour sonder les réseaux IPv6**, le point de distribution sonde automatiquement le réseau IPv6 en utilisant la mise en réseau sans configuration (également appelée *Zeroconf*). Dans ce cas, les plages IP spécifiées sont ignorées car le point de distribution sonde l'ensemble du réseau. L'option **Utiliser Zeroconf pour sonder les réseaux IPv6** est disponible si le point de distribution fonctionne sous Linux. Pour utiliser le sondage Zeroconf IPv6, vous devez installer l'utilitaire avahi-browse sur le point de distribution.

- Dans la section **Avancé**, indiquez le dossier que le point de distribution doit utiliser pour l'enregistrement des données distribuées.

  - **Utiliser le dossier par défaut**

    Lors du choix de cette option, le dossier avec l'Agent d'administration installé sur le point de distribution sera utilisé pour enregistrer les données.

  - **Utiliser le dossier indiqué**

    Lors du choix de cette option, il est possible d'indiquer dans le champ situé ci-dessous le chemin d'accès au dossier. Le dossier peut être local sur le point de distribution ou distant, sur n'importe lequel des appareils faisant partie du réseau de l'entreprise.

    Le compte utilisateur, sous lequel l'Agent d'administration est lancé sur le point de distribution, doit posséder l'accès au dossier indiqué pour lecture et écriture.

Les appareils sélectionnés sont comme des points de distribution.

Seuls les appareils administrés sous Windows peuvent définir l'emplacement réseau. La définition de l'emplacement réseau est inaccessible pour les appareils administrés sous d'autres systèmes d'exploitation.

Suppression d'un appareil de la liste des points de distribution

Pour supprimer un appareil des points de distribution :

1. Dans l'arborescence de la console, sélectionnez l'entrée **Serveur d'administration**.
2. Dans le menu contextuel Serveur d'administration, sélectionnez l'option **Propriétés**.
3. Dans la fenêtre des propriétés du Serveur d'administration, dans la section **Points de distribution**, sélectionnez l'appareil qui remplit les fonctions de point de distribution et cliquez sur le bouton **Supprimer**.

Suite à cette action, l'appareil est supprimé de la liste des points de distribution et arrête de remplir les fonctions de point de distribution.

Il est impossible de supprimer un appareil de la liste des points de distribution s'il a été assigné par le Serveur d'administration automatiquement.

Téléchargement des mises à jour par les points de distribution

Kaspersky Security Center permet aux points de distribution d'obtenir des mises à jour du Serveur d'administration, des serveurs Kaspersky, du dossier local ou réseau.

Si vous n'avez pas besoin de définir une source de mise à jour, nous vous recommandons d'utiliser la tâche *Télécharger les mises à jour dans les stockages des points de distribution* pour un groupe d'administration. Pour en savoir plus, reportez-vous à la section suivante : Création de la tâche de téléchargement des mises à jour sur les stockages des points de distribution.

Pour configurer le téléchargement des mises à jour pour un point de distribution :

1. Dans l'arborescence de la console, sélectionnez l'entrée **Serveur d'administration**.
2. Dans le menu contextuel Serveur d'administration, sélectionnez l'option **Propriétés**.
3. Dans la fenêtre des propriétés du Serveur d'administration, dans la section **Points de distribution**, sélectionnez le point de distribution par lequel les mises à jour seront livrées sur les appareils clients du groupe.
4. Cliquez sur le bouton **Propriétés** pour ouvrir la fenêtre de propriétés du point de distribution sélectionné.
5. Dans la fenêtre des propriétés du point de distribution, sélectionnez la section **Sources des mises à jour**.
6. Sélectionnez la source des mises à jour pour le point de distribution :

   - Pour que le point de distribution récupère les mises à jour du Serveur d'administration, sélectionnez l'option **Récupérer depuis le Serveur d'administration** :

     - **Télécharger des fichiers diff**

       Cette option active la fonction de téléchargement des fichiers diff.

       Cette option est activée par défaut.

   - Pour permettre au point de distribution de recevoir des mises à jour à l'aide d'une tâche, sélectionnez **Utiliser la tâche de téléchargement forcé des mises à jour** :

     - Appuyez sur le bouton **Parcourir** si une telle tâche existe déjà sur l'appareil, puis sélectionnez la tâche dans la liste qui s'affiche.
     - Appuyez sur le bouton **Nouvelle tâche** pour créer la tâche si une telle tâche n'existe pas encore sur l'appareil. Ceci permet de lancer l'Assistant de création d'une tâche. Suivez les instructions de l'assistant.

   Le téléchargement des mises à jour dans les stockages des points de distribution est une tâche locale. Vous devez créer une nouvelle tâche pour chaque appareil qui agit comme point de distribution.

Le point de distribution obtient les mises à jour depuis la source indiquée.

Suppression des mises à jour logicielles dans le stockage

Pour supprimer les mises à jour logicielles dans le stockage du Serveur d'administration, procédez comme suit :

1. Dans l'arborescence de la console, accédez au dossier **Avancé** → **Gestion des applications**, puis le sous-dossier **Mises à jour du logiciel**.
2. Dans l'espace de travail du dossier **Mises à jour du logiciel**, sélectionnez la mise à jour à supprimer.
3. Dans le menu contextuel de la mise à jour, sélectionnez **Supprimer les fichiers des mises à jour**.

Les mises à jour logicielles sont supprimées du stockage du Serveur d'administration.

Installation du correctif pour l'application Kaspersky dans le modèle de cluster

Kaspersky Security Center prend uniquement en charge l'installation manuelle des correctifs pour les applications Kaspersky dans le modèle de cluster.

Pour installer le correctif pour l'application Kaspersky, procédez comme suit :

1. Téléchargez le correctif sur chaque nœud du cluster.
2. Lancez l'installation du correctif sur le nœud actif.
3. Attendez que le correctif soit bien installé.
4. Lancez successivement le correctif sur tous les nœuds secondaires du cluster.

   Au moment du lancement du correctif depuis la ligne de commande, utilisez la clé " `-CLUSTER_SECONDARY_NODE` ".

   Suite à ces actions, le correctif sera installé sur chaque nœud du cluster.
5. Lancez manuellement les services de cluster de Kaspersky.

Chaque nœud du cluster s'affichera dans la Console d'administration en tant qu'appareil sur lequel l'Agent d'administration est installé.

Les informations sur les correctifs installés peuvent être consultées dans le dossier **Mises à jour du logiciel** ou dans le rapport sur les versions de mises à jour des modules logiciels des applications Kaspersky.

Gestion des applications tierces sur les appareils client

Kaspersky Security Center permet d'administrer les applications de Kaspersky et d'autres éditeurs installées sur les appareils clients.

L'administrateur peut exécuter les actions suivantes :

- Créer les catégories d'applications sur la base des critères définis.
- Administrer les catégories d'applications à l'aide des règles spécialement créées.
- Administrer le lancement des applications sur les appareils.
- Exécuter l'inventaire et suivre le registre du logiciel installé sur les appareils.
- Fermer les vulnérabilités du logiciel installé sur les appareils.
- Installer les mises à jour Windows Update et d'autres éditeurs du logiciel sur les appareils.
- Surveiller l'utilisation des clés de licence pour les groupes des applications sous licence.

À propos des applications tierces

Kaspersky Security Center peut vous aider à mettre à jour les logiciels tiers installés sur les appareils clients et à corriger les vulnérabilités du logiciel tiers. Kaspersky Security Center peut mettre à jour les logiciels tiers de la version actuelle à la dernière version uniquement.

La liste des logiciels tiers peut être modifiée et est mise à jour dynamiquement. Vous pouvez vérifier si vous pouvez mettre à jour le logiciel tiers (installé sur les appareils des utilisateurs) avec Kaspersky Security Center en consultant la liste des mises à jour disponibles dans la Console d'administration basée sur MMC et dans Kaspersky Security Center Web Console.

La procédure décrite ci-dessous permet uniquement de consulter la liste des logiciels tiers qui peuvent être mis à jour à l'aide de Kaspersky Security Center. Les étapes sont suivies pour accéder aux informations pertinentes sans lancer de tâches.

Pour afficher la liste des logiciels tiers que vous pouvez mettre à jour avec Kaspersky Security Center dans Kaspersky Security Center Web Console, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Tâches**.
2. Cliquez sur **Ajouter**.

   Ceci permet de lancer l'assistant de création d'une tâche. Parcourez les étapes de l'assistant à l'aide du bouton **Suivant**.
3. À l'étape **Paramètres de nouvelle tâche** de l'assistant, spécifiez les paramètres suivants :

   a. Dans la liste déroulante **Application**, sélectionnez **Kaspersky Security Center**.

   b. Dans le champ **Type de tâche**, sélectionnez **Installation des mises à jour requises et correction des vulnérabilités**.
4. A l'étape **Zone de la tâche** de l'Assistant, sélectionnez l'option **Appareils administrés**.
5. À l'étape **Définissez les règles d'installation des mises à jour** du programme d'installation, cliquez sur le bouton **Ajouter**.

   L'Assistant de création de règles se lance. Parcourez les étapes de l'assistant à l'aide du bouton **Suivant**.

6. À l'étape **Sélectionnez le type de règle** de l'assistant, sélectionnez l'option **Règles pour les mises à jour tierces**.

7. À l'étape **Critères généraux** de l'assistant, sélectionnez l'option **Installer toutes les mises à jour (sauf les mises à jour rejetées)**, puis cliquez sur **Suivant**.

La liste des logiciels tiers s'affiche.

Pour afficher la liste des logiciels tiers que vous pouvez mettre à jour avec Kaspersky Security Center dans la console basée sur MMC, vous devez disposer de la licence Gestion des vulnérabilités et des correctifs. Dans le cas contraire, la tâche **Installation des mises à jour requises et correction des vulnérabilités** n'est pas disponible.

1. Dans l'arborescence de la console sélectionnez le dossier **Appareils administrés**.

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

3. Cliquez sur le bouton **Créer une tâche** pour lancer l'Assistant de création d'une tâche. Suivez les étapes de l'assistant.

4. Sur la page **Sélection du type de tâche** de l'Assistant, sélectionnez **Installation des mises à jour requises et correction des vulnérabilités**.

5. À l'étape **Définissez les règles d'installation des mises à jour** du programme d'installation, cliquez sur le bouton **Ajouter**.

   L'Assistant de création de règles se lance. Parcourez les étapes de l'assistant à l'aide du bouton **Suivant**.

6. À l'étape **Sélectionnez le type de règle** de l'assistant, sélectionnez l'option **Règles pour les mises à jour tierces**.

7. À l'étape **Critères généraux** de l'assistant, sélectionnez l'option **Installer toutes les mises à jour (sauf les mises à jour rejetées)**, puis cliquez sur **Suivant**.

   La liste des logiciels tiers s'affiche.

Installation des mises à jour logicielles tierces

Kaspersky Security Center permet d'administrer les mises à jour du logiciel installé sur les appareils clients et de fermer les vulnérabilités dans les applications de Microsoft et d'autres éditeurs du logiciel à l'aide de l'installation des mises à jour nécessaires.

Kaspersky Security Center permet d'exécuter la recherche de mises à jour à l'aide de la tâche de recherche de mises à jour et télécharge les mises à jour dans le stockage des mises à jour. Après la fin de la recherche de mises à jour, l'application offre à l'administrateur les informations sur les mises à jour disponibles et sur les vulnérabilités dans les applications qui peuvent être fermées à l'aide de ces mises à jour.

Les informations sur les mises à jour Microsoft Windows disponibles proviennent du service Windows Update. Le Serveur d'administration peut être utilisé comme serveur de mises à jour du serveur Windows (WSUS). Pour utiliser le Serveur d'administration comme serveur WSUS, il faut configurer la synchronisation des mises à jour avec Windows Update. Après la configuration de la synchronisation des données avec Windows Update, le Serveur d'administration, avec une fréquence définie, fournit les mises à jour aux services Windows Update sur les appareils en mode centralisé.

Il est aussi possible d'administrer les mises à jour logicielles à l'aide de la stratégie de l'Agent d'administration. Pour cela, il faut créer la stratégie de l'Agent d'administration et de configurer les paramètres des mises à jour du logiciel dans les fenêtres correspondantes de l'Assistant de création de la stratégie.

L'administrateur peut consulter la liste des mises à jour disponibles dans le sous-dossier **Mises à jour du logiciel** inclus dans le dossier **Gestion des applications**. Ce dossier contient la liste des mises à jour obtenues par le Serveur d'administration des applications de Microsoft et d'autres éditeurs du logiciel qui peuvent être diffusées sur les appareils. Après la consultation des informations sur les mises à jour disponibles, l'administrateur peut exécuter l'installation des mises à jour sur les appareils.

La mise à jour de certaines applications Kaspersky Security Center s'effectue par la suppression de la version précédente de l'application et par l'installation d'une nouvelle version.

Une interaction utilisateur peut être requise lorsque vous mettez à jour une application tierce ou corrigez une vulnérabilité dans une application tierce sur un appareil administré. Par exemple, l'utilisateur peut être invité à fermer l'application tierce si elle est actuellement ouverte.

Dans la fenêtre **&Configuration de l'interface** pour les Serveurs d'administration primaire et secondaire, assurez-vous que l'option **Afficher Gestion des vulnérabilités et des correctifs** est activée. Dans le cas contraire, la tâche de recherche de mises à jour ne gère que les mises à jour WSUS.

Pour des raisons de sécurité, toutes les mises à jour logicielles tierces que vous installez à l'aide de la fonction de la gestion des vulnérabilités et des correctifs sont automatiquement analysées à la recherche de logiciels malveillants par les technologies de Kaspersky. Ces technologies sont utilisées pour la vérification automatique des fichiers et incluent la recherche de virus, l'analyse statique, l'analyse dynamique, l'analyse comportementale dans l'environnement sandbox et machine learning.

Les experts de Kaspersky n'effectuent pas d'analyse manuelle des mises à jour du logiciel tiers pouvant être installées par la fonction de la gestion des vulnérabilités et des correctifs. De plus, les experts de Kaspersky ne recherchent pas de vulnérabilités (connues ou inconnues) ou de fonctionnalités non documentées dans ces mises à jour, et n'effectuent pas d'autres types d'analyse des mises à jour que ceux indiqués dans le paragraphe ci-dessus.

Avant l'installation des mises à jour sur tous les appareils, il est possible d'exécuter l'installation de contrôle pour s'assurer que les mises à jour installées ne provoquent pas d'échecs dans le fonctionnement des applications sur les appareils.

Scénario : mise à jour des logiciels tiers

Cette section fournit un scénario pour la mise à jour des logiciels tiers installés sur les appareils client. Les logiciels tiers comprennent des applications de Microsoft et d'autres fournisseurs de logiciels. Les mises à jour des applications de Microsoft sont fournies par le service Windows Update.

Prérequis

Le Serveur d'administration doit être connecté à Internet pour installer les mises à jour de logiciels tiers autres que les logiciels Microsoft.

Par défaut, une connexion Internet n'est pas requise pour que le Serveur d'administration installe les mises à jour logicielles Microsoft sur les appareils administrés. Les appareils administrés peuvent ainsi télécharger les mises à jour logicielles Microsoft directement à partir des serveurs Microsoft Update ou à partir de Windows Server lorsque Microsoft Windows Server Update Services (WSUS) est déployé sur le réseau de votre organisation. Le Serveur d'administration doit être connecté à Internet lorsque vous utilisez le Serveur d'administration comme serveur WSUS.

Étapes

La mise à jour du logiciel tiers s'effectue fait par étapes :

1. **Recherche des mises à jour requises**

   Pour rechercher les mises à jour logicielles tierces requises pour les appareils administrés, exécutez la tâche *Recherche de vulnérabilités et de mises à jour requises*. Une fois cette tâche terminée, Kaspersky Security Center reçoit la liste des vulnérabilités détectées et des mises à jour requises pour les logiciels tiers installés sur les appareils que vous avez spécifiés dans les propriétés de la tâche.

   La tâche *Recherche de vulnérabilités et de mises à jour requises* est créée automatiquement par l'Assistant de configuration initiale du Serveur d'administration. Si vous n'avez pas exécuté l'assistant, créez la tâche ou exécutez l'assistant de démarrage rapide de l'application maintenant.

   Instructions pour :

   - Console d'administration : Recherche de vulnérabilités dans les applications, Planification de la tâche Recherche de vulnérabilités et des mises à jour requises
   - Kaspersky Security Center Web Console : création d'une tâche Recherche de vulnérabilités et de mises à jour requises, paramètres de Recherche de vulnérabilités et de mises à jour requises

2. **Analyser la liste des mises à jour trouvées**

   Consultez la liste des **Mises à jour du logiciel** et décidez des mises à jour que vous souhaitez installer. Pour consulter les informations détaillées de chaque mise à jour, cliquez sur le nom de la mise à jour dans la liste. Pour chaque mise à jour de la liste, vous pouvez également consulter les statistiques de l'installation de la mise à jour sur les appareils client.

   Instructions pour :

   - Console d'administration : Affichage des informations sur les mises à jour disponibles
   - Kaspersky Security Center Web Console : Affichage des informations sur les mises à jour logicielles tierces disponibles

3. **Configuration de l'installation des mises à jour**

   Une fois que Kaspersky Security Center a reçu la liste des mises à jour logicielles tierces, vous pouvez les installer sur les appareils client à l'aide de la tâche *Installation des mises à jour requises et correction des vulnérabilités* ou de la tâche *Installation des mises à jour Windows Update*. Créez une de ces tâches. Vous pouvez créer ces tâches sous l'onglet **Tâches** ou à l'aide de la liste **Mises à jour du logiciel**.

   La tâche *Installation des mises à jour requises et correction des vulnérabilités* est utilisée pour installer les mises à jour des applications de Microsoft, y compris les mises à jour fournies par le service Windows Update et les mises à jour des logiciels d'autres fournisseurs. Notez que cette tâche ne peut être créée que si vous disposez de la licence pour la fonctionnalité Gestion des vulnérabilités et des correctifs.

   La tâche *Installation des mises à jour Windows Update* ne nécessite pas de licence, mais elle peut être utilisée pour installer uniquement les mises à jour de Windows Update.

   Pour installer certaines mises à jour logicielles, vous devez accepter le Contrat de licence utilisateur final (CLUF) du logiciel en cours d'installation. Si vous refusez le CLUF, la mise à jour logicielle ne sera pas installée.

Vous pouvez lancer une tâche d'installation de mise à jour selon la planification. Lorsque vous définissez la planification de la tâche, assurez-vous que la tâche d'installation de la mise à jour est lancée une fois que la tâche *Recherche de vulnérabilités et de mises à jour requises* est terminée.

Instructions pour :

- Console d'administration : Correction des vulnérabilités dans les applications, Affichage des informations sur les mises à jour disponibles
- Kaspersky Security Center Web Console : Création de la tâche Installation des mises à jour requises et correction des vulnérabilités, Création de la tâche Installation des mises à jour Windows Update, Affichage des informations sur les mises à jour logicielles tierces disponibles

4. **Planification des tâches**

   Pour vous assurer que la liste des mises à jour est toujours d'actualité, planifiez la tâche *Recherche de vulnérabilités et de mises à jour requises* pour exécuter automatiquement la tâche de temps à autre. Par défaut, la tâche *Recherche de vulnérabilités et de mises à jour requises* est configurée pour démarrer manuellement.

   Si vous avez créé la tâche *Installation des mises à jour requises et correction des vulnérabilités*, vous pouvez la planifier pour qu'elle soit exécutée à la même fréquence que la tâche *Recherche de vulnérabilités et de mises à jour requises* ou à une fréquence moindre. Lors de la planification de la tâche *Installation des mises à jour Windows Update*, notez qu'avant de démarrer cette tâche, vous devez définir la liste des mises à jour à chaque fois.

   Lors de la planification des tâches, assurez-vous qu'une tâche d'installation de la mise à jour est lancée une fois que la tâche *Recherche de vulnérabilités et de mises à jour requises* est terminée.

5. **Approbation et refus des mises à jour logicielles (facultatif)**

   Si vous avez créé la tâche Installation des mises à jour requises et correction des vulnérabilités, vous pouvez spécifier des règles pour l'installation des mises à jour dans les propriétés de la tâche. Si vous avez créé la tâche Installation des mises à jour Windows Update, ignorez cette étape.

   Pour chaque règle, vous pouvez définir les mises à jour à installer en fonction de l'état de la mise à jour : *Non défini*, *Approuvé* ou *Rejeté*. Par exemple, vous pouvez créer une tâche spécifique pour les serveurs et définir une règle pour cette tâche afin de n'autoriser l'installation que des mises à jour de Windows Update et uniquement celles qui disposent de l'état *Approuvé*. Ensuite, vous définissez manuellement l'état *Approuvé* pour les mises à jour que vous souhaitez installer. Dans ce cas, les mises à jour Windows Update qui disposent de l'état *Non défini* ou *Rejeté* ne seront pas installées sur les serveurs que vous avez spécifiés dans la tâche.

   L'utilisation de l'état *Approuvé* pour gérer l'installation des mises à jour est efficace pour un petit nombre de mises à jour. Pour installer plusieurs mises à jour, utilisez les règles que vous pouvez configurer dans la tâche *Installation des mises à jour requises et correction des vulnérabilités*. Nous vous recommandons de définir l'état *Approuvé* uniquement pour les mises à jour particulières qui ne répondent pas aux critères spécifiés dans les règles. Lorsque vous approuvez manuellement une grande quantité de mises à jour, les performances du Serveur d'administration diminuent, ce qui peut entraîner une surcharge du Serveur d'administration.

   Par défaut, les mises à jour logicielles téléchargées sont à l'état *Non défini*. Vous pouvez modifier l'état en *Approuvé* ou *Rejeté* dans la liste **Mises à jour du logiciel** (**Opérations** → **Gestion des correctifs** → **Mises à jour du logiciel**).

   Instructions pour :

   - Console d'administration : Approbation et refus des mises à jour logicielles
   - Kaspersky Security Center Web Console : Approbation et refus des mises à jour logicielles tierces

6. **Configuration du Serveur d'administration pour qu'il fonctionne comme serveur Windows Server Update Services (WSUS) (facultatif)**

Par défaut, les mises à jour Windows Update sont téléchargées sur les appareils administrés à partir des serveurs Microsoft. Vous pouvez modifier ce paramètre pour utiliser le Serveur d'administration comme serveur WSUS. Dans ce cas, le Serveur d'administration synchronise les données de mise à jour avec Windows Update à la fréquence indiquée et fournit des mises à jour en mode centralisé à Windows Update sur les appareils en réseau.

Pour utiliser le Serveur d'administration comme serveur WSUS, créez la tâche Synchronisation des mises à jour Windows Update et cochez la case **Utiliser le Serveur d'administration comme serveur WSUS** dans la stratégie de l'Agent d'administration.

Instructions pour :

- Console d'administration : Synchronisation des mises à jour Windows Update avec le Serveur d'administration, Configuration des mises à jour Windows dans une stratégie de l'Agent d'administration
- Kaspersky Security Center Web Console : Création de la tâche Synchronisation des mises à jour Windows Update

7. **Exécution d'une tâche d'installation des mises à jour**

   Démarrez la tâche *Installation des mises à jour requises et correction des vulnérabilités* ou la tâche *Installation des mises à jour Windows Update*. Lorsque vous démarrez ces tâches, les mises à jour sont téléchargées et installées sur les appareils administrés. Une fois la tâche terminée, assurez-vous qu'elle possède le statut *Terminée* dans la liste des tâches.

8. **Création du rapport des résultats de l'installation des mises à jour de logiciels tiers (facultatif)**

   Pour consulter les statistiques détaillées concernant l'installation des mises à jour, créez le **Rapport sur les résultats de l'installation des mises à jour du logiciel tiers**.

   Instructions pour :

   - Console d'administration : création et affichage d'un rapport
   - Kaspersky Security Center Web Console : génération et affichage d'un rapport

Résultats

Si vous avez créé et configuré la tâche *Installation des mises à jour requises et correction des vulnérabilités*, les mises à jour sont installées automatiquement sur les appareils administrés. Lorsque de nouvelles mises à jour sont téléchargées dans le stockage du Serveur d'administration, Kaspersky Security Center vérifie si elles répondent aux critères spécifiés dans les règles de mise à jour. Toutes les nouvelles mises à jour qui répondent aux critères seront installées automatiquement lors de la prochaine exécution de la tâche.

Si vous avez créé la tâche *Installation des mises à jour Windows Update*, seules les mises à jour spécifiées dans les propriétés de la tâche *Installation des mises à jour Windows Update* sont installées. À l'avenir, si vous souhaitez installer les nouvelles mises à jour téléchargées dans le stockage du Serveur d'administration, vous devez ajouter les mises à jour requises à la liste des mises à jour dans la tâche existante ou créer une nouvelle tâche *Installation des mises à jour Windows Update*.

Affichage des informations sur les mises à jour disponibles pour les applications tierces

Pour consulter la liste des mises à jour disponibles pour les applications tierces installées sur les appareils client,

Dans l'arborescence de la console, accédez au dossier **Avancé** → **Gestion des applications**, puis le sous-dossier **Mises à jour du logiciel**.

Dans l'espace de travail du dossier, vous pouvez consulter la liste des mises à jour existantes pour les applications installées sur les appareils.

Pour consulter les propriétés de la mise à jour,

Dans l'espace de travail du dossier **Mises à jour du logiciel**, dans le menu contextuel de la mise à jour, sélectionnez l'option **Propriétés**.

Les informations suivantes sont accessibles à la consultation dans la fenêtre des propriétés de la mise à jour :

- Dans la section **Général**, vous pouvez voir l'**État d'approbation de la mise à jour**:
  - **Non défini** - la mise à jour est disponible dans la liste des mises à jour, mais n'est pas approuvée pour l'installation.
  - **Approuvée** - la mise à jour est disponible dans la liste des mises à jour et approuvée pour l'installation.
  - **Rejetée** - la mise à jour est refusée pour l'installation.
- Dans la section **Attributs**, vous pouvez afficher les valeurs du champ **Installé automatiquement** :
  - La valeur **Automatique** est affichée si la tâche *Installation des mises à jour requises et correction des vulnérabilités* peut installer des mises à jour pour l'application. La tâche installe automatiquement les nouvelles mises à jour à partir de l'adresse Web fournie par le fournisseur du logiciel tiers.
  - La valeur **Manuel** s'affiche si Kaspersky Security Center ne peut pas installer automatiquement les mises à jour de l'application. Vous pouvez installer les mises à jour manuellement.

  Le champ **Installé automatiquement** n'est pas affiché pour les mises à jour d'applications Windows.
- La liste des appareils clients pour lesquels la mise à jour est applicable.
- La liste des modules système (prérequis) qui doivent être installés avant la mise à jour (si de tels modules existent).
- Les vulnérabilités logicielles que cette mise à jour ferme.

Approbation et refus des mises à jour du logiciel

Les paramètres d'une tâche d'installation de mise à jour peuvent nécessiter l'approbation des mises à jour à installer. Vous pouvez approuver les mises à jour à installer et refuser les mises à jour qui ne doivent pas installer.

Par exemple, vous souhaitez d'abord vérifier l'installation des mises à jour dans un environnement d'essai et vous assurer qu'elles ne perturbent pas le fonctionnement des appareils avant d'autoriser l'installation de ces mises à jour sur les appareils clients.

L'utilisation de l'état *Approuvé* pour gérer l'installation des mises à jour tierces est efficace pour un petit nombre de mises à jour. Pour installer plusieurs mises à jour tierces, utilisez les règles que vous pouvez configurer dans la tâche *Installation des mises à jour requises et correction des vulnérabilités*. Nous vous recommandons de définir l'état *Approuvé* uniquement pour les mises à jour particulières qui ne répondent pas aux critères spécifiés dans les règles. Lorsque vous approuvez manuellement une grande quantité de mises à jour, les performances du Serveur d'administration diminuent, ce qui peut entraîner une surcharge du Serveur d'administration.

Pour approuver ou refuser une ou plusieurs mises à jour :

1. Dans l'arborescence de la console, sélectionnez le dossier **Avancé → Gestion des applications → Mises à jour du logiciel**.

2. Dans l'espace de travail du dossier **Mises à jour du logiciel**, cliquez sur le lien **Actualiser** en haut à droite et attendez le téléchargement de la liste des mises à jour. Une liste des mises à jour s'affiche.

3. Sélectionnez les mises à jour que vous souhaitez approuver ou refuser.

   La zone d'informations correspondant aux objets sélectionnés apparaît du côté droit de l'espace de travail.

4. Dans la liste déroulante **État d'approbation de la mise à jour**, sélectionnez **Approuvée** pour approuver les mises à jour sélectionnées ou **Rejetée** pour refuser les mises à jour sélectionnées.

   La valeur par défaut est **Non défini**.

Les mises à jour auxquelles vous attribuez l'état **Approuvée** sont placées dans une file d'attente d'installation.

Les mises à jour auxquelles vous attribuez l'état **Rejetée** sont supprimées (si possible) de tous les appareils sur lesquels elles avaient été installées. Et elles ne seront installées sur aucun autre appareil à l'avenir.

Il est impossible de désinstaller certaines mises à jour pour les applications de Kaspersky. Si vous leur attribuez l'état **Rejetée**, Kaspersky Security Center ne les supprime pas des appareils sur lesquels elles avaient été installées. Toutefois, ces mises à jour ne seront jamais installées sur d'autres appareils à l'avenir. S'il est impossible de désinstaller une mise à jour pour des applications de Kaspersky, cette propriété est affichée dans la fenêtre des propriétés de la mise à jour : dans le volet **Sections**, sélectionnez **Général**, et la propriété apparaît dans l'espace de travail sous **Pré-requis d'installation**. Si vous attribuez l'état **Rejetée** aux mises à jour d'un logiciel tiers, ces mises à jour ne sont pas installées sur les appareils où elles ont été planifiées mais pas encore installées. Les mises à jour sont conservées sur les appareils où elles ont déjà été installées. Si vous devez les supprimer, vous pouvez réaliser l'opération manuellement localement.

Synchronisation des mises à jour Windows Update avec le Serveur d'administration

Si vous avez sélectionné **&Utiliser le Serveur d'administration comme serveur WSUS** dans la fenêtre **Paramètres d'administration des mises à jour** de l'Assistant de configuration initiale de l'application, la tâche de synchronisation de Windows Update est créée automatiquement. Il est possible de lancer la tâche dans le dossier **Tâches**. La fonctionnalité de mise à jour du logiciel Microsoft est disponible uniquement une fois que la tâche **Synchronisation des mises à jour Windows Update** s'est terminée avec succès.

Le nombre de mises à jour logicielles Microsoft peut dépasser 10 Go. Assurez-vous que la base de données du Serveur d'administration est capable de recevoir de tels volumes ; dans le cas contraire, la tâche **Synchronisation des mises à jour Windows Update** échouera. La base de données Microsoft SQL Express n'est pas prise en charge pour la tâche **Synchronisation des mises à jour Windows Update**.

La tâche **Synchronisation des mises à jour Windows Update** télécharge uniquement les métadonnées à partir des serveurs Microsoft. Si le réseau n'utilise pas de serveur WSUS, chaque appareil client télécharge indépendamment les mises à jour Microsoft depuis des serveurs externes.

Pour créer la tâche de synchronisation des mises à jour Windows Update avec le Serveur d'administration, procédez comme suit :

1. Dans l'arborescence de la console, accédez au dossier **Avancé** → **Gestion des applications**, puis le sous-dossier **Mises à jour du logiciel**.

2. Cliquez sur le bouton **Actions supplémentaires**, puis sélectionnez l'option **Configurer la synchronisation des mises à jour Windows Update** dans la liste déroulante.

   L'Assistant crée la tâche **Synchronisation des mises à jour Windows Update** affichée dans le dossier dans **Tâches**.

   L'Assistant de création de la tâche de récupération des données depuis le centre de mise à jour Windows démarre. Suivez les instructions de l'assistant.

La tâche de synchronisation des mises à jour Windows Update peut être également créée dans le dossier **Tâches**, en cliquant sur **Créer une tâche**.

Microsoft supprime périodiquement des serveurs de l'entreprise les mises à jour obsolètes de manière à ce que le nombre de mises à jour actuelles soit toujours compris entre 200 000 et 300 000. Afin de réduire l'espace disque utilisé et la taille de la base de données, Kaspersky Security Center supprime les mises à jour obsolètes qui ne figurent plus sur les serveurs de mise à jour de Microsoft.

Pendant l'exécution de la tâche **Synchronisation des mises à jour Windows Update**, l'application reçoit la liste des mises à jour actuelles depuis le serveur de mises à jour de Microsoft. Kaspersky Security Center définit ensuite la liste des mises à jour obsolètes. Lors du lancement suivant de la tâche **Recherche de vulnérabilités et de mises à jour requises**, Kaspersky Security Center identifie toutes les mises à jour obsolètes et détermine leur délai de suppression. Lors du lancement suivant de la tâche **Synchronisation des mises à jour Windows Update**, les mises à jour identifiées 30 jours auparavant comme devant être supprimées sont effectivement supprimées. Kaspersky Security Center effectue également une analyse complémentaire pour la suppression des mises à jour identifiées plus de 180 jours auparavant comme devant être supprimées.

Au terme de l'exécution de la tâche **Synchronisation des mises à jour Windows Update** et de la suppression des mises à jour obsolètes, les codes de hachage des fichiers des mises à jour supprimées peuvent persister dans la base de données, au même titre que les fichiers correspondants dans les fichiers %AllUsersProfile%\Application Data\KasperskyLab\adminkit\1093\.working\wusfiles (s'ils ont été préalablement téléchargés). Vous pouvez exécuter la tâche **Maintenance du Serveur d'administration** pour supprimer ces entrées obsolètes de la base de données, ainsi que les fichiers correspondants.

Étape 1. Définir s'il faut réduire le trafic

Quand Kaspersky Security Center synchronise les mises à jour avec les serveurs Microsoft Windows Update Servers, les informations relatives à l'ensemble des fichiers sont enregistrées dans la base de données du Serveur d'administration. De même, tous les fichiers indispensables à la mise à jour sont téléchargés sur le disque en cas d'interaction avec l'Agent de mises à jour Windows. Plus particulièrement, Kaspersky Security Center enregistre les informations relatives aux fichiers de mises à jour express dans la base de données et les télécharge en fonction des besoins. Le téléchargement des fichiers de mises à jour express provoque la réduction de l'espace disponible sur le disque.

Pour limiter la réduction de l'espace de disque et réduire le trafic, vous pouvez désactiver l'option **Télécharger les mises à jour rapides**.

Quand cette option est sélectionnée, les fichiers de mises à jour express sont téléchargés pendant l'exécution de la tâche. Par défaut, cette option n'est pas sélectionnée.

Étape 2. Applications

Cette section permet de sélectionner les applications dont les mises à jour seront téléchargées.

Si la case **Toutes les applications** est cochée, les mises à jour sont téléchargées pour toutes les applications existantes, ainsi que pour les applications susceptibles d'être éditées à l'avenir.

Par défaut, la case **Toutes les applications** est cochée.

Étape 3. Mise à jours des catégories

Cette section permet de sélectionner les catégories des mises à jour à télécharger sur le Serveur d'administration.

Si la case **Toutes les catégories** est cochée, les mises à jour sont téléchargées pour toutes les catégories de mises à jour disponibles, ainsi que pour les catégories qui pourraient apparaître à l'avenir.

La case **Toutes les catégories** est cochée par défaut.

Étape 4. Mises à jour des langues

Cette fenêtre permet de sélectionner les langues de localisation des mises à jour à télécharger sur le Serveur d'administration. Sélectionnez une des options suivantes de chargement des langues de localisation des mises à jour :

- **Télécharger toutes les langues, y compris les nouvelles langues**

  Si cette option a été sélectionnée, toutes les langues disponibles de localisation des mises à jour seront téléchargées sur le Serveur d'administration. Cette option est sélectionnée par défaut.

- **Télécharger les langues sélectionnées**

  Si cette option a été sélectionnée, la liste permet de sélectionner les langues de localisation des mises à jour à télécharger sur le Serveur d'administration.

Étape 5. Sélection du compte utilisateur pour télécharger une tâche

La fenêtre **Sélection du compte utilisateur pour exécuter la tâche** permet d'indiquer le compte utilisateur sous lequel la tâche va être exécutée. Sélectionnez l'une des options ci-dessous :

- **Compte par défaut**

  La tâche sera lancée sous le même compte utilisateur sous lequel l'application, exécutant cette tâche, a été installée et lancée.

  Cette option est sélectionnée par défaut.

- **Indiquer un compte**

  Remplissez les champs **Compte utilisateur** et **Mot de passe** pour définir les détails d'un compte à partir duquel la tâche est exécutée. Le compte doit disposer de droits suffisants pour cette tâche.

  - **Compte utilisateur**

    Le compte utilisateur au nom duquel la tâche sera lancée.

  - **Mot de passe**

    Mot de passe du compte utilisateur au nom duquel la tâche sera lancée.

Étape 6. Paramètres de la programmation d'une tâche

La page de l'Assistant **Planifier la tâche** permet de programmer le lancement de la tâche. Le cas échéant, configurez les paramètres suivants :

- **Lancement planifié :**

  Sélectionnez la programmation de l'exécution de la tâche, puis configurez la programmation sélectionnée.

  - **Toutes les N heures**

    La tâche s'exécute régulièrement, selon l'intervalle défini en heures, à partir de la date et heure définis.

    La tâche s'exécute par défaut toutes les six heures à partir de la date et de l'heure actuelles du système.

  - **Tous les N jours**

    La tâche s'exécute régulièrement, selon l'intervalle défini en jours. En outre, vous pouvez spécifier la date et l'heure de la première exécution de la tâche. Ces options supplémentaires deviennent disponibles si elles sont prises en charge par l'application pour laquelle vous créez la tâche.

    La tâche s'exécute par défaut chaque jour, à partir de la date et de l'heure actuelle du système.

  - **Toutes les N semaines**

    La tâche s'exécute régulièrement, selon l'intervalle défini en semaines, le jour indiqué de la semaine et à l'heure indiquée.

    La tâche s'exécute par défaut chaque lundi à l'heure système actuelle.

  - **Toutes les N minutes**

    La tâche s'exécute régulièrement, à l'intervalle défini en minutes, à partir de l'heure indiquée le jour de la création de la tâche.

    La tâche s'exécute par défaut toutes les 30 minutes, à partir de l'heure actuelle du système.

  - **Chaque jour (passage à l'heure d'été non pris en charge)**

    La tâche s'exécute régulièrement, selon l'intervalle défini en jours. Cette programmation ne tient pas compte du passage à l'heure d'été. Cela signifie que lorsque les horloges sont avancées ou reculées d'une heure au début ou à la fin de l'été, l'heure de lancement réelle de la tâche ne change pas.

    Nous déconseillons d'adopter cette programmation. Elle est requise pour la rétrocompatibilité avec Kaspersky Security Center.

    La tâche démarre par défaut chaque jour à l'heure système actuelle.

  - **Chaque semaine**

    La tâche s'exécute chaque semaine, le jour défini et à l'heure indiquée.

- **Par jours de la semaine**

  La tâche s'exécute régulièrement les jours définis de la semaine, à l'heure indiquée.

  Par défaut, la tâche s'exécute chaque vendredi à 18h00.

- **Chaque mois**

  La tâche s'exécute régulièrement le jour du mois défini, à l'heure indiquée.

  Si le jour en question ne figure pas dans le mois, la tâche s'exécute le dernier jour.

  La tâche s'exécute par défaut le premier jour de chaque mois, à l'heure système actuelle.

- **Manuel**

  La tâche ne s'exécute pas automatiquement. Vous pouvez uniquement la lancer manuellement.

  Cette option est sélectionnée par défaut.

- **Une fois**

  La tâche est exécutée une seule fois, à la date et à l'heure indiquées (par défaut, le jour de la création de la tâche).

- **Chaque mois, les jours indiqués des semaines sélectionnées**

  La tâche s'exécute régulièrement les jours du mois définis, à l'heure indiquée.

  Par défaut, aucun jour du mois n'est sélectionné. L'heure de début par défaut est 18:00.

- **Lors de la détection d'une attaque de virus**

  La tâche s'exécute après un événement *Attaque de virus* de virus. Sélectionnez les types d'application qui vont surveiller les propagations de virus. Les types suivants de Application sont présent :

  - Antivirus pour postes de travail et serveurs de fichiers
  - Antivirus de protection du périmètre
  - Antivirus pour systèmes de messagerie

  Tous les types d'application sont cochés par défaut.

  Il se peut que vous souhaitiez exécuter différentes tâches en fonction du type d'application de sécurité qui signale une propagation de virus. Dans ce cas, supprimez la sélection des types d'application dont vous n'avez pas besoin.

- **Après l'exécution d'une autre tâche**

La tâche actuelle démarre à la fin d'une autre tâche. Cette option ne fonctionne que si les deux tâches sont affectées aux mêmes appareils. Par exemple, vous pouvez exécuter la tâche *Administration des appareils* avec l'option **&Activer l'appareil** et, une fois celle-ci terminée, exécuter la tâche de *recherche de virus* comme tâche de déclenchement.

Il faut sélectionner la tâche de déclenchement dans le tableau et l'état avec lequel cette tâche doit se terminer (**Terminée avec succès** ou **Échec**).

Si nécessaire, vous pouvez rechercher, trier et filtrer les tâches dans le tableau comme suit :

- Saisissez le nom de la tâche dans le champ de recherche pour rechercher une tâche par son nom.
- Cliquez sur l'icône de tri pour trier les tâches par nom.

  Par défaut, les tâches sont triées par ordre alphabétique croissant.
- Cliquez sur l'icône du filtre, et dans la fenêtre qui s'ouvre, filtrez les tâches par groupe, puis cliquez sur le bouton **Appliquer**.

- **Lancer les tâches non exécutées**

  Cette option détermine le comportement d'une tâche si un appareil client n'est pas visible sur le réseau quand la tâche est sur le point de démarrer.

  Si la case est Activé, lors du lancement suivant de l'application de Kaspersky sur cet appareil client, une tentative de lancement de la tâche sera faite. Si la programmation de la tâche est **Manuel**, **Une fois** ou **Immédiatement**, la tâche est immédiatement lancée dès que l'appareil apparaît sur le réseau ou immédiatement après l'inclusion de l'appareil dans la zone d'action de la tâche.

  Si cette option est désactivée, seules les tâches planifiées s'exécutent sur les appareils clients. Pour les planifications **Manuel**, **Une fois** et **Immédiatement**, les tâches s'exécutent uniquement sur les appareils clients qui sont visibles sur le réseau. Par exemple, vous pouvez désactiver cette option pour une tâche qui consomme des ressources que vous voulez exécuter uniquement en dehors des heures de bureau.

  Cette option est Inactif par défaut.

- Adopter un décalage aléatoire automatique pour les lancements de tâche

  Si cette option est activée, la tâche est lancée sur les appareils clients de manière aléatoire au cours d'un intervalle défini. C'est ce qu'on appelle un *lancement échelonné d'une tâche*. Un lancement échelonné de tâche permet d'éviter la communication simultanée d'un nombre important d'appareils clients avec le Serveur d'administration lors du lancement de la tâche programmée.

  Le temps du lancement aléatoire est automatiquement calculée lors de la création d'une tâche selon le nombre d'appareils clients sur lesquels la tâche est diffusée. Par la suite, la tâche démarre toujours à l'heure de lancement calculée. Toutefois, quand les paramètres de la tâche sont modifiés ou si la tâche est lancée manuellement, la valeur calculée de l'heure de lancement de la tâche est modifiée.

  Si la case n'est pas cochée, le lancement de la tâche sur les appareils clients s'opère selon la planification.

- Décaler aléatoirement le lancement de la tâche dans un intervalle de (min.)

  Si cette option est activée, la tâche est lancée sur les appareils clients de manière aléatoire au cours de l'intervalle défini. Un lancement échelonné de tâche permet d'éviter la communication simultanée d'un nombre important d'appareils clients avec le Serveur d'administration lors du lancement de la tâche programmée.

  Si la case n'est pas cochée, le lancement de la tâche sur les appareils clients s'opère selon la planification.

  Cette option est Inactif par défaut. Par défaut, la valeur de cet intervalle est de une minute.

Étape 7. Définition du nom de la tâche

La fenêtre **Définition du nom de la tâche** permet de renseigner le nom de la tâche que vous créez. Un nom de tâche ne peut pas compter plus de 100 caractères et ni des caractères spéciaux (`"*<>?\:|`). La valeur par défaut est *Synchronisation des mises à jour Windows Update*.

Étape 8. Fin de la création d'une tâche

Dans la fenêtre **Fin de la création de la tâche**, cliquez sur le bouton **Terminé** pour quitter l'Assistant.

Si vous souhaitez que la tâche démarre directement à la fin de l'Assistant, cochez la case **&Lancer la tâche à la fin de l'Assistant**

La tâche de synchronisation des mises à jour Windows Update qui vient d'être créée apparaît dans la liste des tâches dans le dossier **Tâches** de l'arborescence de la console.

Installation manuelle des mises à jour sur les appareils

Si vous avez sélectionné **Rechercher et installer les mises à jour requises** sur la page **Paramètres d'administration des mises à jour** de l'Assistant de configuration initiale de l'application, la tâche *Installation des mises à jour requises et correction des vulnérabilités* est automatiquement créée. Il est possible d'exécuter ou d'arrêter la tâche dans le dossier **Appareils administrés** sous l'onglet **Tâches**.

Si, dans l'Assistant de configuration initiale de l'application vous avez sélectionné l'option **Rechercher les mises à jour requises**, vous pouvez installer les mises à jour du logiciel sur les appareils clients à l'aide de la tâche *Installation des mises à jour requises et correction des vulnérabilités*.

Vous pouvez réaliser une des opérations suivantes :

- Créer une tâche pour installer les mises à jour.
- Ajouter une règle pour installer une mise à jour à une tâche de mise à jour existante.
- Dans les paramètres d'une tâche d'installation de mise à jour existante, configurez une installation d'essai des mises à jour.

Une interaction utilisateur peut être requise lorsque vous mettez à jour une application tierce ou corrigez une vulnérabilité dans une application tierce sur un appareil administré. Par exemple, l'utilisateur peut être invité à fermer l'application tierce si elle est actuellement ouverte.

Installation des mises à jour via la création d'une tâche d'installation

Vous pouvez réaliser une des opérations suivantes :

- Créer une tâche pour installer certaines mises à jour.
- Sélectionner une mise à jour et créer une tâche pour installer celle-ci et d'autres similaires.

Pour installer des mises à jour particulières :

1. Dans l'arborescence de la console, accédez au dossier **Avancé** → **Gestion des applications**, puis le sous-dossier **Mises à jour du logiciel**.
2. Dans l'espace de travail, sélectionnez les mises à jour que vous souhaitez installer.
3. Réalisez une des opérations suivantes :
   - Cliquez-droit sur l'une des mises à jour sélectionnées dans la liste, puis sélectionnez l'option **Installer la mise à jour** → **Nouvelle tâche**.
   - Cliquez sur le lien **Installer la mise à jour (créer la tâche)** dans la zone d'informations correspondant à la mise à jour sélectionnée.
4. Faites votre choix dans l'invite qui s'affiche au sujet de l'installation de toutes les mise à jour de l'application antérieures. Cliquez sur **Oui** si vous acceptez d'installer les versions successives de l'application de manière incrémentielle si cela s'impose pour installer les mises à jour sélectionnées. Cliquez sur **Non** si vous souhaitez mettre à jour les applications de manière directe, sans installer les versions intermédiaires. S'il est impossible d'installer les mises à jour sélectionnées sans installer les versions antérieures de l'application, la mise à jour de l'application échoue.

   L'Assistant de création de la tâche d'installation des mises à jour et de correction des vulnérabilités démarre. Suivez les étapes de l'assistant.

5. Sur la page **Sélection de l'option de redémarrage du système d'exploitation** option de l'Assistant, sélectionnez l'action à réaliser lorsque le système d'exploitation sur les appareils clients doit redémarrer après l'opération :

- **Ne pas redémarrer l'appareil**

  Les appareils clients ne redémarrent pas automatiquement après l'opération. Pour arrêter le fonctionnement, il faut redémarrer l'appareil (par exemple, manuellement ou à l'aide d'une tâche d'administration des appareils). Les informations sur la nécessité du redémarrage sont enregistrées dans les résultats de la tâche et dans l'état de l'appareil. Cette option convient aux tâches d' sur les serveurs et autres appareils pour lesquels la continuité des opérations est critique.

- **Redémarrer l'appareil**

  Dans ce cas, le redémarrage des appareils clients est toujours exécuté automatiquement, si celui-ci est requis pour terminer l'opération. Cette option convient aux tâches d' sur des appareils pour lesquels des interruptions périodiques sont admises (débranchement, redémarrage).

- **Confirmer l'action auprès de l'utilisateur**

  Le message qui signale que l'appareil client doit être redémarré manuellement s'affiche sur l'écran de l'appareil. Pour cette option, il est possible de configurer des paramètres avancés : le texte du message pour l'utilisateur, la fréquence du message, ainsi que le délai à l'issue duquel le redémarrage sera forcé (sans confirmation de l'utilisateur). Cette option convient le mieux pour les postes de travail sur lesquels les utilisateurs doivent pouvoir sélectionner l'heure de redémarrage qui leur convient le mieux.

  Cette option est sélectionnée par défaut.

  - **Répéter la demande toutes les (min.)**

    Quand cette option est activée, l'application invite l'utilisateur à redémarrer le système d'exploitation selon la fréquence indiquée.

    Cette option est activée par défaut. L'intervalle par défaut est de 5 minutes. La valeur peut être comprise entre 1 et 1 440 minutes.

    Si cette option est désactivée, l'invite est affichée une seule fois.

  - **Redémarrer au bout de (min.)**

    Après avoir averti l'utilisateur, l'application force le redémarrage du système d'exploitation à l'issue de l'intervalle défini.

    Cette option est activée par défaut. Le délai par défaut est de 30 minutes. La valeur peut être comprise entre 1 et 1 440 minutes.

- **Forcer la fermeture des applications dans les sessions bloquées**

Les applications en cours d'exécution peuvent empêcher le redémarrage de l'appareil client. Par exemple, si un document est en train d'être modifié dans un logiciel de traitement de texte et qu'il n'est pas enregistré, l'application n'autorise pas le redémarrage de l'appareil.

Quand cette option est activée, l'arrêt forcé de ces applications sur un appareil verrouillé doit avoir lieu avant de pouvoir redémarrer l'appareil. Les utilisateurs pourraient perdre toute modification qui n'a pas été enregistrée à ce moment.

Si cette option est désactivée, un appareil verrouillé n'est pas redémarré. L'état de la tâche sur cet appareil indique qu'il faut redémarrer l'appareil. Les utilisateurs doivent quitter manuellement toutes les applications en cours d'exécution sur les appareils verrouillés, puis redémarrer ces appareils.

Cette option est Inactif par défaut.

6. La page **Planifier la tâche** de l'Assistant vous permet de programmer le lancement de la tâche. Le cas échéant, configurez les paramètres suivants :

- **Lancement planifié :**

  Sélectionnez la programmation de l'exécution de la tâche, puis configurez la programmation sélectionnée.

  - **Toutes les N heures**

    La tâche s'exécute régulièrement, selon l'intervalle défini en heures, à partir de la date et heure définis.

    La tâche s'exécute par défaut toutes les six heures à partir de la date et de l'heure actuelles du système.

  - **Tous les N jours**

    La tâche s'exécute régulièrement, selon l'intervalle défini en jours. En outre, vous pouvez spécifier la date et l'heure de la première exécution de la tâche. Ces options supplémentaires deviennent disponibles si elles sont prises en charge par l'application pour laquelle vous créez la tâche.

    La tâche s'exécute par défaut chaque jour, à partir de la date et de l'heure actuelle du système.

  - **Toutes les N semaines**

    La tâche s'exécute régulièrement, selon l'intervalle défini en semaines, le jour indiqué de la semaine et à l'heure indiquée.

    La tâche s'exécute par défaut chaque lundi à l'heure système actuelle.

  - **Toutes les N minutes**

    La tâche s'exécute régulièrement, à l'intervalle défini en minutes, à partir de l'heure indiquée le jour de la création de la tâche.

    La tâche s'exécute par défaut toutes les 30 minutes, à partir de l'heure actuelle du système.

  - **Chaque jour (passage à l'heure d'été non pris en charge)**

    La tâche s'exécute régulièrement, selon l'intervalle défini en jours. Cette programmation ne tient pas compte du passage à l'heure d'été. Cela signifie que lorsque les horloges sont avancées ou reculées d'une heure au début ou à la fin de l'été, l'heure de lancement réelle de la tâche ne change pas.

    Nous déconseillons d'adopter cette programmation. Elle est requise pour la rétrocompatibilité avec Kaspersky Security Center.

    La tâche démarre par défaut chaque jour à l'heure système actuelle.

  - **Chaque semaine**

    La tâche s'exécute chaque semaine, le jour défini et à l'heure indiquée.

- **Par jours de la semaine**

  La tâche s'exécute régulièrement les jours définis de la semaine, à l'heure indiquée.

  Par défaut, la tâche s'exécute chaque vendredi à 18h00.

- **Chaque mois**

  La tâche s'exécute régulièrement le jour du mois défini, à l'heure indiquée.

  Si le jour en question ne figure pas dans le mois, la tâche s'exécute le dernier jour.

  La tâche s'exécute par défaut le premier jour de chaque mois, à l'heure système actuelle.

- **Manuel**

  La tâche ne s'exécute pas automatiquement. Vous pouvez uniquement la lancer manuellement.

  Cette option est sélectionnée par défaut.

- **Chaque mois, les jours indiqués des semaines sélectionnées**

  La tâche s'exécute régulièrement les jours du mois définis, à l'heure indiquée.

  Par défaut, aucun jour du mois n'est sélectionné. L'heure de début par défaut est 18:00.

- **Lors de la détection d'une attaque de virus**

  La tâche s'exécute après un événement *Attaque de virus* de virus. Sélectionnez les types d'application qui vont surveiller les propagations de virus. Les types suivants de Application sont présent :

  - Antivirus pour postes de travail et serveurs de fichiers
  - Antivirus de protection du périmètre
  - Antivirus pour systèmes de messagerie

  Tous les types d'application sont cochés par défaut.

  Il se peut que vous souhaitiez exécuter différentes tâches en fonction du type d'application de sécurité qui signale une propagation de virus. Dans ce cas, supprimez la sélection des types d'application dont vous n'avez pas besoin.

- **Après l'exécution d'une autre tâche**

La tâche actuelle démarre à la fin d'une autre tâche. Cette option ne fonctionne que si les deux tâches sont affectées aux mêmes appareils. Par exemple, vous pouvez exécuter la tâche *Administration des appareils* avec l'option **&Activer l'appareil** et, une fois celle-ci terminée, exécuter la tâche de *recherche de virus* comme tâche de déclenchement.

Il faut sélectionner la tâche de déclenchement dans le tableau et l'état avec lequel cette tâche doit se terminer (**Terminée avec succès** ou **Échec**).

Si nécessaire, vous pouvez rechercher, trier et filtrer les tâches dans le tableau comme suit :

- Saisissez le nom de la tâche dans le champ de recherche pour rechercher une tâche par son nom.
- Cliquez sur l'icône de tri pour trier les tâches par nom.

  Par défaut, les tâches sont triées par ordre alphabétique croissant.
- Cliquez sur l'icône du filtre, et dans la fenêtre qui s'ouvre, filtrez les tâches par groupe, puis cliquez sur le bouton **Appliquer**.

- **Lancer les tâches non exécutées**

  Cette option détermine le comportement d'une tâche si un appareil client n'est pas visible sur le réseau quand la tâche est sur le point de démarrer.

  Si la case est Activé, lors du lancement suivant de l'application de Kaspersky sur cet appareil client, une tentative de lancement de la tâche sera faite. Si la programmation de la tâche est **Manuel**, **Une fois** ou **Immédiatement**, la tâche est immédiatement lancée dès que l'appareil apparaît sur le réseau ou immédiatement après l'inclusion de l'appareil dans la zone d'action de la tâche.

  Si cette option est désactivée, seules les tâches planifiées s'exécutent sur les appareils clients. Pour les planifications **Manuel**, **Une fois** et **Immédiatement**, les tâches s'exécutent uniquement sur les appareils clients qui sont visibles sur le réseau. Par exemple, vous pouvez désactiver cette option pour une tâche qui consomme des ressources que vous voulez exécuter uniquement en dehors des heures de bureau.

  Cette option est Inactif par défaut.

- **Adopter un décalage aléatoire automatique pour les lancements de tâche**

  Si cette option est activée, la tâche est lancée sur les appareils clients de manière aléatoire au cours d'un intervalle défini. C'est ce qu'on appelle un *lancement échelonné d'une tâche*. Un lancement échelonné de tâche permet d'éviter la communication simultanée d'un nombre important d'appareils clients avec le Serveur d'administration lors du lancement de la tâche programmée.

  Le temps du lancement aléatoire est automatiquement calculée lors de la création d'une tâche selon le nombre d'appareils clients sur lesquels la tâche est diffusée. Par la suite, la tâche démarre toujours à l'heure de lancement calculée. Toutefois, quand les paramètres de la tâche sont modifiés ou si la tâche est lancée manuellement, la valeur calculée de l'heure de lancement de la tâche est modifiée.

  Si la case n'est pas cochée, le lancement de la tâche sur les appareils clients s'opère selon la planification.

- **Décaler aléatoirement le lancement de la tâche dans un intervalle de (min.)**

Si cette option est activée, la tâche est lancée sur les appareils clients de manière aléatoire au cours de l'intervalle défini. Un lancement échelonné de tâche permet d'éviter la communication simultanée d'un nombre important d'appareils clients avec le Serveur d'administration lors du lancement de la tâche programmée.

Si la case n'est pas cochée, le lancement de la tâche sur les appareils clients s'opère selon la planification.

Cette option est Inactif par défaut. Par défaut, la valeur de cet intervalle est de une minute.

7. La page **Définition du nom de la tâche** de l'Assistant permet de renseigner le nom de la tâche en cours de création. Le nom de la tâche ne peut pas contenir plus de 100 symboles et contenir de symboles spéciaux ("*<>?\:|).

8. Sur la page **Fin de la création de la tâche** de l'Assistant, cliquez sur le bouton **Terminer** pour quitter l'Assistant.

   Si vous souhaitez que la tâche démarre directement à la fin de l'Assistant, cochez la case **&Lancer la tâche à la fin de l'Assistant**.

Une fois que l'Assistant a terminé son opération, la tâche **Installation des mises à jour requises et correction des vulnérabilités** apparaît dans le dossier **Tâches**.

Vous pouvez activer l'installation automatique des modules système (prérequis) avant l'installation d'une mise à jour dans les propriétés de la tâche *Installation des mises à jour requises et correction des vulnérabilités*. Dans ce cas, avant l'installation d'une mise à jour, une installation de tous les modules système requis est exécutée. La liste de ces modules est à consulter dans les propriétés de la mise à jour.

Dans les propriétés de la tâche *Installation des mises à jour requises et correction des vulnérabilités*, vous pouvez autoriser l'installation des mises à jour qui permettent de passer à une nouvelle version de l'application.

Si, dans les paramètres de la tâche, les règles d'installation des mises à jour d'éditeurs étrangers sont configurées, le Serveur d'administration télécharge les mises à jour requises à partir du site des éditeurs. Les mises à jour sont conservées dans le stockage du Serveur d'administration et ensuite sont diffusées et sont installées sur les appareils où elles sont appliquées.

Si dans les paramètres de la tâche sont configurées les règles d'installation des mises à jour Microsoft et que le Serveur d'administration est utilisé comme serveur WSUS, le Serveur d'administration télécharge les mises à jour requises dans le stockage et les diffuse ensuite aux appareils administrés. Si le réseau n'utilise pas de serveur WSUS, chaque appareil client télécharge indépendamment les mises à jour Microsoft depuis des serveurs externes.

Pour installer une certaine mise à jour et des mises à jour similaires :

1. Dans l'arborescence de la console, accédez au dossier **Avancé** → **Gestion des applications**, puis le sous-dossier **Mises à jour du logiciel**.

2. Dans l'espace de travail, sélectionnez la mise à jour que vous souhaitez installer.

3. Cliquez sur le bouton **Lancer l'Assistant d'installation de la mise à jour**.

   L'Assistant d'installation de la mise à jour démarre.

   Les fonctionnalités de l'Assistant d'installation de la mise à jour sont uniquement accessibles en présence d'une licence pour le fonctionnement de Gestion des vulnérabilités et des correctifs.

   Suivez les étapes de l'assistant.

4. Dans la page **Recherche des tâches existantes d'installation de la mise à jour**, configurez les paramètres suivants :

   - **&Rechercher les tâches d'installation de cette mise à jour**

     Quand cette option est activée, l'Assistant d'installation de la mise à jour recherche les tâches existantes qui installent la mise à jour sélectionnée.

     Si cette option est désactivée ou si la recherche ne trouve aucune tâche applicable, l'Assistant d'installation de la mise à jour vous invite à créer une règle ou une tâche pour installer la mise à jour.

     Cette option est activée par défaut.

   - **&Approuver l'installation de la mise à jour**

     La mise à jour sélectionnée est approuvée pour l'installation. Activez cette option si certaines règles appliquées de l'installation de la mise à jour autorisent l'installation des mises à jour confirmées uniquement.

     Cette option est Inactif par défaut.

5. Si vous décidez de recherche des tâches existantes d'installation de la mise à jour et si quelques tâches sont ainsi récupérées, vous pouvez consulter leurs propriétés ou les lancer manuellement. Il n'y a rien d'autre à faire.

   Sinon, cliquez sur le bouton **Nouvelle tâche d'installation de la mise à jour**.

6. Sélectionnez le type de règle d'installation à ajouter à la nouvelle tâche, puis cliquez sur le bouton **Terminer**.

7. Faites votre choix dans l'invite qui s'affiche au sujet de l'installation de toutes les mise à jour de l'application antérieures. Cliquez sur **Oui** si vous acceptez d'installer les versions successives de l'application de manière incrémentielle si cela s'impose pour installer les mises à jour sélectionnées. Cliquez sur **Non** si vous souhaitez mettre à jour les applications de manière directe, sans installer les versions intermédiaires. S'il est impossible d'installer les mises à jour sélectionnées sans installer les versions antérieures de l'application, la mise à jour de l'application échoue.

   L'Assistant de création de la tâche d'installation des mises à jour et de correction des vulnérabilités démarre. Suivez les étapes de l'assistant.

8. Sur la page **Sélection de l'option de redémarrage du système d'exploitation** option de l'Assistant, sélectionnez l'action à réaliser lorsque le système d'exploitation sur les appareils clients doit redémarrer après l'opération :

- Ne pas redémarrer l'appareil

  Les appareils clients ne redémarrent pas automatiquement après l'opération. Pour arrêter le fonctionnement, il faut redémarrer l'appareil (par exemple, manuellement ou à l'aide d'une tâche d'administration des appareils). Les informations sur la nécessité du redémarrage sont enregistrées dans les résultats de la tâche et dans l'état de l'appareil. Cette option convient aux tâches d' sur les serveurs et autres appareils pour lesquels la continuité des opérations est critique.

- Redémarrer l'appareil

  Dans ce cas, le redémarrage des appareils clients est toujours exécuté automatiquement, si celui-ci est requis pour terminer l'opération. Cette option convient aux tâches d' sur des appareils pour lesquels des interruptions périodiques sont admises (débranchement, redémarrage).

- Confirmer l'action auprès de l'utilisateur

  Le message qui signale que l'appareil client doit être redémarré manuellement s'affiche sur l'écran de l'appareil. Pour cette option, il est possible de configurer des paramètres avancés : le texte du message pour l'utilisateur, la fréquence du message, ainsi que le délai à l'issue duquel le redémarrage sera forcé (sans confirmation de l'utilisateur). Cette option convient le mieux pour les postes de travail sur lesquels les utilisateurs doivent pouvoir sélectionner l'heure de redémarrage qui leur convient le mieux.

  Cette option est sélectionnée par défaut.

  - Répéter la demande toutes les (min.)

    Quand cette option est activée, l'application invite l'utilisateur à redémarrer le système d'exploitation selon la fréquence indiquée.

    Cette option est activée par défaut. L'intervalle par défaut est de 5 minutes. La valeur peut être comprise entre 1 et 1 440 minutes.

    Si cette option est désactivée, l'invite est affichée une seule fois.

  - Redémarrer au bout de (min.)

    Après avoir averti l'utilisateur, l'application force le redémarrage du système d'exploitation à l'issue de l'intervalle défini.

    Cette option est activée par défaut. Le délai par défaut est de 30 minutes. La valeur peut être comprise entre 1 et 1 440 minutes.

- Forcer la fermeture des applications dans les sessions bloquées

Les applications en cours d'exécution peuvent empêcher le redémarrage de l'appareil client. Par exemple, si un document est en train d'être modifié dans un logiciel de traitement de texte et qu'il n'est pas enregistré, l'application n'autorise pas le redémarrage de l'appareil.

Quand cette option est activée, l'arrêt forcé de ces applications sur un appareil verrouillé doit avoir lieu avant de pouvoir redémarrer l'appareil. Les utilisateurs pourraient perdre toute modification qui n'a pas été enregistrée à ce moment.

Si cette option est désactivée, un appareil verrouillé n'est pas redémarré. L'état de la tâche sur cet appareil indique qu'il faut redémarrer l'appareil. Les utilisateurs doivent quitter manuellement toutes les applications en cours d'exécution sur les appareils verrouillés, puis redémarrer ces appareils.

Cette option est Inactif par défaut.

9. Sur la page **Sélectionnez les appareils auxquels la tâche sera affectée** de l'Assistant, sélectionnez l'une des options suivantes :

- Sélectionner les appareils détectés sur le réseau par le Serveur d'administration

  la tâche est affectée à un ensemble d'appareils. L'ensemble d'appareils peut reprendre aussi bien des appareils de groupes d'administration que des appareils non définis.

  Par exemple, vous pourriez utiliser cette option dans une tâche d'installation d'un Agent d'administration sur des appareils non définis.

- Définir les adresses des appareils manuellement ou les importer à partir d'une liste

  Vous pouvez définir les noms NetBIOS, les noms DNS, les adresses IP, ainsi que les plages d'adresses IP auxquels il convient d'affecter la tâche.

  Vous pourriez utiliser cette option pour exécuter une tâche pour un sous-réseau défini. Par exemple, vous pourriez souhaiter installer une certaine application sur les appareils des comptables ou analyser des appareils dans un sous-réseau qui est probablement infecté.

- Attribuer la tâche à une sélection d'appareils

  La tâche est affectée aux appareils qui appartiennent à une sélection d'appareils. Vous pouvez définir une des sélections existantes.

  Par exemple, vous pourriez souhaiter utiliser cette option pour exécuter une tâche sur des appareils dotés d'une version du système d'exploitation spécifique.

- Attribuer la tâche à un groupe d'administration

  La tâche est affectée aux appareils qui appartiennent à un groupe d'administration. Vous pouvez renseigner un des groupes existants ou en créer un.

  Par exemple, vous pourriez souhaiter utiliser cette option pour exécuter une tâche d'envoi de messages pour les utilisateurs si le message est particulier pour les appareils repris dans un groupe d'administration spécifique.

  Si une tâche est attribuée à un groupe d'administration, l'onglet **Sécurité** ne s'affiche pas dans la fenêtre des propriétés de la tâche, car les tâches de groupe sont soumises aux paramètres de sécurité des groupes auxquels elles s'appliquent.

10. La page **Planifier la tâche** de l'Assistant vous permet de programmer le lancement de la tâche. Le cas échéant, configurez les paramètres suivants :

- **Lancement planifié :**

  Sélectionnez la programmation de l'exécution de la tâche, puis configurez la programmation sélectionnée.

  - **Toutes les N heures**

    La tâche s'exécute régulièrement, selon l'intervalle défini en heures, à partir de la date et heure définis.

    La tâche s'exécute par défaut toutes les six heures à partir de la date et de l'heure actuelles du système.

  - **Tous les N jours**

    La tâche s'exécute régulièrement, selon l'intervalle défini en jours. En outre, vous pouvez spécifier la date et l'heure de la première exécution de la tâche. Ces options supplémentaires deviennent disponibles si elles sont prises en charge par l'application pour laquelle vous créez la tâche.

    La tâche s'exécute par défaut chaque jour, à partir de la date et de l'heure actuelle du système.

  - **Toutes les N semaines**

    La tâche s'exécute régulièrement, selon l'intervalle défini en semaines, le jour indiqué de la semaine et à l'heure indiquée.

    La tâche s'exécute par défaut chaque lundi à l'heure système actuelle.

  - **Toutes les N minutes**

    La tâche s'exécute régulièrement, à l'intervalle défini en minutes, à partir de l'heure indiquée le jour de la création de la tâche.

    La tâche s'exécute par défaut toutes les 30 minutes, à partir de l'heure actuelle du système.

  - **Chaque jour (passage à l'heure d'été non pris en charge)**

    La tâche s'exécute régulièrement, selon l'intervalle défini en jours. Cette programmation ne tient pas compte du passage à l'heure d'été. Cela signifie que lorsque les horloges sont avancées ou reculées d'une heure au début ou à la fin de l'été, l'heure de lancement réelle de la tâche ne change pas.

    Nous déconseillons d'adopter cette programmation. Elle est requise pour la rétrocompatibilité avec Kaspersky Security Center.

    La tâche démarre par défaut chaque jour à l'heure système actuelle.

  - **Chaque semaine**

    La tâche s'exécute chaque semaine, le jour défini et à l'heure indiquée.

- **Par jours de la semaine**

  La tâche s'exécute régulièrement les jours définis de la semaine, à l'heure indiquée.

  Par défaut, la tâche s'exécute chaque vendredi à 18h00.

- **Chaque mois**

  La tâche s'exécute régulièrement le jour du mois défini, à l'heure indiquée.

  Si le jour en question ne figure pas dans le mois, la tâche s'exécute le dernier jour.

  La tâche s'exécute par défaut le premier jour de chaque mois, à l'heure système actuelle.

- **Manuel** (Sélectionné par défaut)

  La tâche ne s'exécute pas automatiquement. Vous pouvez uniquement la lancer manuellement.

  Cette option est sélectionnée par défaut.

- **Chaque mois, les jours indiqués des semaines sélectionnées**

  La tâche s'exécute régulièrement les jours du mois définis, à l'heure indiquée.

  Par défaut, aucun jour du mois n'est sélectionné. L'heure de début par défaut est 18:00.

- **Lors de la détection d'une attaque de virus**

  La tâche s'exécute après un événement *Attaque de virus* de virus. Sélectionnez les types d'application qui vont surveiller les propagations de virus. Les types suivants de Application sont présent :

  - Antivirus pour postes de travail et serveurs de fichiers
  - Antivirus de protection du périmètre
  - Antivirus pour systèmes de messagerie

  Tous les types d'application sont cochés par défaut.

  Il se peut que vous souhaitiez exécuter différentes tâches en fonction du type d'application de sécurité qui signale une propagation de virus. Dans ce cas, supprimez la sélection des types d'application dont vous n'avez pas besoin.

- **Après l'exécution d'une autre tâche**

La tâche actuelle démarre à la fin d'une autre tâche. Cette option ne fonctionne que si les deux tâches sont affectées aux mêmes appareils. Par exemple, vous pouvez exécuter la tâche *Administration des appareils* avec l'option **&Activer l'appareil** et, une fois celle-ci terminée, exécuter la tâche de *recherche de virus* comme tâche de déclenchement.

Il faut sélectionner la tâche de déclenchement dans le tableau et l'état avec lequel cette tâche doit se terminer (**Terminée avec succès** ou **Échec**).

Si nécessaire, vous pouvez rechercher, trier et filtrer les tâches dans le tableau comme suit :

- Saisissez le nom de la tâche dans le champ de recherche pour rechercher une tâche par son nom.
- Cliquez sur l'icône de tri pour trier les tâches par nom.

  Par défaut, les tâches sont triées par ordre alphabétique croissant.
- Cliquez sur l'icône du filtre, et dans la fenêtre qui s'ouvre, filtrez les tâches par groupe, puis cliquez sur le bouton **Appliquer**.

- **Lancer les tâches non exécutées**

  Cette option détermine le comportement d'une tâche si un appareil client n'est pas visible sur le réseau quand la tâche est sur le point de démarrer.

  Si la case est Activé, lors du lancement suivant de l'application de Kaspersky sur cet appareil client, une tentative de lancement de la tâche sera faite. Si la programmation de la tâche est **Manuel**, **Une fois** ou **Immédiatement**, la tâche est immédiatement lancée dès que l'appareil apparaît sur le réseau ou immédiatement après l'inclusion de l'appareil dans la zone d'action de la tâche.

  Si cette option est désactivée, seules les tâches planifiées s'exécutent sur les appareils clients. Pour les planifications **Manuel**, **Une fois** et **Immédiatement**, les tâches s'exécutent uniquement sur les appareils clients qui sont visibles sur le réseau. Par exemple, vous pouvez désactiver cette option pour une tâche qui consomme des ressources que vous voulez exécuter uniquement en dehors des heures de bureau.

  Cette option est Inactif par défaut.

- **Décaler aléatoirement le lancement de la tâche dans un intervalle de (min.)**

  Si cette option est activée, la tâche est lancée sur les appareils clients de manière aléatoire au cours d'un intervalle défini. C'est ce qu'on appelle un *lancement échelonné d'une tâche*. Un lancement échelonné de tâche permet d'éviter la communication simultanée d'un nombre important d'appareils clients avec le Serveur d'administration lors du lancement de la tâche programmée.

  Le temps du lancement aléatoire est automatiquement calculée lors de la création d'une tâche selon le nombre d'appareils clients sur lesquels la tâche est diffusée. Par la suite, la tâche démarre toujours à l'heure de lancement calculée. Toutefois, quand les paramètres de la tâche sont modifiés ou si la tâche est lancée manuellement, la valeur calculée de l'heure de lancement de la tâche est modifiée.

  Si la case n'est pas cochée, le lancement de la tâche sur les appareils clients s'opère selon la planification.

- **Décaler aléatoirement le lancement de la tâche dans un intervalle de (min.)**

Si cette option est activée, la tâche est lancée sur les appareils clients de manière aléatoire au cours de l'intervalle défini. Un lancement échelonné de tâche permet d'éviter la communication simultanée d'un nombre important d'appareils clients avec le Serveur d'administration lors du lancement de la tâche programmée.

Si la case n'est pas cochée, le lancement de la tâche sur les appareils clients s'opère selon la planification.

Cette option est Inactif par défaut. Par défaut, la valeur de cet intervalle est de une minute.

11. La page **Définition du nom de la tâche** de l'Assistant permet de renseigner le nom de la tâche en cours de création. Le nom de la tâche ne peut pas contenir plus de 100 symboles et contenir de symboles spéciaux ("*<>?\:|).

12. Sur la page **Fin de la création de la tâche** de l'Assistant, cliquez sur le bouton **Terminer** pour quitter l'Assistant.

    Si vous souhaitez que la tâche démarre directement à la fin de l'Assistant, cochez la case **&Lancer la tâche à la fin de l'Assistant**.

Une fois que l'Assistant a terminé, la tâche **Installation des mises à jour requises et correction des vulnérabilités** est créée. Cette tâche s'affiche dans le dossier **Tâches**.

En plus des paramètres que vous définissez lors de la création de la tâche, vous pouvez modifier d'autres propriétés de la tâche créée.

Après l'installation de la nouvelle version de l'application, le fonctionnement d'autres applications, installées sur les appareils et qui dépendent du fonctionnement de l'application installée, peut être troublé.

Installation d'une mise à jour en ajoutant une règle à une tâche d'installation existante

Pour installer une mise à jour en ajoutant une règle à une tâche d'installation existante:

1. Dans l'arborescence de la console, accédez au dossier **Avancé** → **Gestion des applications**, puis le sous-dossier **Mises à jour du logiciel**.

2. Dans l'espace de travail, sélectionnez la mise à jour que vous souhaitez installer.

3. Cliquez sur le bouton **Lancer l'Assistant d'installation de la mise à jour**.

   L'Assistant d'installation de la mise à jour démarre.

   Les fonctionnalités de l'Assistant d'installation de la mise à jour sont uniquement accessibles en présence d'une licence pour le fonctionnement de Gestion des vulnérabilités et des correctifs.

   Suivez les étapes de l'assistant.

4. Dans la page **Recherche des tâches existantes d'installation de la mise à jour**, configurez les paramètres suivants :

   - **&Rechercher les tâches d'installation de cette mise à jour**

     Quand cette option est activée, l'Assistant d'installation de la mise à jour recherche les tâches existantes qui installent la mise à jour sélectionnée.

     Si cette option est désactivée ou si la recherche ne trouve aucune tâche applicable, l'Assistant d'installation de la mise à jour vous invite à créer une règle ou une tâche pour installer la mise à jour.

     Cette option est activée par défaut.

   - **&Approuver l'installation de la mise à jour**

     La mise à jour sélectionnée est approuvée pour l'installation. Activez cette option si certaines règles appliquées de l'installation de la mise à jour autorisent l'installation des mises à jour confirmées uniquement.

     Cette option est Inactif par défaut.

5. Si vous décidez de recherche des tâches existantes d'installation de la mise à jour et si quelques tâches sont ainsi récupérées, vous pouvez consulter leurs propriétés ou les lancer manuellement. Il n'y a rien d'autre à faire.

   Dans le cas contraire, cliquez sur le bouton **Ajouter une règle d'installation de la mise à jour**.

6. Sélectionnez la tâche à laquelle vous souhaitez ajouter une règle, puis cliquez sur le bouton **Ajouter une règle**.

   Vous pouvez également consulter les propriétés des tâches existantes, les lancer manuellement ou créer une tâche.

7. Sélectionnez le type de la règle à ajouter à la tâche sélectionnée, puis cliquez sur le bouton **Terminer**.

8. Faites votre choix dans l'invite qui s'affiche au sujet de l'installation de toutes les mise à jour de l'application antérieures. Cliquez sur **Oui** si vous acceptez d'installer les versions successives de l'application de manière incrémentielle si cela s'impose pour installer les mises à jour sélectionnées. Cliquez sur **Non** si vous souhaitez mettre à jour les applications de manière directe, sans installer les versions intermédiaires. S'il est impossible d'installer les mises à jour sélectionnées sans installer les versions antérieures de l'application, la mise à jour de l'application échoue.

Une nouvelle règle pour l'ajout d'une mise à jour est ajouté à la tâche **Installation des mises à jour requises et correction des vulnérabilités** existante.

Configuration d'une installation de contrôle des mises à jour

Pour configurer l'installation de contrôle des mises à jour, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez la tâche **Installation des mises à jour requises et correction des vulnérabilités** dans le dossier **Appareils administrés** de l'onglet **Tâches**.

2. Dans le menu contextuel de la tâche, choisissez l'option **Propriétés**.

   La fenêtre des propriétés de la tâche **Installation des mises à jour requises et correction des vulnérabilités** s'ouvre.

3. Dans la fenêtre des propriétés de la tâche, dans la section **Installation de contrôle**, sélectionnez l'une des options disponibles de l'installation de contrôle :

   - **Ne pas analyser**. Sélectionnez cette option si vous ne voulez pas exécuter l'installation de contrôle des mises à jour.

   - **Lancer l'analyse sur les &appareils indiqués**. Sélectionnez cette option si vous voulez vérifier l'installation des mises à jour sur certains appareils. Cliquez sur le bouton **Ajouter** et sélectionnez les appareils sur lesquels vous devez exécuter l'installation de contrôle des mises à jour.

   - **Lancer l'analyse sur les appareils dans le &groupe indiqué**. Sélectionnez cette option si vous voulez vérifier l'installation des mises à jour sur le groupe d'appareils. Dans le champ **Définissez le groupe test**, indiquez le groupe d'appareils sur lesquels exécuter l'installation de contrôle.

   - **Lancer l'analyse sur le &pourcentage indiqué des appareils**. Sélectionnez cette option si vous voulez lancer l'analyse des mises à jour sur une partie des appareils. Dans le champ **Le pourcentage des appareils de test du nombre total des appareils cibles**, indiquez le pourcentage des appareils qui requièrent l'exécution de l'installation de contrôle des mises à jour.

4. Lors de la sélection de n'importe quelle option autre que **Ne pas analyser**, indiquez dans le champ **Temps nécessaire pour décider si l'installation doit être poursuivie, en heures** le nombre d'heures qui doit s'écouler après l'installation de contrôle des mises à jour avant de lancer l'installation des mises à jour sur tous les appareils.

Configuration des mises à jour Windows dans la stratégie de l'Agent d'administration

Pour configurer les mises à jour Windows dans la stratégie de l'Agent d'administration, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez **Appareils administrés**.

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

3. Sélectionnez une stratégie d'Agent d'administration.

4. Dans le menu contextuel de la stratégie, sélectionnez l'option **Propriétés**.

   La fenêtre des propriétés de la stratégie de l'Agent d'administration s'ouvre.

5. Dans le volet **Sections**, sélectionnez **Mises à jour et vulnérabilités du logiciel**.

6. Sélectionnez l'option **&Utiliser le Serveur d'administration comme serveur WSUS** pour télécharger les mises à jour Windows sur le Serveur d'administration puis les distribuer sur les appareils clients à l'aide de l'Agent d'administration.

   Si l'option n'est pas sélectionnée, les mises à jour Windows ne sont pas téléchargées sur le Serveur d'administration. Dans ce cas, les appareils clients reçoivent les mises à jour Windows directement depuis les serveurs Microsoft.

7. Sélectionnez l'ensemble de mises à jour que les utilisateurs peuvent installer sur leurs appareils manuellement en utilisant Windows Update.

Sur les appareils exécutés sous Windows 10, si Windows Update a déjà trouvé des mises à jour pour l'appareil, la nouvelle option que vous sélectionnez sous **Autoriser les utilisateurs à gérer l'installation des mises à jour de Windows Update** ne sera appliquée qu'une fois les mises à jour installées.

Sélectionnez une option dans la liste déroulante :

- **Autoriser les utilisateurs à installer toutes les mises à jour Windows Update applicables**

  Les utilisateurs peuvent installer toutes les mises à jour Microsoft Windows Update applicables à leurs appareils.

  Sélectionnez cette option si vous ne voulez pas exécuter l'installation de contrôle des mises à jour.

  Lorsque l'utilisateur installe des mises à jour Microsoft Windows Update manuellement, les mises à jour peuvent être téléchargées depuis les serveurs de Microsoft au lieu des Serveurs d'administration. Ceci est possible si le Serveur d'administration n'a pas encore téléchargé ces mises à jour. Le téléchargement des mises à jour depuis les serveurs de Microsoft génère un trafic supplémentaire.

- **Autoriser les utilisateurs à installer uniquement les mises à jour Windows Update autorisées**

  Les utilisateurs peuvent installer toutes les mises à jour Microsoft Windows Update applicables à leurs appareils et que vous avez approuvées.

  Par exemple, vous souhaitez d'abord vérifier l'installation des mises à jour dans un environnement d'essai et vous assurer qu'elles ne perturbent pas le fonctionnement des appareils avant d'autoriser l'installation de ces mises à jour confirmées sur les appareils clients.

  Lorsque l'utilisateur installe des mises à jour Microsoft Windows Update manuellement, les mises à jour peuvent être téléchargées depuis les serveurs de Microsoft au lieu des Serveurs d'administration. Ceci est possible si le Serveur d'administration n'a pas encore téléchargé ces mises à jour. Le téléchargement des mises à jour depuis les serveurs de Microsoft génère un trafic supplémentaire.

- **Ne pas autoriser les utilisateurs à installer les mises à jour Windows Update**

  Les utilisateurs ne peuvent pas installer manuellement les mises à jour Microsoft Windows Update sur leurs appareils. Toutes les mises à jour applicables sont installées selon votre configuration.

  Choisissez cette option, si vous voulez administrer centralement l'installation des mises à jour.

  Par exemple, il se peut que vous souhaitiez optimiser la programmation des mises à jour afin de ne pas surcharger le réseau. Vous pouvez programmer les mises à jour en dehors des heures de travail afin qu'elles n'interfèrent pas avec la productivité de l'utilisateur.

8. Sélectionnez le mode de recherche de Windows Update :

- **Actif**

  Si cette option a été sélectionnée, le Serveur d'administration à l'aide de l'Agent d'administration initie la demande de l'Agent de mises à jour Windows sur l'appareil client à la source des mises à jour : Windows Update Servers or WSUS. Ensuite, l'Agent d'administration transmet sur le Serveur d'administration les informations obtenues en provenance de l'Agent de mises à jour Windows.

  L'option ne prend effet que si l'option **Se connecter au serveur de mise à jour pour mettre à jour les données** de la tâche *Recherche de vulnérabilités et de mises à jour requises* est sélectionnée.

  Cette option est sélectionnée par défaut.

- **Passif**

  Si cette option a été sélectionnée, l'Agent d'administration transmet périodiquement sur le Serveur d'administration les informations sur les mises à jour obtenues lors de la dernières synchronisation de l'Agent de mises à jour Windows avec la source des mises à jour. Si la synchronisation de l'Agent de mises à jour Windows avec la source des mises à jour n'est pas exécutée, les données sur les mises à jour sur le Serveur d'administration vieillissent.

  Sélectionnez cette option si vous souhaitez obtenir des mises à jour à partir du cache mémoire de la source des mises à jour.

- **Désactivé**

  Si cette option a été sélectionnée, le Serveur d'administration ne formule aucune requête d'informations sur les mises à jour.

  Sélectionnez cette option si, par exemple, vous souhaitez d'abord tester les mises à jour sur votre appareil local.

9. Sélectionnez l'option **Analyser les fichiers exécutables à la recherche de vulnérabilités lors du lancement** si vous souhaitez analyser les fichiers exécutables pour détecter les vulnérabilités lors de leur exécution.

10. Assurez-vous que l'édition est verrouillée pour tous les paramètres que vous avez modifiés. Sinon, les modifications ne s'appliquent pas.

11. Cliquez sur le bouton **Appliquer**.

Correction des vulnérabilités logicielles tierces

Cette section décrit les fonctions de Kaspersky Security Center associées à la correction des vulnérabilités dans les logiciels installés sur les appareils administrés.

Scénario : Recherche et correction des vulnérabilités dans les logiciels tiers

Cette section fournit un scénario de recherche et de réparation des vulnérabilités sur les appareils administrés sous Windows. Vous pouvez rechercher et corriger les vulnérabilités dans les applications du système d'exploitation et dans les logiciels tiers, y compris les logiciels Microsoft.

Prérequis

- Kaspersky Security Center est déployé dans votre entreprise.
- Il existe des appareils administrés sous Windows dans votre organisation.
- Une connexion Internet est requise pour que le Serveur d'administration puisse effectuer les tâches suivantes :
  - Pour dresser une liste des correctifs recommandés pour les vulnérabilités des logiciels Microsoft. La liste est créée et régulièrement mise à jour par des spécialistes de Kaspersky.
  - Pour corriger les vulnérabilités de logiciels tiers autres que les logiciels Microsoft.

Étapes

La recherche et la correction des vulnérabilités logicielles s'effectuent par étapes :

1. **Recherche de vulnérabilités dans les logiciels installés sur les appareils administrés**

   Pour rechercher les vulnérabilités dans les logiciels installés sur les appareils administrés, exécutez la tâche *Recherche de vulnérabilités et de mises à jour requises*. Une fois cette tâche terminée, Kaspersky Security Center reçoit la liste des vulnérabilités détectées et des mises à jour requises pour les logiciels tiers installés sur les appareils que vous avez spécifiés dans les propriétés de la tâche.

   La tâche *Recherche de vulnérabilités et de mises à jour requises* est créée automatiquement par l'Assistant de configuration initiale de l'application Kaspersky Security Center. Si vous n'aviez pas exécuté l'Assistant, démarrez-le maintenant ou créez la tâche manuellement.

   Instructions pour :

   - Console d'administration : Recherche de vulnérabilités dans les applications, Planification de la tâche Recherche de vulnérabilités et des mises à jour requises
   - Kaspersky Security Center Web Console : création d'une tâche Recherche de vulnérabilités et de mises à jour requises, paramètres de Recherche de vulnérabilités et de mises à jour requises

2. **Analyser la liste des vulnérabilités logicielles détectées**

   Consultez la liste **Vulnérabilités dans les applications** et décidez quelles vulnérabilités doivent être corrigées. Pour consulter les informations détaillées de chaque vulnérabilité, cliquez sur le nom de la vulnérabilité dans la liste. Pour chaque vulnérabilité de la liste, vous pouvez également consulter les statistiques de la vulnérabilité sur les appareils administrés.

   Instructions pour :

   - Console d'administration : consultation des informations concernant les vulnérabilités logicielles, consultation des statistiques des vulnérabilités sur les appareils administrés
   - Kaspersky Security Center Web Console : Affichage des informations sur les vulnérabilités logicielles, Affichage des statistiques des vulnérabilités sur les appareils administrés

3. **Configuration de la correction des vulnérabilités**

   Lorsque des vulnérabilités sont détectées dans les applications, vous pouvez les corriger sur les appareils administrés à l'aide de la tâche *Installation des mises à jour requises et correction des vulnérabilités* ou de la tâche *Corriger les vulnérabilités*.

La tâche *Installation des mises à jour requises et correction des vulnérabilités* est utilisée pour effectuer les mises à jour et réparer les vulnérabilités de logiciels tiers, y compris les logiciels Microsoft, installés sur les appareils administrés. Cette tâche vous permet d'installer plusieurs mises à jour et de corriger différentes vulnérabilités en fonction de certaines règles. Notez que cette tâche ne peut être créée que si vous disposez de la licence pour la fonctionnalité Gestion des vulnérabilités et des correctifs. Pour corriger les vulnérabilités dans les applications, la tâche *Installation des mises à jour requises et correction des vulnérabilités* utilise les mises à jour logicielles recommandées.

La tâche *Corriger les vulnérabilités* ne nécessite pas l'option de licence pour la fonction Gestion des vulnérabilités et des correctifs. Pour utiliser cette tâche, vous devez spécifier manuellement les correctifs servant à corriger les vulnérabilités du logiciel tiers répertorié dans les paramètres de la tâche. La tâche *Corriger les vulnérabilités* utilise les correctifs recommandés pour les logiciels Microsoft et les correctifs utilisateurs pour les logiciels tiers.

Vous pouvez démarrer l'Assistant de correction des vulnérabilités qui crée automatiquement l'une de ces tâches ou vous pouvez créer l'une de ces tâches manuellement.

Instructions pour :

- Console d'administration : Sélection des correctifs utilisateur pour les vulnérabilités dans le logiciel tiers, Correction des vulnérabilités dans les applications
- Kaspersky Security Center Web Console : Sélection des correctifs utilisateur pour les vulnérabilités dans le logiciel tiers, Correction des vulnérabilités dans le logiciels tiers, Création de la tâche Installation des mises à jour requises et correction des vulnérabilités

4 Planification des tâches

Pour vous assurer que la liste des vulnérabilités est toujours d'actualité, planifiez la tâche *Recherche de vulnérabilités et de mises à jour requises* pour l'exécuter automatiquement de temps à autre. La fréquence moyenne recommandée est d'une fois par semaine.

Si vous avez créé la tâche *Installation des mises à jour requises et correction des vulnérabilités*, vous pouvez la planifier pour qu'elle soit exécutée à la même fréquence que la tâche *Recherche de vulnérabilités et de mises à jour requises* ou à une fréquence moindre. Lors de la planification de la tâche *Corriger les vulnérabilités*, notez que vous devez sélectionner des correctifs pour les logiciels Microsoft ou définir des correctifs utilisateur pour les logiciels tiers à chaque fois avant de démarrer la tâche.

Lors de la planification des tâches, assurez-vous qu'une tâche pour corriger la vulnérabilité démarre une fois que la tâche *Recherche de vulnérabilités et de mises à jour requises* est terminée.

5 Ignorer les vulnérabilités dans les applications (facultatif)

Vous pouvez si vous les souhaitez ignorer les vulnérabilités dans les applications à corriger sur tous les appareils administrés ou seulement sur les appareils administrés sélectionnés.

Instructions pour :

- Console d'administration : ignorer les vulnérabilités dans les applications
- Kaspersky Security Center Web Console : ignorer les vulnérabilités dans les applications

6 Exécution d'une tâche de correction de la vulnérabilité

Démarrez la tâche *Installation des mises à jour requises et correction des vulnérabilités* ou la tâche *Corriger la vulnérabilité*. Lorsque la tâche est terminée, assurez-vous qu'elle possède le statut *Terminée* dans la liste des tâches.

7 Créer le rapport sur les résultats de la correction des vulnérabilités dans les applications (facultatif)

Pour consulter les statistiques détaillées concernant la correction des vulnérabilités, générez le rapport sur les vulnérabilités. Le rapport affiche des informations sur les vulnérabilités dans les applications non corrigées. Ainsi, vous pouvez vous faire une idée de la recherche et la correction des vulnérabilités dans les logiciels tiers, y compris les logiciels Microsoft, dans votre organisation.

Instructions pour :

- Console d'administration : création et affichage d'un rapport
- Kaspersky Security Center Web Console : génération et affichage d'un rapport

8. **Vérification de la configuration de la recherche et de la correction des vulnérabilités dans les logiciels tiers**

   Assurez-vous d'avoir effectué les tâches suivantes :

   - Obtenu et vérifié la liste des vulnérabilités logicielles sur les appareils administrés
   - Ignoré les vulnérabilités dans les applications que vous souhaitiez ignorer
   - Configuré la tâche de correction des vulnérabilités
   - Planifié les tâches de recherche et de correction des vulnérabilités logicielles pour qu'elles démarrent en séquence
   - Vérifié que la tâche de correction des vulnérabilités dans les applications a été exécutée

Résultats

Si vous avez créé et configuré la tâche *Installation des mises à jour requises et correction des vulnérabilités*, les vulnérabilités sont corrigées automatiquement sur les appareils administrés. Lorsque la tâche est exécutée, elle met en corrélation la liste des mises à jour logicielles disponibles avec les règles spécifiées dans les paramètres de la tâche. Toutes les mises à jour logicielles qui répondent aux critères des règles seront téléchargées dans le stockage du Serveur d'administration et seront installées pour corriger les vulnérabilités dans les applications.

Si vous avez créé la tâche *Corriger les vulnérabilités*, seules les vulnérabilités dans les applications des logiciels Microsoft sont corrigées.

À propos de la recherche et de la correction des vulnérabilités dans les applications

Kaspersky Security Center détecte et répare les vulnérabilités dans les applications sur les appareils administrés exécutant des familles de systèmes d'exploitation Microsoft Windows. Les vulnérabilités sont détectées dans le système d'exploitation et les logiciels tiers, y compris les logiciels Microsoft.

> La fonctionnalité des mises à jour (y compris la fourniture de mises à jour des signatures antivirus et des bases de code) ainsi que la fonctionnalité KSN peuvent ne pas être disponibles dans le logiciel aux États-Unis.

Recherche des vulnérabilités dans les applications

Pour rechercher des vulnérabilités dans les applications, Kaspersky Security Center utilise les caractéristiques de la base de données des vulnérabilités connues. Cette base de données est créée par les spécialistes de Kaspersky. Elle contient des informations sur les vulnérabilités, telles que la description, la date de détection et le niveau de gravité de la vulnérabilité. Vous pouvez recevoir des informations sur les vulnérabilités dans les applications sur le site Kaspersky.

Kaspersky Security Center utilise la tâche *Recherche de vulnérabilités et de mises à jour requises* pour détecter d'éventuelles vulnérabilités logicielles.

Dans certains cas, les vulnérabilités détectées dans un système d'exploitation Microsoft Windows peuvent être corrigées à l'aide d'une des méthodes suivantes :

- Installation d'une mise à jour pour le système d'exploitation.
- Mise à niveau du système d'exploitation vers une version plus récente (par exemple, de Windows 10 vers Windows 11).

Dans ce scénario, Kaspersky Security Center affiche deux entrées pour la même vulnérabilité.

Correction des vulnérabilités logicielles

Pour corriger les vulnérabilités dans les applications, Kaspersky Security Center utilise les mises à jour logicielles publiées par les fournisseurs de logiciels. Les métadonnées des mises à jour logicielles sont téléchargées sur le stockage du Serveur d'administration après l'exécution des tâches suivantes :

- *Téléchargement des mises à jour sur le stockage du Serveur d'administration*. Cette tâche est destinée à télécharger les métadonnées des mises à jour pour Kaspersky et les logiciels tiers. Cette tâche est créée automatiquement par l'Assistant de configuration initiale de l'application Kaspersky Security Center. Vous pouvez créer manuellement la tâche Télécharger les mises à jour dans le stockage du Serveur d'administration.
- *Synchronisation des mises à jour Windows Update*. Cette tâche est destinée à télécharger les métadonnées des mises à jour pour les logiciels Microsoft.

Les mises à jour logicielles visant à corriger les vulnérabilités peuvent être représentées sous forme de paquets de distribution complets ou de correctifs. Les mises à jour logicielles qui corrigent des vulnérabilités dans les applications sont appelées *correctifs*. L'installation *des correctifs recommandés* est préconisée par les spécialistes Kaspersky. L'installation *des correctifs utilisateur* est manuellement spécifiée par les utilisateurs. Pour installer un correctif utilisateur, vous devez créer un paquet d'installation contenant ce correctif.

Si vous détenez la licence de Kaspersky Security Center assortie de la fonctionnalité Gestion des vulnérabilités et des correctifs, pour corriger les vulnérabilités dans les applications, vous pouvez utiliser la tâche *Installation des mises à jour requises et correction des vulnérabilités*. Cette tâche corrige automatiquement de nombreuses vulnérabilités en installant les correctifs recommandés. Pour cette tâche, vous pouvez configurer manuellement certaines règles pour corriger plusieurs vulnérabilités.

Si vous ne détenez pas la licence de Kaspersky Security Center assortie de la fonctionnalité Gestion des vulnérabilités et des correctifs, pour corriger les vulnérabilités dans les applications, vous pouvez utiliser la tâche *Corriger les vulnérabilités*. À l'aide de cette tâche, vous pouvez corriger les vulnérabilités en installant les correctifs recommandés pour les logiciels Microsoft et les correctifs utilisateur pour les autres logiciels tiers.

Pour des raisons de sécurité, toutes les mises à jour logicielles tierces que vous installez à l'aide de la fonction de la gestion des vulnérabilités et des correctifs sont automatiquement analysées à la recherche de logiciels malveillants par les technologies de Kaspersky. Ces technologies sont utilisées pour la vérification automatique des fichiers et incluent la recherche de virus, l'analyse statique, l'analyse dynamique, l'analyse comportementale dans l'environnement sandbox et machine learning.

Les experts de Kaspersky n'effectuent pas d'analyse manuelle des mises à jour du logiciel tiers pouvant être installées par la fonction de la gestion des vulnérabilités et des correctifs. De plus, les experts de Kaspersky ne recherchent pas de vulnérabilités (connues ou inconnues) ou de fonctionnalités non documentées dans ces mises à jour, et n'effectuent pas d'autres types d'analyse des mises à jour que ceux indiqués dans le paragraphe ci-dessus.

Une interaction utilisateur peut être requise lorsque vous mettez à jour une application tierce ou corrigez une vulnérabilité dans une application tierce sur un appareil administré. Par exemple, l'utilisateur peut être invité à fermer l'application tierce si elle est actuellement ouverte.

Pour corriger certaines vulnérabilités dans les applications, vous devrez accepter le Contrat de licence utilisateur final (CLUF) du logiciel en cours d'installation si l'acceptation du CLUF est demandée. Si vous refusez le CLUF, la vulnérabilité logicielle ne sera pas corrigée.

Consultation des informations relatives aux vulnérabilités dans les applications

Pour consulter la liste des vulnérabilités détectées sur les appareils clients,

Dans l'arborescence de la console, accédez au dossier **Avancé** → **Gestion des applications**, puis le sous-dossier **Vulnérabilités dans les applications**.

La page affiche une liste des vulnérabilités dans les applications détectées sur les appareils administrés.

Pour obtenir les informations sur la vulnérabilité sélectionnée,

Dans le menu contextuel de la vulnérabilité, sélectionnez **Propriétés**.

La fenêtre des propriétés de la vulnérabilité s'ouvre. Cette fenêtre affiche les informations suivantes :

- L'application contenant la vulnérabilité.
- La liste des appareils avec la vulnérabilité détectée.
- les informations sur la correction de la vulnérabilité.

Pour consulter le rapport sur toutes les vulnérabilités détectées,

Dans le dossier **Vulnérabilités dans les applications**, cliquez sur le lien **Consulter le rapport sur les vulnérabilités**.

Le rapport sur les vulnérabilités dans les applications installées sur les appareils sera créé. Le rapport peut être consulté dans l'entrée portant le nom du Serveur d'administration concerné, en ouvrant l'onglet **Rapports**.

Consultation des statistiques relatives aux vulnérabilités sur les appareils administrés

Vous pouvez consulter les statistiques pour chaque vulnérabilité dans les applications des appareils administrés. Les statistiques sont représentées sous forme de diagramme. Le diagramme affiche le nombre d'appareils ayant les états suivants :

- *Ignorée sur : <nombre d'appareils>*. Cet état est attribué si vous avez réglé manuellement l'option d'ignorer la vulnérabilité dans les propriétés de cette dernière.
- *Corrigée sur : <nombre d'appareils>*. Cet état est attribué si la tâche visant à corriger la vulnérabilité est terminée avec succès.
- *Correctif prévu sur : <nombre d'appareils>*. Cet état est attribué si vous avez créé la tâche visant à corriger la vulnérabilité, mais qu'elle n'a pas encore été effectuée.
- *Correctif appliqué sur : <nombre d'appareils>*. Cet état est attribué si vous avez sélectionné manuellement la mise à jour du logiciel pour corriger la vulnérabilité, mais que cette mise à jour n'a pas corrigé la vulnérabilité.
- *Correctif nécessaire sur : <nombre d'appareils>*. Cet état est attribué si la vulnérabilité a été corrigée uniquement sur certains appareils administrés et si la correction de la vulnérabilité est nécessaire sur d'autres appareils.

Pour consulter les statistiques d'une vulnérabilité sur les appareils administrés :

1. Dans l'arborescence de la console, accédez au dossier **Avancé** → **Gestion des applications**, puis le sous-dossier **Vulnérabilités dans les applications**.

   La page affiche une liste des vulnérabilités dans les applications détectées sur les appareils administrés.

2. Sélectionnez une vulnérabilité pour laquelle vous souhaitez afficher les statistiques.

   Dans le bloc servant à travailler avec un objet sélectionné, un diagramme des états de vulnérabilité est affiché. Cliquer sur un état ouvre une liste des appareils sur lesquels la vulnérabilité possède l'état sélectionné.

Recherche de vulnérabilités dans les applications

Si vous avez configuré l'application à l'aide de l'Assistant de configuration initiale de l'application, la tâche *Recherche de vulnérabilités* est créée automatiquement. Il est possible de consulter la tâche dans le dossier **Appareils administrés**, sous l'onglet **Tâches**.

Pour créer une tâche de recherche de vulnérabilités dans les applications installées sur les appareils clients, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez **Avancé** → **Gestion des applications**, puis sélectionnez le sous-dossier **Vulnérabilités dans les applications**.

2. Dans l'espace de travail, sélectionnez **Actions supplémentaires** → **Configurer la recherche de vulnérabilités**.

   Si une tâche de recherche de vulnérabilités existe déjà, l'onglet **Tâches** du dossier **Appareils administrés** s'affiche, avec la tâche existante sélectionnée. Dans le cas contraire, l'Assistant de création de la tâche de recherche de vulnérabilités et de mises à jour requises démarre. Suivez les étapes de l'assistant.

3. Dans la fenêtre **Sélection du type de tâche**, sélectionnez **Recherche de vulnérabilités et de mises à jour requises**.

4. Sur la page **Paramètres** de l'Assistant, définissez les paramètres de la tâche comme suit :

- **Rechercher les vulnérabilités et les mises à jour indiquées par Microsoft**

  Lors de la recherche de vulnérabilités et de mises à jour, Kaspersky Security Center utilise les informations sur les mises à jour Microsoft applicables à partir de la source des mises à jour Microsoft disponibles à ce moment là.

  Par exemple, pensez à désactiver cette option si vous avez différentes tâches avec différents paramètres pour les mises à jour Microsoft et les mises à jour d'applications tierces.

  Cette option est activée par défaut.

  Les informations sur les mises à jour facultatives de Microsoft Windows Update ne sont pas envoyées au Serveur d'administration.

- **Se connecter au serveur de mise à jour pour mettre à jour les données**

L'Agent de mises à jour Windows sur un appareil administré se connecte à la source des mises à jour Microsoft. Les serveurs suivants peuvent servir de source de mises à jour Microsoft :

- Serveur d'administration de Kaspersky Security Center (voir les paramètres de stratégie de l'Agent d'administration)
- Serveur Windows sur lequel Microsoft Windows Server Update Services (WSUS) est déployé dans le réseau de votre organisation
- Serveurs de mises à jour Microsoft

Si cette option est activée, l'Agent de mises à jour Windows sur un appareil administré se connecte à la source de mise à jour Microsoft pour actualiser les informations relatives aux mises à jour Microsoft Windows applicables.

Si cette option est désactivée, l'Agent de mises à jour Windows sur un appareil administré utilise les informations relatives aux mises à jour Microsoft Windows obtenues antérieurement auprès de la source des mises à jour Microsoft.

La connexion à la source des mises à jour Microsoft peut requérir beaucoup de ressources. Pensez à désactiver cette option si vous définissez une connexion régulière à cette source de mises à jour dans une autre tâche ou dans les propriétés de la stratégie de l'Agent d'administration, dans la section **Mises à jour et vulnérabilités du logiciel**. Si vous ne souhaitez pas désactiver cette option, pour réduire la surcharge, vous pouvez configurer la planification des tâches pour randomiser le délai de démarrage des tâches dans les 360 minutes.

Cette option est activée par défaut.

La combinaison des options suivantes des paramètres de la stratégie de l'Agent d'administration définit le mode d'obtention des mises à jour :

- L'Agent de mises à jour Windows sur un appareil administré se connecte au Serveur de mises à jour pour obtenir les mises à jour uniquement si l'option **Se connecter au serveur de mise à jour pour mettre à jour les données** est activée dans les propriétés de la tâche *Recherche de vulnérabilités et de mises à jour requises* et si l'option **Mode de recherche des mises à jour Windows Update** est définie sur **Actif** dans les paramètres de la stratégie de l'Agent d'administration.
- Si vous n'avez pas besoin de l'Agent d'administration pour établir une connexion à la source des mises à jour Microsoft Windows et télécharger les mises à jour lors de l'exécution de la tâche *Recherche de vulnérabilités*, vous pouvez définir l'option **Mode de recherche des mises à jour Windows Update** sur **Passif**, tandis que l'option **Se connecter au serveur de mise à jour pour mettre à jour les données** doit rester activée. Cela vous permet d'économiser des ressources et d'utiliser les mises à jour de Windows déjà reçues pour vérifier la présence de vulnérabilités. Vous pouvez utiliser le mode passif si vous configurez la réception des mises à jour Microsoft Windows différemment. Si la réception des mises à jour Microsoft Windows n'est pas configurée d'une autre manière, ne définissez pas l'option du **Mode de recherche des mises à jour Windows Update** sur **Passif**, car dans ce cas, les informations sur les mises à jour ne seront jamais reçues.
- Quel que soit l'état de l'option **Se connecter au serveur de mise à jour pour mettre à jour les données** (activé ou désactivé), si l'option **Mode de recherche des mises à jour Windows Update** est définie sur **Désactivé**, Kaspersky Security Center ne demande aucune information sur les mises à jour.

- Rechercher les vulnérabilités et les mises à jour de tiers indiquées par Kaspersky

Si cette option est activée, Kaspersky Security Center recherche des vulnérabilités et les mises à jour requises des produits tiers (applications développées par des éditeurs d'application autres que Kaspersky et Microsoft) dans le Registre Windows et dans les dossiers définis sous **Indiquez les chemins pour la recherche avancée des applications dans le système de fichiers**. La liste complète des produits tiers pris en charge est administrée par Kaspersky.

Si cette option est désactivée, Kaspersky Security Center ne recherche pas les vulnérabilités et les mises à jour requises pour les applications tiers. Par exemple, pensez à désactiver cette option si vous avez différentes tâches avec différents paramètres pour les mises à jour Microsoft Windows et les mises à jour d'applications tierces.

Cette option est activée par défaut.

- **Indiquez les chemins pour la recherche avancée des applications dans le système de fichiers**

  Les dossiers dans lesquels Kaspersky Security Center recherche des produits tiers qui requièrent une correction de la vulnérabilité et l'installation d'une mise à jour. Vous pouvez utiliser des variables système.

  Indiquez les dossiers dans lesquels les applications doivent être installées. Par défaut, la liste contient les dossiers système dans lesquels la majorité des applications sont installées.

- **Activer le diagnostic avancé**

  Quand cette fonction est activée, l'Agent d'administration enregistre des fichiers de trace même si l'écriture de fichiers de trace est désactivée pour l'Agent d'administration dans l'utilitaire de diagnostic à distance Kaspersky Security Center. Les traces sont enregistrées dans deux fichiers en alternance la taille de chacun de ces fichiers est déterminée par la valeur paramètre **Taille maximale (Mo) des fichiers de diagnostic avancé**. Quand les deux fichiers sont remplis, l'Agent d'administration écrit à nouveau dans ceux-ci. Les fichiers avec les traces sont stockés dans le dossier %WINDIR%\Temp. Ces fichiers sont accessibles dans l'utilitaire de diagnostic à distance, vous pouvez les télécharger ou les supprimer à cet endroit.

  Quand cette fonction est désactivée, l'Agent d'administration enregistre les traces conformément aux paramètres définis dans l'utilitaire de diagnostic à distance Kaspersky Security Center. Aucune trace complémentaire n'est écrite.

  Lors de la création d'une tâche, il n'est pas nécessaire d'activer le diagnostic avancé. Par contre, vous pouvez activer cette fonction plus tard si, par exemple, une tâche échoue sur certains appareils et que vous souhaitez obtenir des informations complémentaires lors d'une autre exécution de la tâche.

  Cette option est Inactif par défaut.

- **Taille maximale (Mo) des fichiers de diagnostic avancé**

  La valeur par défaut est de 100 Mo, mais elle peut se situer entre 1 et 2 048 Mo. Il peut arriver qu'un expert du Support Technique de Kaspersky vous demande de modifier la valeur par défaut lorsque les informations reprises dans les fichiers de diagnostic avancés que vous avez envoyés ne suffisent pas pour résoudre le problème.

5. La page **Planifier la tâche** de l'Assistant vous permet de programmer le lancement de la tâche. Le cas échéant, configurez les paramètres suivants :

- **Lancement planifié :**

  Sélectionnez la programmation de l'exécution de la tâche, puis configurez la programmation sélectionnée.

  - **Toutes les N heures**

    La tâche s'exécute régulièrement, selon l'intervalle défini en heures, à partir de la date et heure définis.

    La tâche s'exécute par défaut toutes les six heures à partir de la date et de l'heure actuelles du système.

  - **Tous les N jours**

    La tâche s'exécute régulièrement, selon l'intervalle défini en jours. En outre, vous pouvez spécifier la date et l'heure de la première exécution de la tâche. Ces options supplémentaires deviennent disponibles si elles sont prises en charge par l'application pour laquelle vous créez la tâche.

    La tâche s'exécute par défaut chaque jour, à partir de la date et de l'heure actuelle du système.

  - **Toutes les N semaines**

    La tâche s'exécute régulièrement, selon l'intervalle défini en semaines, le jour indiqué de la semaine et à l'heure indiquée.

    La tâche s'exécute par défaut chaque lundi à l'heure système actuelle.

  - **Toutes les N minutes**

    La tâche s'exécute régulièrement, à l'intervalle défini en minutes, à partir de l'heure indiquée le jour de la création de la tâche.

    La tâche s'exécute par défaut toutes les 30 minutes, à partir de l'heure actuelle du système.

  - **Chaque jour (passage à l'heure d'été non pris en charge)**

    La tâche s'exécute régulièrement, selon l'intervalle défini en jours. Cette programmation ne tient pas compte du passage à l'heure d'été. Cela signifie que lorsque les horloges sont avancées ou reculées d'une heure au début ou à la fin de l'été, l'heure de lancement réelle de la tâche ne change pas.

    Nous déconseillons d'adopter cette programmation. Elle est requise pour la rétrocompatibilité avec Kaspersky Security Center.

    La tâche démarre par défaut chaque jour à l'heure système actuelle.

  - **Chaque semaine**

    La tâche s'exécute chaque semaine, le jour défini et à l'heure indiquée.

- **Par jours de la semaine**

  La tâche s'exécute régulièrement les jours définis de la semaine, à l'heure indiquée.

  Par défaut, la tâche s'exécute chaque vendredi à 18h00.

- **Chaque mois**

  La tâche s'exécute régulièrement le jour du mois défini, à l'heure indiquée.

  Si le jour en question ne figure pas dans le mois, la tâche s'exécute le dernier jour.

  La tâche s'exécute par défaut le premier jour de chaque mois, à l'heure système actuelle.

- **Manuel**

  La tâche ne s'exécute pas automatiquement. Vous pouvez uniquement la lancer manuellement.

  Cette option est sélectionnée par défaut.

- **Chaque mois, les jours indiqués des semaines sélectionnées**

  La tâche s'exécute régulièrement les jours du mois définis, à l'heure indiquée.

  Par défaut, aucun jour du mois n'est sélectionné. L'heure de début par défaut est 18:00.

- **Lors du téléchargement des mises à jour dans le stockage**

  La tâche s'exécute après le téléchargement des mises à jour dans le stockage. Par exemple, vous pouvez utiliser cette programmation pour rechercher les vulnérabilités et les mises à jour requises.

- **Lors de la détection d'une attaque de virus**

  La tâche s'exécute après un événement *Attaque de virus* de virus. Sélectionnez les types d'application qui vont surveiller les propagations de virus. Les types suivants de Application sont présent :

  - Antivirus pour postes de travail et serveurs de fichiers
  - Antivirus de protection du périmètre
  - Antivirus pour systèmes de messagerie

  Tous les types d'application sont cochés par défaut.

  Il se peut que vous souhaitiez exécuter différentes tâches en fonction du type d'application de sécurité qui signale une propagation de virus. Dans ce cas, supprimez la sélection des types d'application dont vous n'avez pas besoin.

- **Après l'exécution d'une autre tâche**

La tâche actuelle démarre à la fin d'une autre tâche. Cette option ne fonctionne que si les deux tâches sont affectées aux mêmes appareils. Par exemple, vous pouvez exécuter la tâche *Administration des appareils* avec l'option **&Activer l'appareil** et, une fois celle-ci terminée, exécuter la tâche de *recherche de virus* comme tâche de déclenchement.

Il faut sélectionner la tâche de déclenchement dans le tableau et l'état avec lequel cette tâche doit se terminer (**Terminée avec succès** ou **Échec**).

Si nécessaire, vous pouvez rechercher, trier et filtrer les tâches dans le tableau comme suit :

- Saisissez le nom de la tâche dans le champ de recherche pour rechercher une tâche par son nom.
- Cliquez sur l'icône de tri pour trier les tâches par nom.

  Par défaut, les tâches sont triées par ordre alphabétique croissant.
- Cliquez sur l'icône du filtre, et dans la fenêtre qui s'ouvre, filtrez les tâches par groupe, puis cliquez sur le bouton **Appliquer**.

- **Lancer les tâches non exécutées**

  Cette option détermine le comportement d'une tâche si un appareil client n'est pas visible sur le réseau quand la tâche est sur le point de démarrer.

  Si la case est Activé, lors du lancement suivant de l'application de Kaspersky sur cet appareil client, une tentative de lancement de la tâche sera faite. Si la programmation de la tâche est **Manuel**, **Une fois** ou **Immédiatement**, la tâche est immédiatement lancée dès que l'appareil apparaît sur le réseau ou immédiatement après l'inclusion de l'appareil dans la zone d'action de la tâche.

  Si cette option est désactivée, seules les tâches planifiées s'exécutent sur les appareils clients. Pour les planifications **Manuel**, **Une fois** et **Immédiatement**, les tâches s'exécutent uniquement sur les appareils clients qui sont visibles sur le réseau. Par exemple, vous pouvez désactiver cette option pour une tâche qui consomme des ressources que vous voulez exécuter uniquement en dehors des heures de bureau.

  Cette option est Inactif par défaut.

- **Adopter un décalage aléatoire automatique pour les lancements de tâche**

  Si cette option est activée, la tâche est lancée sur les appareils clients de manière aléatoire au cours d'un intervalle défini. C'est ce qu'on appelle un *lancement échelonné d'une tâche*. Un lancement échelonné de tâche permet d'éviter la communication simultanée d'un nombre important d'appareils clients avec le Serveur d'administration lors du lancement de la tâche programmée.

  Le temps du lancement aléatoire est automatiquement calculée lors de la création d'une tâche selon le nombre d'appareils clients sur lesquels la tâche est diffusée. Par la suite, la tâche démarre toujours à l'heure de lancement calculée. Toutefois, quand les paramètres de la tâche sont modifiés ou si la tâche est lancée manuellement, la valeur calculée de l'heure de lancement de la tâche est modifiée.

  Si la case n'est pas cochée, le lancement de la tâche sur les appareils clients s'opère selon la planification.

- **Décaler aléatoirement le lancement de la tâche dans un intervalle de (min.)**

Si cette option est activée, la tâche est lancée sur les appareils clients de manière aléatoire au cours de l'intervalle défini. Un lancement échelonné de tâche permet d'éviter la communication simultanée d'un nombre important d'appareils clients avec le Serveur d'administration lors du lancement de la tâche programmée.

Si la case n'est pas cochée, le lancement de la tâche sur les appareils clients s'opère selon la planification.

Cette option est Inactif par défaut. Par défaut, la valeur de cet intervalle est de une minute.

6. La page **Définition du nom de la tâche** de l'Assistant permet de renseigner le nom de la tâche en cours de création. Le nom de la tâche ne peut pas contenir plus de 100 symboles et contenir de symboles spéciaux ("*<>?\:|).

7. Sur la page **Fin de la création de la tâche** de l'Assistant, cliquez sur le bouton **Terminer** pour quitter l'Assistant.

   Si vous souhaitez que la tâche démarre directement à la fin de l'Assistant, cochez la case **&Lancer la tâche à la fin de l'Assistant**.

Une fois que l'Assistant a terminé son opération, la tâche **Recherche de vulnérabilités et de mises à jour requises** apparaît dans la liste des tâches dans le dossier **Appareils administrés**, sous l'onglet **Tâches**.

En plus des paramètres que vous définissez lors de la création de la tâche, vous pouvez modifier d'autres propriétés de la tâche créée.

À la suite de l'exécution de la tâche *Recherche de vulnérabilités et de mises à jour requises*, le Serveur d'administration affiche une liste des vulnérabilités détectées dans les applications installées sur l'appareil et des mises à jour logicielles indispensables pour éliminer les vulnérabilités détectées.

Si l'erreur 0x80240033 « Erreur de l'agent de mise à jour Windows 80240033 (« Les conditions de licence n'ont pas pu être téléchargées ») » s'affiche, vous pouvez résoudre ce problème via le registre Windows.

Le Serveur d'administration n'affiche pas la liste des mises à jour logicielles requises lorsque vous effectuez deux tâches de manière séquentielle : la tâche *Synchronisation des mises à jour Windows Update* pour laquelle l'option **Télécharger les mises à jour rapides** est désactivée, puis la tâche *Recherche de vulnérabilités et de mises à jour requises*. Afin d'afficher la liste des mises à jour logicielles requises, vous devez réexécuter la tâche *Recherche de vulnérabilités et de mises à jour requises*.

L'Agent d'administration reçoit les informations relatives aux mises à jour Windows et d'autres produits de Microsoft disponibles depuis Windows Update ou depuis le Serveur d'administration, si le Serveur d'administration est utilisé comme serveur WSUS. Les informations sont transmises au moment du lancement des applications (si c'est configuré dans la stratégie) et du lancement périodique de la tâche *Recherche de vulnérabilités et de mises à jour requises* sur les appareils clients.

Correction des vulnérabilités dans les applications

Si vous avez sélectionné **Rechercher et installer les mises à jour requises** sur la page **Paramètres d'administration des mises à jour** de l'Assistant de configuration initiale de l'application, la tâche *Installation des mises à jour requises et correction des vulnérabilités* est automatiquement créée. La tâche s'affiche dans l'espace de travail du dossier **Appareils administrés** sous l'onglet **Tâches**.

Dans le cas contraire, vous pouvez réaliser une des opérations suivantes :

- Créez une tâche pour corriger les vulnérabilités en installant les mises à jour disponibles.
- Ajoutez une règle pour corriger une vulnérabilité à une tâche de correction de la vulnérabilité existante.

Une interaction utilisateur peut être requise lorsque vous mettez à jour une application tierce ou corrigez une vulnérabilité dans une application tierce sur un appareil administré. Par exemple, l'utilisateur peut être invité à fermer l'application tierce si elle est actuellement ouverte.

Correction d'une vulnérabilité via la création d'une tâche de correction de la vulnérabilité

Vous pouvez réaliser une des opérations suivantes :

- Créer une tâche pour corriger plusieurs vulnérabilités qui respectent certaines règles.
- Sélectionner une vulnérabilité et créer une tâche pour la corriger ainsi que d'autres vulnérabilités similaires.

Pour corriger des vulnérabilités qui respectent certaines règles :

1. Dans l'arborescence de la console, sélectionnez le Serveur d'administration sur les appareils pour lesquels vous voulez éliminer les vulnérabilités.
2. Dans le menu **Consulter** de la fenêtre principale de l'application, sélectionnez **&Configuration de l'interface**.
3. Dans la fenêtre qui s'ouvre, cochez la case **Afficher Gestion des vulnérabilités et des correctifs**, puis cliquez sur **OK**.
4. Dans la fenêtre contenant le message de l'application, cliquez sur **OK**.
5. Redémarrez la Console d'administration pour que les modifications prennent effet.
6. Dans l'arborescence de la console sélectionnez le dossier **Appareils administrés**.
7. Dans l'espace de travail, sélectionnez l'onglet **Tâches**.
8. Cliquez sur le bouton **Créer une tâche** pour lancer l'Assistant de création d'une tâche. Suivez les étapes de l'assistant.
9. Sur la page **Sélection du type de tâche** de l'Assistant, sélectionnez **Installation des mises à jour requises et correction des vulnérabilités**.

   Si la tâche ne s'affiche pas, vérifiez si votre compte dispose des privilèges **Lire**, **Modifier** et **Exécuter** pour la zone fonctionnelle **Administration du système** : **Gestion des vulnérabilités et des correctifs** Vous ne pouvez pas créer et configurer la tâche *Installation des mises à jour requises et correction des vulnérabilités* sans ces privilèges d'accès.

10. Sur la page **Paramètres** de l'Assistant, définissez les paramètres de la tâche comme suit :

- **Définissez les règles d'installation des mises à jour**

  Ces règles sont appliquées à l'installation des mises à jour sur les appareils clients. Si les règles ne sont pas définies, la tâche n'a rien à exécuter. Pour en savoir plus sur l'utilisation des règles, consultez le point Règles pour l'installation de la mise à jour.

- **Commencer l'installation au moment du &redémarrage ou de l'arrêt de l'appareil**

  Si cette option est activée, les mises à jour sont installées lors du redémarrage ou de l'arrêt de l'appareil. Dans le cas contraire, les mises à jour sont installées selon la programmation.

  Utilisez cette option si l'installation des mises à jour peut avoir un impact sur les performances de l'appareil.

  Cette option est Inactif par défaut.

- **Installer les modules système général requis**

  Si cette option est activée, l'application, avant d'installer une mise à jour, installe automatiquement tous les composants généraux système (prérequis) requis pour l'installation de la mise à jour. Par exemple, il peut s'agir des mises à jour du système d'exploitation.

  Si cette option est désactivée, vous devrez peut-être installer les prérequis manuellement.

  Cette option est Inactif par défaut.

- **Autoriser l'&installation de la nouvelle version de l'application lors de la mise à jour**

  Si cette option est activée, les mises à jour sont autorisées lorsqu'elles entraînent l'installation d'une nouvelle version d'un logiciel.

  Si cette option est désactivée, le logiciel n'est pas mis à jour. Vous pouvez alors installer les nouvelles versions du logiciel manuellement ou via un autre tâche. Par exemple, vous pouvez utiliser cette option si l'infrastructure de votre entreprise n'est pas prise en charge par une nouvelle version du logiciel ou si vous souhaitez vérifier une mise à jour dans une infrastructure d'essai.

  Cette option est activée par défaut.

  La mise à jour d'une application peut provoquer un dysfonctionnement des applications dépendantes installées sur les appareils clients.

- **Télécharger les mises à jour sur l'appareil sans les &installer**

  Quand cette option est activée, l'application télécharge les mises à jour sur l'appareil, mais ne les installe pas automatiquement. Vous pouvez installer les mises à jour manuellement par la suite.

  Les mises à jour Microsoft sont téléchargées dans le stockage Windows système. Les mises à jour des produits tiers (applications développées par des éditeurs d'application autres que Kaspersky et Microsoft) sont téléchargées dans le dossier indiqué dans le champ **Télécharger les mises à jour sur**.

  Si cette option est désactivée, les mises à jour sont installées automatiquement sur l'appareil.

  Cette option est Inactif par défaut.

- **Télécharger les mises à jour sur**

  Ce dossier est utilisé dans le cadre du téléchargement des mises à jour de produits tiers (applications développées par des éditeurs de logiciels autres que Kaspersky et Microsoft).

- **Activer le diagnostic avancé**

  Quand cette fonction est activée, l'Agent d'administration enregistre des fichiers de trace même si l'écriture de fichiers de trace est désactivée pour l'Agent d'administration dans l'utilitaire de diagnostic à distance Kaspersky Security Center. Les traces sont enregistrées dans deux fichiers en alternance la taille de chacun de ces fichiers est déterminée par la valeur paramètre **Taille maximale (Mo) des fichiers de diagnostic avancé**. Quand les deux fichiers sont remplis, l'Agent d'administration écrit à nouveau dans ceux-ci. Les fichiers avec les traces sont stockés dans le dossier %WINDIR%\Temp. Ces fichiers sont accessibles dans l'utilitaire de diagnostic à distance, vous pouvez les télécharger ou les supprimer à cet endroit.

  Quand cette fonction est désactivée, l'Agent d'administration enregistre les traces conformément aux paramètres définis dans l'utilitaire de diagnostic à distance Kaspersky Security Center. Aucune trace complémentaire n'est écrite.

  Lors de la création d'une tâche, il n'est pas nécessaire d'activer le diagnostic avancé. Par contre, vous pouvez activer cette fonction plus tard si, par exemple, une tâche échoue sur certains appareils et que vous souhaitez obtenir des informations complémentaires lors d'une autre exécution de la tâche.

  Cette option est Inactif par défaut.

- **Taille maximale (Mo) des fichiers de diagnostic avancé**

  La valeur par défaut est de 100 Mo, mais elle peut se situer entre 1 et 2 048 Mo. Il peut arriver qu'un expert du Support Technique de Kaspersky vous demande de modifier la valeur par défaut lorsque les informations reprises dans les fichiers de diagnostic avancés que vous avez envoyés ne suffisent pas pour résoudre le problème.

11. Sur la page **Sélection de l'option de redémarrage du système d'exploitation** de l'Assistant, sélectionnez l'action à réaliser lorsque le système d'exploitation sur les appareils clients doit redémarrer après l'opération :

- **Ne pas redémarrer l'appareil**

  Les appareils clients ne redémarrent pas automatiquement après l'opération. Pour arrêter le fonctionnement, il faut redémarrer l'appareil (par exemple, manuellement ou à l'aide d'une tâche d'administration des appareils). Les informations sur la nécessité du redémarrage sont enregistrées dans les résultats de la tâche et dans l'état de l'appareil. Cette option convient aux tâches d' sur les serveurs et autres appareils pour lesquels la continuité des opérations est critique.

- **Redémarrer l'appareil**

  Dans ce cas, le redémarrage des appareils clients est toujours exécuté automatiquement, si celui-ci est requis pour terminer l'opération. Cette option convient aux tâches d' sur des appareils pour lesquels des interruptions périodiques sont admises (débranchement, redémarrage).

- **Confirmer l'action auprès de l'utilisateur**

  Le message qui signale que l'appareil client doit être redémarré manuellement s'affiche sur l'écran de l'appareil. Pour cette option, il est possible de configurer des paramètres avancés : le texte du message pour l'utilisateur, la fréquence du message, ainsi que le délai à l'issue duquel le redémarrage sera forcé (sans confirmation de l'utilisateur). Cette option convient le mieux pour les postes de travail sur lesquels les utilisateurs doivent pouvoir sélectionner l'heure de redémarrage qui leur convient le mieux.

  Cette option est sélectionnée par défaut.

  - **Répéter la demande toutes les (min.)**

    Quand cette option est activée, l'application invite l'utilisateur à redémarrer le système d'exploitation selon la fréquence indiquée.

    Cette option est activée par défaut. L'intervalle par défaut est de 5 minutes. La valeur peut être comprise entre 1 et 1 440 minutes.

    Si cette option est désactivée, l'invite est affichée une seule fois.

  - **Redémarrer au bout de (min.)**

    Après avoir averti l'utilisateur, l'application force le redémarrage du système d'exploitation à l'issue de l'intervalle défini.

    Cette option est activée par défaut. Le délai par défaut est de 30 minutes. La valeur peut être comprise entre 1 et 1 440 minutes.

- **Forcer la fermeture des applications dans les sessions bloquées**

Les applications en cours d'exécution peuvent empêcher le redémarrage de l'appareil client. Par exemple, si un document est en train d'être modifié dans un logiciel de traitement de texte et qu'il n'est pas enregistré, l'application n'autorise pas le redémarrage de l'appareil.

Quand cette option est activée, l'arrêt forcé de ces applications sur un appareil verrouillé doit avoir lieu avant de pouvoir redémarrer l'appareil. Les utilisateurs pourraient perdre toute modification qui n'a pas été enregistrée à ce moment.

Si cette option est désactivée, un appareil verrouillé n'est pas redémarré. L'état de la tâche sur cet appareil indique qu'il faut redémarrer l'appareil. Les utilisateurs doivent quitter manuellement toutes les applications en cours d'exécution sur les appareils verrouillés, puis redémarrer ces appareils.

Cette option est Inactif par défaut.

12. La page **Planifier la tâche** de l'Assistant vous permet de programmer le lancement de la tâche. Le cas échéant, configurez les paramètres suivants :

- **Lancement planifié :**

  Sélectionnez la programmation de l'exécution de la tâche, puis configurez la programmation sélectionnée.

  - **Toutes les N heures**

    La tâche s'exécute régulièrement, selon l'intervalle défini en heures, à partir de la date et heure définis.

    La tâche s'exécute par défaut toutes les six heures à partir de la date et de l'heure actuelles du système.

  - **Tous les N jours**

    La tâche s'exécute régulièrement, selon l'intervalle défini en jours. En outre, vous pouvez spécifier la date et l'heure de la première exécution de la tâche. Ces options supplémentaires deviennent disponibles si elles sont prises en charge par l'application pour laquelle vous créez la tâche.

    La tâche s'exécute par défaut chaque jour, à partir de la date et de l'heure actuelle du système.

  - **Toutes les N semaines**

    La tâche s'exécute régulièrement, selon l'intervalle défini en semaines, le jour indiqué de la semaine et à l'heure indiquée.

    La tâche s'exécute par défaut chaque lundi à l'heure système actuelle.

  - **Toutes les N minutes**

    La tâche s'exécute régulièrement, à l'intervalle défini en minutes, à partir de l'heure indiquée le jour de la création de la tâche.

    La tâche s'exécute par défaut toutes les 30 minutes, à partir de l'heure actuelle du système.

  - **Chaque jour (passage à l'heure d'été non pris en charge)**

    La tâche s'exécute régulièrement, selon l'intervalle défini en jours. Cette programmation ne tient pas compte du passage à l'heure d'été. Cela signifie que lorsque les horloges sont avancées ou reculées d'une heure au début ou à la fin de l'été, l'heure de lancement réelle de la tâche ne change pas.

    Nous déconseillons d'adopter cette programmation. Elle est requise pour la rétrocompatibilité avec Kaspersky Security Center.

    La tâche démarre par défaut chaque jour à l'heure système actuelle.

  - **Chaque semaine**

    La tâche s'exécute chaque semaine, le jour défini et à l'heure indiquée.

- **Par jours de la semaine**

  La tâche s'exécute régulièrement les jours définis de la semaine, à l'heure indiquée.

  Par défaut, la tâche s'exécute chaque vendredi à 18h00.

- **Chaque mois**

  La tâche s'exécute régulièrement le jour du mois défini, à l'heure indiquée.

  Si le jour en question ne figure pas dans le mois, la tâche s'exécute le dernier jour.

  La tâche s'exécute par défaut le premier jour de chaque mois, à l'heure système actuelle.

- **Manuel**

  La tâche ne s'exécute pas automatiquement. Vous pouvez uniquement la lancer manuellement.

  Cette option est sélectionnée par défaut.

- **Chaque mois, les jours indiqués des semaines sélectionnées**

  La tâche s'exécute régulièrement les jours du mois définis, à l'heure indiquée.

  Par défaut, aucun jour du mois n'est sélectionné. L'heure de début par défaut est 18:00.

- **Lors de la détection d'une attaque de virus**

  La tâche s'exécute après un événement *Attaque de virus* de virus. Sélectionnez les types d'application qui vont surveiller les propagations de virus. Les types suivants de Application sont présent :

  - Antivirus pour postes de travail et serveurs de fichiers
  - Antivirus de protection du périmètre
  - Antivirus pour systèmes de messagerie

  Tous les types d'application sont cochés par défaut.

  Il se peut que vous souhaitiez exécuter différentes tâches en fonction du type d'application de sécurité qui signale une propagation de virus. Dans ce cas, supprimez la sélection des types d'application dont vous n'avez pas besoin.

- **Après l'exécution d'une autre tâche**

La tâche actuelle démarre à la fin d'une autre tâche. Cette option ne fonctionne que si les deux tâches sont affectées aux mêmes appareils. Par exemple, vous pouvez exécuter la tâche *Administration des appareils* avec l'option **&Activer l'appareil** et, une fois celle-ci terminée, exécuter la tâche de *recherche de virus* comme tâche de déclenchement.

Il faut sélectionner la tâche de déclenchement dans le tableau et l'état avec lequel cette tâche doit se terminer (**Terminée avec succès** ou **Échec**).

Si nécessaire, vous pouvez rechercher, trier et filtrer les tâches dans le tableau comme suit :

- Saisissez le nom de la tâche dans le champ de recherche pour rechercher une tâche par son nom.
- Cliquez sur l'icône de tri pour trier les tâches par nom.

  Par défaut, les tâches sont triées par ordre alphabétique croissant.
- Cliquez sur l'icône du filtre, et dans la fenêtre qui s'ouvre, filtrez les tâches par groupe, puis cliquez sur le bouton **Appliquer**.

- **Lancer les tâches non exécutées**

  Cette option détermine le comportement d'une tâche si un appareil client n'est pas visible sur le réseau quand la tâche est sur le point de démarrer.

  Si la case est Activé, lors du lancement suivant de l'application de Kaspersky sur cet appareil client, une tentative de lancement de la tâche sera faite. Si la programmation de la tâche est **Manuel**, **Une fois** ou **Immédiatement**, la tâche est immédiatement lancée dès que l'appareil apparaît sur le réseau ou immédiatement après l'inclusion de l'appareil dans la zone d'action de la tâche.

  Si cette option est désactivée, seules les tâches planifiées s'exécutent sur les appareils clients. Pour les planifications **Manuel**, **Une fois** et **Immédiatement**, les tâches s'exécutent uniquement sur les appareils clients qui sont visibles sur le réseau. Par exemple, vous pouvez désactiver cette option pour une tâche qui consomme des ressources que vous voulez exécuter uniquement en dehors des heures de bureau.

  Cette option est Inactif par défaut.

- **Adopter un décalage aléatoire automatique pour les lancements de tâche**

  Si cette option est activée, la tâche est lancée sur les appareils clients de manière aléatoire au cours d'un intervalle défini. C'est ce qu'on appelle un *lancement échelonné d'une tâche*. Un lancement échelonné de tâche permet d'éviter la communication simultanée d'un nombre important d'appareils clients avec le Serveur d'administration lors du lancement de la tâche programmée.

  Le temps du lancement aléatoire est automatiquement calculée lors de la création d'une tâche selon le nombre d'appareils clients sur lesquels la tâche est diffusée. Par la suite, la tâche démarre toujours à l'heure de lancement calculée. Toutefois, quand les paramètres de la tâche sont modifiés ou si la tâche est lancée manuellement, la valeur calculée de l'heure de lancement de la tâche est modifiée.

  Si la case n'est pas cochée, le lancement de la tâche sur les appareils clients s'opère selon la planification.

- **Décaler aléatoirement le lancement de la tâche dans un intervalle de (min.)**

Si cette option est activée, la tâche est lancée sur les appareils clients de manière aléatoire au cours de l'intervalle défini. Un lancement échelonné de tâche permet d'éviter la communication simultanée d'un nombre important d'appareils clients avec le Serveur d'administration lors du lancement de la tâche programmée.

Si la case n'est pas cochée, le lancement de la tâche sur les appareils clients s'opère selon la planification.

Cette option est Inactif par défaut. Par défaut, la valeur de cet intervalle est de une minute.

13. La page **Définition du nom de la tâche** de l'Assistant permet de renseigner le nom de la tâche en cours de création. Le nom de la tâche ne peut pas contenir plus de 100 symboles et contenir de symboles spéciaux ("*<>?\:|).

14. Sur la page **Fin de la création de la tâche** de l'Assistant, cliquez sur le bouton **Terminer** pour quitter l'Assistant.

    Si vous souhaitez que la tâche démarre directement à la fin de l'Assistant, cochez la case **&Lancer la tâche à la fin de l'Assistant**.

Une fois que l'Assistant a terminé son fonctionnement, la tâche **Installation des mises à jour requises et correction des vulnérabilités** est créée. Cette tâche s'affiche dans le dossier **Tâches**.

En plus des paramètres que vous définissez lors de la création de la tâche, vous pouvez modifier d'autres propriétés de la tâche créée.

Si les résultats de la tâche contiennent l'erreur 0x80240033 « Erreur de l'agent de mise à jour Windows 80240033 (« Les conditions de licence n'ont pas pu être téléchargées ») », vous pouvez résoudre ce problème via le registre Windows.

Pour corriger une vulnérabilité particulière et des vulnérabilités similaires :

1. Dans l'arborescence de la console, accédez au dossier **Avancé** → **Gestion des applications**, puis le sous-dossier **Vulnérabilités dans les applications**.

2. Choisissez la vulnérabilité que vous voulez corriger.

3. Cliquez sur le bouton **Lancer l'Assistant de correction des vulnérabilités**.

   L'Assistant de correction des vulnérabilités s'ouvre.

   La fonctionnalité de l'Assistant de correction des vulnérabilités est accessible en présence d'une licence pour le fonctionnement de Gestion des vulnérabilités et des correctifs.

   Suivez les étapes de l'assistant.

4. Dans la fenêtre **Recherche des tâches existantes de correction de la vulnérabilité**, définissez les paramètres suivants :

   - **Afficher uniquement les tâches corrigeant la vulnérabilité sélectionnée**

     Quand cette option est activée, l'Assistant de correction des vulnérabilités recherche les tâches existantes qui corrigent la vulnérabilité sélectionnée.

     Si cette option est désactivée ou si la recherche ne donne aucune tâche applicable, l'Assistant de correction des vulnérabilités vous demande de créer une règle ou une tâche pour corriger la vulnérabilité.

     Cette option est activée par défaut.

   - **Approuver les mises à jour qui corrigent la vulnérabilité sélectionnée**

     Les mises à jour qui corrigent une vulnérabilité seront approuvées pour l'installation. Activez cette option si certaines règles appliquées de l'installation de la mise à jour autorisent uniquement l'installation des mises à jour confirmées.

     Cette option est Inactif par défaut.

5. Si vous décidez de recherche des tâches existantes de correction de la vulnérabilité et si quelques tâches sont ainsi récupérées, vous pouvez consulter leurs propriétés ou les lancer manuellement. Il n'y a rien d'autre à faire.

   Sinon, cliquez sur le bouton **Nouvelle tâche de correction de la vulnérabilité**.

6. Sélectionnez le type de la règle de correction de la vulnérabilité à ajouter à la tâche sélectionnée, puis cliquez sur le bouton **Terminer**.

7. Faites votre choix dans l'invite qui s'affiche au sujet de l'installation de toutes les mise à jour de l'application antérieures. Cliquez sur **Oui** si vous acceptez d'installer les versions successives de l'application de manière incrémentielle si cela s'impose pour installer les mises à jour sélectionnées. Cliquez sur **Non** si vous souhaitez mettre à jour les applications de manière directe, sans installer les versions intermédiaires. S'il est impossible d'installer les mises à jour sélectionnées sans installer les versions antérieures de l'application, la mise à jour de l'application échoue.

   L'Assistant de création de la tâche d'installation des mises à jour et de correction des vulnérabilités démarre. Suivez les étapes de l'assistant.

8. Sur la page **Sélection de l'option de redémarrage du système d'exploitation** option de l'Assistant, sélectionnez l'action à réaliser lorsque le système d'exploitation sur les appareils clients doit redémarrer après l'opération :

- **Ne pas redémarrer l'appareil**

  Les appareils clients ne redémarrent pas automatiquement après l'opération. Pour arrêter le fonctionnement, il faut redémarrer l'appareil (par exemple, manuellement ou à l'aide d'une tâche d'administration des appareils). Les informations sur la nécessité du redémarrage sont enregistrées dans les résultats de la tâche et dans l'état de l'appareil. Cette option convient aux tâches d' sur les serveurs et autres appareils pour lesquels la continuité des opérations est critique.

- **Redémarrer l'appareil**

  Dans ce cas, le redémarrage des appareils clients est toujours exécuté automatiquement, si celui-ci est requis pour terminer l'opération. Cette option convient aux tâches d' sur des appareils pour lesquels des interruptions périodiques sont admises (débranchement, redémarrage).

- **Confirmer l'action auprès de l'utilisateur**

  Le message qui signale que l'appareil client doit être redémarré manuellement s'affiche sur l'écran de l'appareil. Pour cette option, il est possible de configurer des paramètres avancés : le texte du message pour l'utilisateur, la fréquence du message, ainsi que le délai à l'issue duquel le redémarrage sera forcé (sans confirmation de l'utilisateur). Cette option convient le mieux pour les postes de travail sur lesquels les utilisateurs doivent pouvoir sélectionner l'heure de redémarrage qui leur convient le mieux.

  Cette option est sélectionnée par défaut.

  - **Répéter la demande toutes les (min.)**

    Quand cette option est activée, l'application invite l'utilisateur à redémarrer le système d'exploitation selon la fréquence indiquée.

    Cette option est activée par défaut. L'intervalle par défaut est de 5 minutes. La valeur peut être comprise entre 1 et 1 440 minutes.

    Si cette option est désactivée, l'invite est affichée une seule fois.

  - **Redémarrer au bout de (min.)**

    Après avoir averti l'utilisateur, l'application force le redémarrage du système d'exploitation à l'issue de l'intervalle défini.

    Cette option est activée par défaut. Le délai par défaut est de 30 minutes. La valeur peut être comprise entre 1 et 1 440 minutes.

- **Forcer la fermeture des applications dans les sessions bloquées**

Les applications en cours d'exécution peuvent empêcher le redémarrage de l'appareil client. Par exemple, si un document est en train d'être modifié dans un logiciel de traitement de texte et qu'il n'est pas enregistré, l'application n'autorise pas le redémarrage de l'appareil.

Quand cette option est activée, l'arrêt forcé de ces applications sur un appareil verrouillé doit avoir lieu avant de pouvoir redémarrer l'appareil. Les utilisateurs pourraient perdre toute modification qui n'a pas été enregistrée à ce moment.

Si cette option est désactivée, un appareil verrouillé n'est pas redémarré. L'état de la tâche sur cet appareil indique qu'il faut redémarrer l'appareil. Les utilisateurs doivent quitter manuellement toutes les applications en cours d'exécution sur les appareils verrouillés, puis redémarrer ces appareils.

Cette option est Inactif par défaut.

9. Sur la page **Sélectionnez les appareils auxquels la tâche sera affectée** de l'Assistant, sélectionnez l'une des options suivantes :

- Sélectionner les appareils détectés sur le réseau par le Serveur d'administration

  la tâche est affectée à un ensemble d'appareils. L'ensemble d'appareils peut reprendre aussi bien des appareils de groupes d'administration que des appareils non définis.

  Par exemple, vous pourriez utiliser cette option dans une tâche d'installation d'un Agent d'administration sur des appareils non définis.

- Définir les adresses des appareils manuellement ou les importer à partir d'une liste

  Vous pouvez définir les noms NetBIOS, les noms DNS, les adresses IP, ainsi que les plages d'adresses IP auxquels il convient d'affecter la tâche.

  Vous pourriez utiliser cette option pour exécuter une tâche pour un sous-réseau défini. Par exemple, vous pourriez souhaiter installer une certaine application sur les appareils des comptables ou analyser des appareils dans un sous-réseau qui est probablement infecté.

- Attribuer la tâche à une sélection d'appareils

  La tâche est affectée aux appareils qui appartiennent à une sélection d'appareils. Vous pouvez définir une des sélections existantes.

  Par exemple, vous pourriez souhaiter utiliser cette option pour exécuter une tâche sur des appareils dotés d'une version du système d'exploitation spécifique.

- Attribuer la tâche à un groupe d'administration

  La tâche est affectée aux appareils qui appartiennent à un groupe d'administration. Vous pouvez renseigner un des groupes existants ou en créer un.

  Par exemple, vous pourriez souhaiter utiliser cette option pour exécuter une tâche d'envoi de messages pour les utilisateurs si le message est particulier pour les appareils repris dans un groupe d'administration spécifique.

  Si une tâche est attribuée à un groupe d'administration, l'onglet **Sécurité** ne s'affiche pas dans la fenêtre des propriétés de la tâche, car les tâches de groupe sont soumises aux paramètres de sécurité des groupes auxquels elles s'appliquent.

10. La page **Planifier la tâche** de l'Assistant vous permet de programmer le lancement de la tâche. Le cas échéant, configurez les paramètres suivants :

- **Lancement planifié :**

  Sélectionnez la programmation de l'exécution de la tâche, puis configurez la programmation sélectionnée.

  - **Toutes les N heures**

    La tâche s'exécute régulièrement, selon l'intervalle défini en heures, à partir de la date et heure définis.

    La tâche s'exécute par défaut toutes les six heures à partir de la date et de l'heure actuelles du système.

  - **Tous les N jours**

    La tâche s'exécute régulièrement, selon l'intervalle défini en jours. En outre, vous pouvez spécifier la date et l'heure de la première exécution de la tâche. Ces options supplémentaires deviennent disponibles si elles sont prises en charge par l'application pour laquelle vous créez la tâche.

    La tâche s'exécute par défaut chaque jour, à partir de la date et de l'heure actuelle du système.

  - **Toutes les N semaines**

    La tâche s'exécute régulièrement, selon l'intervalle défini en semaines, le jour indiqué de la semaine et à l'heure indiquée.

    La tâche s'exécute par défaut chaque lundi à l'heure système actuelle.

  - **Toutes les N minutes**

    La tâche s'exécute régulièrement, à l'intervalle défini en minutes, à partir de l'heure indiquée le jour de la création de la tâche.

    La tâche s'exécute par défaut toutes les 30 minutes, à partir de l'heure actuelle du système.

  - **Chaque jour (passage à l'heure d'été non pris en charge)**

    La tâche s'exécute régulièrement, selon l'intervalle défini en jours. Cette programmation ne tient pas compte du passage à l'heure d'été. Cela signifie que lorsque les horloges sont avancées ou reculées d'une heure au début ou à la fin de l'été, l'heure de lancement réelle de la tâche ne change pas.

    Nous déconseillons d'adopter cette programmation. Elle est requise pour la rétrocompatibilité avec Kaspersky Security Center.

    La tâche démarre par défaut chaque jour à l'heure système actuelle.

  - **Chaque semaine**

    La tâche s'exécute chaque semaine, le jour défini et à l'heure indiquée.

- **Par jours de la semaine**

  La tâche s'exécute régulièrement les jours définis de la semaine, à l'heure indiquée.

  Par défaut, la tâche s'exécute chaque vendredi à 18h00.

- **Chaque mois**

  La tâche s'exécute régulièrement le jour du mois défini, à l'heure indiquée.

  Si le jour en question ne figure pas dans le mois, la tâche s'exécute le dernier jour.

  La tâche s'exécute par défaut le premier jour de chaque mois, à l'heure système actuelle.

- **Manuel**

  La tâche ne s'exécute pas automatiquement. Vous pouvez uniquement la lancer manuellement.

  Cette option est sélectionnée par défaut.

- **Chaque mois, les jours indiqués des semaines sélectionnées**

  La tâche s'exécute régulièrement les jours du mois définis, à l'heure indiquée.

  Par défaut, aucun jour du mois n'est sélectionné. L'heure de début par défaut est 18:00.

- **Lors de la détection d'une attaque de virus**

  La tâche s'exécute après un événement *Attaque de virus* de virus. Sélectionnez les types d'application qui vont surveiller les propagations de virus. Les types suivants de Application sont présent :

  - Antivirus pour postes de travail et serveurs de fichiers
  - Antivirus de protection du périmètre
  - Antivirus pour systèmes de messagerie

  Tous les types d'application sont cochés par défaut.

  Il se peut que vous souhaitiez exécuter différentes tâches en fonction du type d'application de sécurité qui signale une propagation de virus. Dans ce cas, supprimez la sélection des types d'application dont vous n'avez pas besoin.

- **Après l'exécution d'une autre tâche**

La tâche actuelle démarre à la fin d'une autre tâche. Cette option ne fonctionne que si les deux tâches sont affectées aux mêmes appareils. Par exemple, vous pouvez exécuter la tâche *Administration des appareils* avec l'option **&Activer l'appareil** et, une fois celle-ci terminée, exécuter la tâche de *recherche de virus* comme tâche de déclenchement.

Il faut sélectionner la tâche de déclenchement dans le tableau et l'état avec lequel cette tâche doit se terminer (**Terminée avec succès** ou **Échec**).

Si nécessaire, vous pouvez rechercher, trier et filtrer les tâches dans le tableau comme suit :

- Saisissez le nom de la tâche dans le champ de recherche pour rechercher une tâche par son nom.
- Cliquez sur l'icône de tri pour trier les tâches par nom.

  Par défaut, les tâches sont triées par ordre alphabétique croissant.
- Cliquez sur l'icône du filtre, et dans la fenêtre qui s'ouvre, filtrez les tâches par groupe, puis cliquez sur le bouton **Appliquer**.

- **Lancer les tâches non exécutées**

  Cette option détermine le comportement d'une tâche si un appareil client n'est pas visible sur le réseau quand la tâche est sur le point de démarrer.

  Si la case est Activé, lors du lancement suivant de l'application de Kaspersky sur cet appareil client, une tentative de lancement de la tâche sera faite. Si la programmation de la tâche est **Manuel**, **Une fois** ou **Immédiatement**, la tâche est immédiatement lancée dès que l'appareil apparaît sur le réseau ou immédiatement après l'inclusion de l'appareil dans la zone d'action de la tâche.

  Si cette option est désactivée, seules les tâches planifiées s'exécutent sur les appareils clients. Pour les planifications **Manuel**, **Une fois** et **Immédiatement**, les tâches s'exécutent uniquement sur les appareils clients qui sont visibles sur le réseau. Par exemple, vous pouvez désactiver cette option pour une tâche qui consomme des ressources que vous voulez exécuter uniquement en dehors des heures de bureau.

  Cette option est Inactif par défaut.

- **Adopter un décalage aléatoire automatique pour les lancements de tâche**

  Si cette option est activée, la tâche est lancée sur les appareils clients de manière aléatoire au cours d'un intervalle défini. C'est ce qu'on appelle un *lancement échelonné d'une tâche*. Un lancement échelonné de tâche permet d'éviter la communication simultanée d'un nombre important d'appareils clients avec le Serveur d'administration lors du lancement de la tâche programmée.

  Le temps du lancement aléatoire est automatiquement calculée lors de la création d'une tâche selon le nombre d'appareils clients sur lesquels la tâche est diffusée. Par la suite, la tâche démarre toujours à l'heure de lancement calculée. Toutefois, quand les paramètres de la tâche sont modifiés ou si la tâche est lancée manuellement, la valeur calculée de l'heure de lancement de la tâche est modifiée.

  Si la case n'est pas cochée, le lancement de la tâche sur les appareils clients s'opère selon la planification.

- **Décaler aléatoirement le lancement de la tâche dans un intervalle de (min.)**

Si cette option est activée, la tâche est lancée sur les appareils clients de manière aléatoire au cours de l'intervalle défini. Un lancement échelonné de tâche permet d'éviter la communication simultanée d'un nombre important d'appareils clients avec le Serveur d'administration lors du lancement de la tâche programmée.

Si la case n'est pas cochée, le lancement de la tâche sur les appareils clients s'opère selon la planification.

Cette option est Inactif par défaut. Par défaut, la valeur de cet intervalle est de une minute.

11. La page **Définition du nom de la tâche** de l'Assistant permet de renseigner le nom de la tâche en cours de création. Le nom de la tâche ne peut pas contenir plus de 100 symboles et contenir de symboles spéciaux ("*<>?\:|).

12. Sur la page **Fin de la création de la tâche** de l'Assistant, cliquez sur le bouton **Terminer** pour quitter l'Assistant.

    Si vous souhaitez que la tâche démarre directement à la fin de l'Assistant, cochez la case **&Lancer la tâche à la fin de l'Assistant**.

Quand l'Assistant a terminé, la tâche **Installation des mises à jour requises et correction des vulnérabilités** est créée. Cette tâche s'affiche dans le dossier **Tâches**.

En plus des paramètres que vous définissez lors de la création de la tâche, vous pouvez modifier d'autres propriétés de la tâche créée.

Correction d'une vulnérabilité via l'ajout d'une règle à une tâche de correction de la vulnérabilité existante

Pour corriger une vulnérabilité via l'ajout d'une règle à une tâche de correction de la vulnérabilité existante

1. Dans l'arborescence de la console, accédez au dossier **Avancé** → **Gestion des applications**, puis le sous-dossier **Vulnérabilités dans les applications**.

2. Choisissez la vulnérabilité que vous voulez corriger.

3. Cliquez sur le bouton **Lancer l'Assistant de correction des vulnérabilités**.

   L'Assistant de correction des vulnérabilités s'ouvre.

   La fonctionnalité de l'Assistant de correction des vulnérabilités est accessible en présence d'une licence pour le fonctionnement de Gestion des vulnérabilités et des correctifs.

   Suivez les étapes de l'assistant.

4. Dans la fenêtre **Recherche des tâches existantes de correction de la vulnérabilité**, définissez les paramètres suivants :

   - **Afficher uniquement les tâches corrigeant la vulnérabilité sélectionnée**

     Quand cette option est activée, l'Assistant de correction des vulnérabilités recherche les tâches existantes qui corrigent la vulnérabilité sélectionnée.

     Si cette option est désactivée ou si la recherche ne donne aucune tâche applicable, l'Assistant de correction des vulnérabilités vous demande de créer une règle ou une tâche pour corriger la vulnérabilité.

     Cette option est activée par défaut.

   - **Approuver les mises à jour qui corrigent la vulnérabilité sélectionnée**

     Les mises à jour qui corrigent une vulnérabilité seront approuvées pour l'installation. Activez cette option si certaines règles appliquées de l'installation de la mise à jour autorisent uniquement l'installation des mises à jour confirmées.

     Cette option est Inactif par défaut.

5. Si vous décidez de recherche des tâches existantes de correction de la vulnérabilité et si quelques tâches sont ainsi récupérées, vous pouvez consulter leurs propriétés ou les lancer manuellement. Il n'y a rien d'autre à faire.

   Dans le cas contraire, cliquez sur le bouton **Ajouter une règle de correction de la vulnérabilité à la tâche existante**.

6. Sélectionnez la tâche à laquelle vous souhaitez ajouter une règle, puis cliquez sur le bouton **Ajouter une règle**.

   Vous pouvez également consulter les propriétés des tâches existantes, les lancer manuellement ou créer une tâche.

7. Sélectionnez le type de règle à ajouter à la tâche sélectionnée, puis cliquez sur le bouton **Terminer**.

8. Faites votre choix dans l'invite qui s'affiche au sujet de l'installation de toutes les mise à jour de l'application antérieures. Cliquez sur **Oui** si vous acceptez d'installer les versions successives de l'application de manière incrémentielle si cela s'impose pour installer les mises à jour sélectionnées. Cliquez sur **Non** si vous souhaitez mettre à jour les applications de manière directe, sans installer les versions intermédiaires. S'il est impossible d'installer les mises à jour sélectionnées sans installer les versions antérieures de l'application, la mise à jour de l'application échoue.

Une nouvelle règle pour la correction de la vulnérabilité est ajoutée à la tâche **Installation des mises à jour requises et correction des vulnérabilités** existante.

Correction des vulnérabilités dans un réseau isolé

Cette section décrit les étapes que vous pouvez suivre pour corriger les vulnérabilités des logiciels tiers sur les appareils administrés connectés à des Serveurs d'administration sans accès à Internet.

Scénario : Correction des vulnérabilités des logiciels tiers dans un réseau isolé

Vous pouvez installer des mises à jour et corriger les vulnérabilités des logiciels tiers installés sur les appareils administrés dans un réseau isolé. De tels réseaux incluent les Serveurs d'administration et les appareils administrés qui y sont connectés et qui n'ont pas accès à Internet. Pour corriger les vulnérabilités d'un tel réseau, vous avez besoin d'un Serveur d'administration connecté à Internet. Ensuite, vous pourrez télécharger des correctifs (mises à jour nécessaires) en utilisant le Serveur d'administration avec accès à Internet et transmettre les correctifs à des Serveurs d'administration isolés.

Vous pouvez télécharger les mises à jour logicielles tierces émises par les éditeurs de logiciels, mais vous ne pouvez pas télécharger les mises à jour des logiciels Microsoft sur les Serveurs d'administration isolés à l'aide de Kaspersky Security Center.

Pour savoir comment fonctionne le processus de correction des vulnérabilités dans un réseau isolé, consultez la description et le schéma de ce processus.

Prérequis

Avant de commencer, procédez comme suit :

1. Attribuez un appareil pour la connexion à Internet et le téléchargement des correctifs. Cet appareil sera considéré comme le Serveur d'administration avec accès à Internet.
2. Installez Kaspersky Security Center, au plus tôt de version 14, sur les appareils suivants :
   - Appareil alloué, qui agira comme Serveur d'administration avec accès à Internet
   - Appareils isolés, qui agiront comme Serveurs d'administration isolés d'Internet (ci-après dénommés Serveurs d'administration isolés)
3. Assurez-vous que chaque Serveur d'administration dispose suffisamment d'espace disque pour télécharger et stocker les mises à jour et les correctifs.

Étapes

L'installation des mises à jour et la correction des vulnérabilités des logiciels tiers sur les appareils administrés des Serveurs d'administration isolés comprennent les étapes suivantes :

1. **Configuration du Serveur d'administration avec accès à Internet**

   Préparez votre Serveur d'administration avec un accès à Internet pour administrer les demandes de mises à jour logicielles tierces requises et pour télécharger les correctifs.

2. **Configuration des Serveurs d'administration isolés**

   Préparez vos Serveurs d'administration isolés afin qu'ils puissent former régulièrement des listes de mises à jour requises et administrer les correctifs téléchargés par le Serveur d'administration avec accès à Internet. Après la configuration, les Serveurs d'administration isolés n'essayent plus de télécharger les correctifs depuis Internet. Au lieu de cela, ils obtiennent des mises à jour via des correctifs.

3. **Transmission des correctifs et installation des mises à jour sur des Serveurs d'administration isolés**

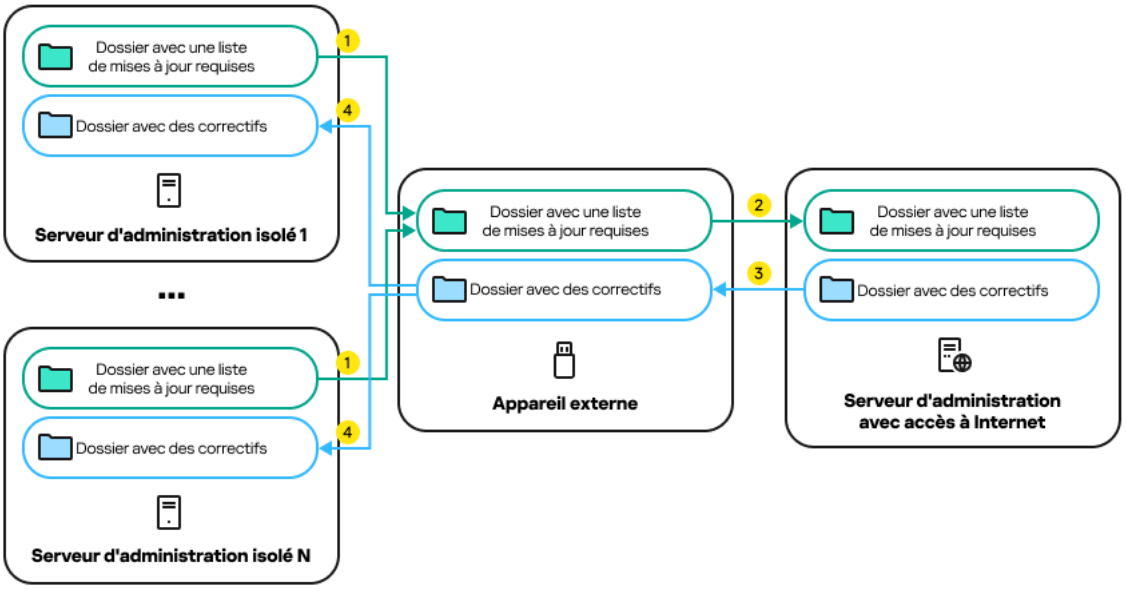
Une fois la configuration des Serveurs d'administration terminée, vous pouvez transmettre les listes de mises à jour et les correctifs requis entre le Serveur d'administration avec accès à Internet et les Serveurs d'administration isolés. Ensuite, les mises à jour des correctifs seront installées sur les appareils administrés à l'aide de la tâche *Installation des mises à jour requises et correction des vulnérabilités*.

Résultats

Ainsi, les mises à jour des logiciels tiers sont transmises aux Serveurs d'administration isolés et installées sur les appareils administrés connectés à l'aide de Kaspersky Security Center. Il suffit de configurer les Serveurs d'administration une fois, et après cela, vous pouvez obtenir des mises à jour aussi souvent que nécessaire, par exemple une ou plusieurs fois par jour.

À propos de la correction des vulnérabilités des logiciels tiers dans un réseau isolé

Le processus de correction des vulnérabilités des logiciels tiers dans un réseau isolé est illustré dans la figure et décrit ci-dessous. Vous pouvez répéter ce processus périodiquement.



Le processus de transmission des correctifs et la liste des mises à jour nécessaires entre le Serveur d'administration avec accès à Internet et les Serveurs d'administration isolés

Chaque Serveur d'administration isolé d'Internet (ci-après dénommé Serveur d'administration isolé) génère une liste des mises à jour qui doivent être installées sur les appareils administrés connectés à ce Serveur d'administration. La liste des mises à jour requises est stockée dans un dossier spécifique et présente un ensemble de fichiers binaires. Chaque fichier a un nom qui contient l'ID du correctif avec la mise à jour requise. Par conséquent, chaque fichier de la liste pointe vers un correctif spécifique.

En utilisant un appareil externe, vous transférez la liste des mises à jour nécessaires du Serveur d'administration isolé vers le Serveur d'administration attribué avec accès à Internet. Ensuite, le Serveur d'administration alloué télécharge les correctifs depuis Internet et les place dans un dossier séparé.

Lorsque tous les correctifs sont téléchargés et placés dans le dossier spécial qui leur est destiné, vous déplacez les correctifs vers chaque Serveur d'administration isolé à partir duquel vous avez extrait une liste des mises à jour requises. Vous enregistrez les correctifs dans le dossier créé spécialement pour eux sur le Serveur d'administration isolé. Par conséquent, la tâche *Installation des mises à jour requises et correction des vulnérabilités* exécute les correctifs et installe les mises à jour sur les appareils administrés des Serveurs d'administration isolés.

Configuration du Serveur d'administration avec accès à Internet pour corriger les vulnérabilités dans un réseau isolé

Pour préparer la correction des vulnérabilités et la transmission des correctifs dans un réseau isolé, configurez d'abord le Serveur d'administration avec un accès à Internet, puis configurer des Serveurs d'administration isolés.

Pour configurer le Serveur d'administration avec accès à Internet :

1. Créez deux dossiers sur un disque où le Serveur d'administration est installé :

   - Dossier pour la liste des mises à jour requises
   - Dossier pour les correctifs

   Vous pouvez nommer ces dossiers comme vous souhaitez.

2. Accordez les droits d'accès à la modification au groupe KLAdmins dans les dossiers créés, en utilisant les outils d'administration standard du système d'exploitation.

3. Utilisez l'utilitaire klscflag pour écrire les chemins d'accès aux dossiers dans les propriétés du Serveur d'administration.

   Exécutez l'invite de commande Windows en utilisant les droits d'administrateur, puis remplacez votre répertoire actuel par celui contenant l'utilitaire klscflag. L'utilitaire klsclag se trouve dans le dossier dans lequel le Serveur d'administration est installé. Chemin d'installation par défaut est <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

4. Saisissez les commandes suivantes à l'invite de commande Windows :

   - Pour définir le chemin d'accès au dossier des correctifs :
     `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v "<path to the folder>"`
   - Pour définir le chemin d'accès au dossier pour la liste des mises à jour requises :
     `klscflag -fset -pv klserver -n VAPM_REQ_IMPORT_PATH -t s -v "<path to the folder>"`

   Exemple : `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v "C:\<dossier pour les correctifs>"`

5. Si nécessaire, utilisez l'utilitaire klscflag pour spécifier la fréquence à laquelle le Serveur d'administration doit vérifier les nouvelles demandes de correctif :
   `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PERIOD_SEC -t d -v <valeur en secondes>`

   La valeur par défaut est égale à 120 secondes.

   Exemple : `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PERIOD_SEC -t d -v 150`

6. Créez la tâche *Recherche de vulnérabilités et de mises à jour requises* pour obtenir des informations sur les correctifs des logiciels tiers installés sur les appareils administrés, puis définissez la planification de la tâche.

7. Créez la tâche *Corriger les vulnérabilités* pour spécifier les correctifs pour les logiciels tiers utilisés pour corriger les vulnérabilités, puis définissez la planification de la tâche.

   Démarrez les tâches manuellement si vous souhaitez qu'elles s'exécutent plus tôt qu'il n'est spécifié dans la planification. L'ordre de lancement des tâches est important. La tâche *Corriger les vulnérabilités* doit être lancée après la tâche *Recherche de vulnérabilités et de mises à jour requises*.

8. Relancez le service du Serveur d'administration.

Le Serveur d'administration avec accès à Internet est maintenant prêt à télécharger et à transmettre les mises à jour aux Serveurs d'administration isolés. Avant de commencer à corriger les vulnérabilités, configurez des Serveurs d'administration isolés.

Configuration des Serveurs d'administration isolés pour corriger les vulnérabilités d'un réseau isolé

Après avoir terminé la configuration du Serveur d'administration avec accès à Internet, préparez chaque Serveur d'administration isolé de votre réseau afin de pouvoir corriger les vulnérabilités et installer les mises à jour sur les appareils administrés connectés à des Serveurs d'administration isolés.

Pour configurer des Serveurs d'administration isolés, réalisez les actions suivantes sur chaque Serveur d'administration :

1. Activez une clé de licence pour la fonction Gestion des vulnérabilités et des correctifs (VAPM).

2. Créez deux dossiers sur un disque où le Serveur d'administration est installé :

   - Dossier où apparaîtra la liste des mises à jour requises
   - Dossier pour les correctifs

   Vous pouvez nommer ces dossiers comme vous souhaitez.

3. Accordez les droits d'accès *Modifier* au groupe KLAdmins dans les dossiers créés, en utilisant les outils d'administration standard du système d'exploitation.

4. Utilisez l'utilitaire klscflag pour écrire les chemins d'accès aux dossiers dans les propriétés du Serveur d'administration.

   Exécutez l'invite de commande Windows en utilisant les droits d'administrateur, puis remplacez votre répertoire actuel par celui contenant l'utilitaire klscflag. L'utilitaire klsclag se trouve dans le dossier dans lequel le Serveur d'administration est installé. Chemin d'installation par défaut est <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

5. Saisissez les commandes suivantes à l'invite de commande Windows :

   - Pour définir le chemin d'accès au dossier des correctifs :
     `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v "<chemin d'accès au dossier>"`
   - Pour définir le chemin d'accès au dossier pour la liste des mises à jour requises :
     `klscflag -fset -pv klserver -n VAPM_REQ_EXPORT_PATH -t s -v "<chemin d'accès au dossier>"`

   Exemple : `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v "C:\<dossier pour les correctifs>"`

6. Si nécessaire, utilisez l'utilitaire klscflag pour spécifier la fréquence à laquelle le Serveur d'administration isolé doit rechercher de nouveaux correctifs :
   ```
   klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PERIOD_SEC -t d -v <valeur en secondes>
   ```
   La valeur par défaut est égale à 120 secondes.
   Exemple : `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PERIOD_SEC -t d -v 150`

7. Si nécessaire, utilisez l'utilitaire klscflag pour calculer les hachages SHA256 des correctifs :
   ```
   klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_VERIFY_HASH -t d -v 1
   ```
   Si vous saisissez cette commande, vous pouvez vous assurer que les correctifs n'ont pas été modifiés lors de leur transfert sur le Serveur d'administration isolé et que vous avez reçu les bons correctifs contenant les mises à jour requises.
   Par défaut, Kaspersky Security Center ne calcule pas les hachages SHA256 des correctifs. Si vous activez cette option, après la réception des correctifs par le Serveur d'administration isolé, Kaspersky Security Center calcule leurs hachages et compare les valeurs acquises avec les hachages stockés dans la base de données du Serveur d'administration. Si le hachage calculé ne correspond pas au hachage de la base de données, l'erreur se produit et vous devez remplacer les mauvais correctifs.

8. Créez la tâche *Recherche de vulnérabilités et de mises à jour requises* pour obtenir des informations sur les correctifs des logiciels tiers installés sur les appareils administrés, puis définissez la planification de la tâche.

9. Créez la tâche *Corriger les vulnérabilités* pour spécifier les correctifs pour les logiciels tiers utilisés pour corriger les vulnérabilités, puis définissez la planification de la tâche.
   Démarrez les tâches manuellement si vous souhaitez qu'elles s'exécutent plus tôt qu'il n'est spécifié dans la planification. L'ordre de lancement des tâches est important. La tâche *Corriger les vulnérabilités* doit être lancée après la tâche *Recherche de vulnérabilités et de mises à jour requises*.

10. Relancez le service du Serveur d'administration.

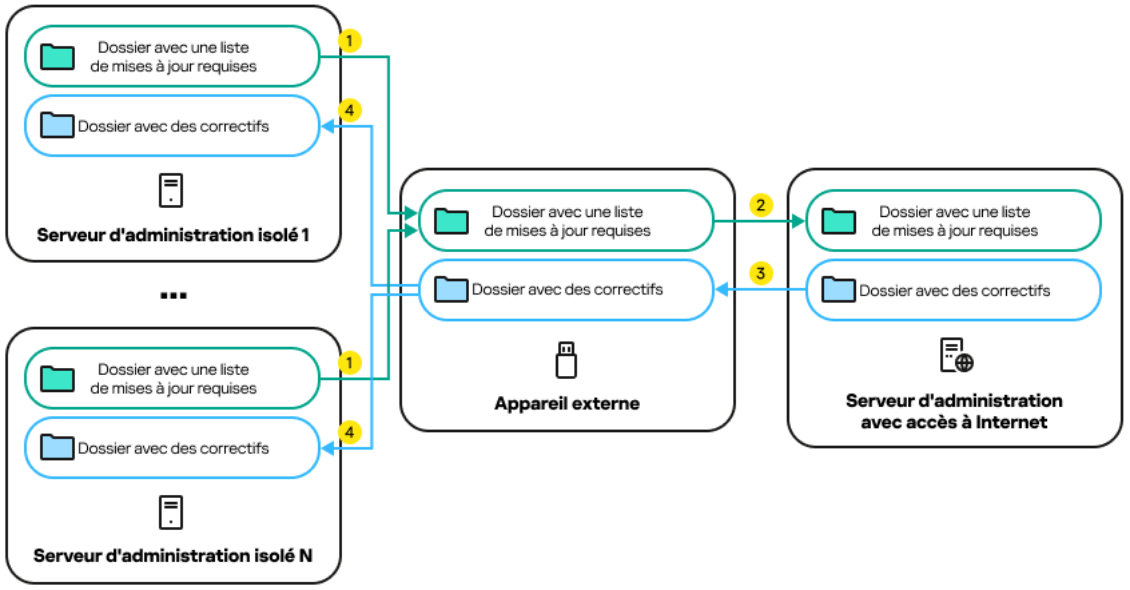
Après avoir configuré tous les Serveurs d'administration, vous pouvez déplacer les correctifs et les listes de mises à jour requises et corrigez les vulnérabilités des logiciels tiers sur les appareils administrés dans le réseau isolé.

Transmission des correctifs et installation des mises à jour dans un réseau isolé

Après avoir terminé la configuration des Serveurs d'administration, vous pouvez transférer des correctifs contenant les mises à jour nécessaires du Serveur d'administration avec accès à Internet vers des Serveurs d'administration isolés. Vous pouvez transmettre et installer des mises à jour aussi souvent que nécessaire, par exemple, une ou plusieurs fois par jour.

Vous avez besoin d'un appareil externe, tel qu'un lecteur amovible, pour transférer les correctifs et la liste des mises à jour nécessaires entre les Serveurs d'administration. Par conséquent, assurez-vous que l'appareil externe a suffisamment d'espace disque pour télécharger et stocker les correctifs.

Le processus de transmission des correctifs et la liste des mises à jour requises sont illustrés dans la figure et sont décrits ci-dessous :



Le processus de transmission des correctifs et la liste des mises à jour nécessaires entre le Serveur d'administration avec accès à Internet et les Serveurs d'administration isolés

Pour installer les mises à jour et corriger les vulnérabilités sur les appareils administrés connectés aux Serveurs d'administration isolés :

1. Lancez la tâche *Installation des mises à jour requises et correction des vulnérabilités* si elle n'est pas encore en cours d'exécution.

2. Connectez un appareil externe à n'importe quel Serveur d'administration isolé.

3. Créez deux dossiers sur l'appareil externe : un pour la liste des mises à jour requises et un pour les correctifs. Vous pouvez nommer ces dossiers comme vous souhaitez.

   Si vous avez créé ces dossiers précédemment, effacez-les.

4. Copiez la liste des mises à jour requises de chaque Serveur d'administration isolé et collez cette liste dans le dossier de la liste des mises à jour requises sur l'appareil externe.

   Ainsi, vous réunissez toutes les listes acquises de tous les Serveurs d'administration isolés dans un seul dossier. Par conséquent, ce dossier doit contenir des fichiers binaires avec les identifiants des correctifs requis pour tous les Serveurs d'administration isolés.

5. Connectez l'appareil externe au Serveur d'administration avec accès à Internet.

6. Copiez la liste des mises à jour requises à partir de l'appareil externe et collez cette liste dans le dossier de la liste des mises à jour requises sur le Serveur d'administration avec accès Internet.

   Tous les correctifs requis sont automatiquement téléchargés depuis Internet dans le dossier des correctifs sur le Serveur d'administration. Cela peut prendre plusieurs heures.

7. Assurez-vous que tous les correctifs requis sont téléchargés. Pour ce faire, vous pouvez effectuer une des actions suivantes :

   - Vérifiez le dossier des correctifs sur le Serveur d'administration avec accès à Internet. Tous les correctifs spécifiés dans la liste des mises à jour requises doivent être téléchargés dans un dossier nécessaire. Ceci est plus pratique si un petit nombre de correctifs est requis.

   - Préparez un script spécial, par exemple un script shell. Si vous obtenez un grand nombre de correctifs, il sera difficile de vérifier par vous-même que tous les correctifs ont été téléchargés. Dans de tels cas, il est préférable d'automatiser le contrôle.

8. Copiez les correctifs depuis le Serveur d'administration avec accès Internet et collez-les dans le dossier correspondant sur votre appareil externe.

9. Transférez les correctifs sur chaque Serveur d'administration isolé. Mettez les correctifs dans un dossier spécifique pour eux.

Par conséquent, chaque Serveur d'administration isolé crée une liste réelle des mises à jour qui sont nécessaires pour les appareils administrés connectés au Serveur d'administration actuel. Une fois que le Serveur d'administration avec accès à Internet a reçu la liste des mises à jour requises, le Serveur d'administration télécharge les correctifs depuis Internet. Lorsque ces correctifs apparaissent sur des Serveurs d'administration isolés, la tâche *Installation des mises à jour requises et correction des vulnérabilités* gère les correctifs. Ainsi, les mises à jour sont installées sur les appareils administrés et les vulnérabilités des logiciels tiers sont corrigées.

Lorsque la tâche *Installation des mises à jour requises et correction des vulnérabilités* est en cours d'exécution, ne redémarrez pas l'appareil du Serveur d'administration et n'exécutez pas la tâche *Sauvegarde des données du Serveur d'administration* (cela entraînera également un redémarrage). Par conséquent, la tâche *Installation des mises à jour requises et correction des vulnérabilités* est interrompue et les mises à jour ne sont pas installées. Dans ce cas, vous devez redémarrer cette tâche manuellement ou attendre que la tâche démarre selon la planification configurée.

Désactivation de la possibilité de transmettre les correctifs et d'installer les mises à jour dans un réseau isolé

Vous pouvez désactiver la transmission des correctifs sur des Serveurs d'administration isolés, par exemple, si vous avez décidé de retirer un ou plusieurs Serveurs d'administration d'un réseau isolé. Ainsi, vous pouvez réduire le nombre de correctifs et le temps nécessaire pour les télécharger.

Pour désactiver la possibilité de transmettre les correctifs sur des Serveurs d'administration isolés :

1. Si vous souhaitez sortir tous les Serveurs d'administration de l'isolement, supprimez dans les propriétés du Serveur d'administration avec accès à Internet les chemins d'accès aux dossiers des correctifs et la liste des mises à jour requises. Si vous souhaitez conserver certains Serveurs d'administration dans un réseau isolé, ignorez cette étape.

   Exécutez l'invite de commande Windows en utilisant les droits d'administrateur, puis remplacez votre répertoire actuel par celui contenant l'utilitaire klscflag. L'utilitaire klsclag se trouve dans le dossier dans lequel le Serveur d'administration est installé. Chemin d'installation par défaut est <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

   Saisissez les commandes suivantes à l'invite de commande :

   - Pour supprimer le chemin d'accès au dossier des correctifs :
     ```
     klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v ""
     ```
   - Pour supprimer le chemin d'accès au dossier pour une liste des mises à jour requises :
     ```
     klscflag -fset -pv klserver -n VAPM_REQ_IMPORT_PATH -t s -v ""
     ```

2. Redémarrez le service du Serveur d'administration si vous avez supprimé les chemins d'accès aux dossiers sur ce Serveur d'administration.

3. Dans les propriétés de chaque Serveur d'administration que vous souhaitez sortir de l'isolement, supprimez les chemins d'accès aux dossiers des correctifs et la liste des mises à jour requises.

   Saisissez les commandes suivantes à l'invite de commande Windows, en utilisant les droits d'administrateur :

   - Pour supprimer le chemin d'accès au dossier des correctifs :
     ```
     klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v ""
     ```
   - Pour supprimer le chemin d'accès au dossier pour une liste des mises à jour requises :
     ```
     klscflag -fset -pv klserver -n VAPM_REQ_EXPORT_PATH -t s -v ""
     ```

4. Redémarrez le service de chaque Serveur d'administration sur lequel vous avez supprimé les chemins d'accès aux dossiers.

Par conséquent, si vous avez reconfiguré le Serveur d'administration avec un accès à Internet, vous ne recevrez plus les correctifs via Kaspersky Security Center. Si vous n'avez reconfiguré que certains Serveurs d'administration isolés, par exemple, en retirant certains du réseau isolé, vous allez obtenir des correctifs uniquement pour les Serveurs d'administration isolés restants.

Si vous souhaitez commencer à corriger les vulnérabilités sur les Serveurs d'administration isolés désactivés à l'avenir, vous devez configurer ces Serveurs d'administration et le Serveur d'administration avec accès à internet encore une fois.

Ignorer les vulnérabilités dans les applications

Vous pouvez ignorer les vulnérabilités dans les applications à corriger. Par exemple, les raisons d'ignorer les vulnérabilités dans les applications peuvent être les suivantes :

- Vous ne considérez pas la vulnérabilité dans l'application comme critique pour votre entreprise.
- Vous savez que la correction de la vulnérabilité dans l'application peut endommager les données relatives au logiciel pour lequel la correction de la vulnérabilité était nécessaire.
- Vous êtes sûr que la vulnérabilité dans l'application n'est pas dangereuse pour le réseau de votre entreprise car vous utilisez d'autres mesures pour protéger vos appareils administrés.

Vous pouvez ignorer une vulnérabilité dans une application sur tous appareils administrés ou seulement sur les appareils administrés sélectionnés.

Pour ignorer une vulnérabilité logicielle sur tous les appareils administrés :

1. Dans l'arborescence de la console, accédez au dossier **Avancé** → **Gestion des applications**, puis le sous-dossier **Vulnérabilités dans les applications**.

   L'espace de travail du dossier affiche une liste des vulnérabilités dans les applications détectées sur les appareils par l'Agent d'administration installé sur ces appareils.

2. Choisissez la vulnérabilité à ignorer.

3. Dans le menu contextuel de la vulnérabilité, sélectionnez **Propriétés**.

   La fenêtre des propriétés de la vulnérabilité s'ouvre.

4. Dans la section **Général**, sélectionnez l'option **Ignorer la vulnérabilité**.

5. Cliquez sur le bouton **OK**.

   La fenêtre des propriétés de la vulnérabilité logicielle se ferme.

La vulnérabilité logicielle est ignorée sur les appareils administrés.

Pour ignorer une vulnérabilité logicielle sur l'appareil administré sélectionné :

1. Ouvrez la fenêtre des propriétés de l'appareil administré sélectionné, puis sélectionnez la section **Vulnérabilités dans les applications**.

2. Sélectionnez une vulnérabilité logicielle.

3. Ignorez la vulnérabilité sélectionnée.

La vulnérabilité logicielle est ignorée sur l'appareil sélectionné.

La vulnérabilité dans l'application ignorée ne sera pas corrigée après la fin de la tâche *Corriger les vulnérabilités* ou de la tâche *Installation des mises à jour requises et correction des vulnérabilités*. Vous pouvez exclure les vulnérabilités logicielles ignorées de la liste des vulnérabilités à l'aide d'un filtre.

Sélection des correctifs utilisateur pour les vulnérabilités dans le logiciel tiers

Pour utiliser la tâche *Corriger les vulnérabilités*, vous devez spécifier manuellement les mises à jour logicielles visant à corriger les vulnérabilités logicielles tierces répertorié dans les paramètres de la tâche. La tâche *Corriger les vulnérabilités* utilise les correctifs recommandés pour les logiciels Microsoft et les correctifs utilisateur pour d'autres logiciels tiers. Les *correctifs des utilisateurs* sont des mises à jour logicielles corrigeant les vulnérabilités pour lesquelles l'administrateur a précisé manuellement qu'elles sont à installer.

Pour sélectionner les correctifs des vulnérabilités dans les logiciels tiers :

1. Dans l'arborescence de la console, accédez au dossier **Avancé** → **Gestion des applications**, puis le sous-dossier **Vulnérabilités dans les applications**.

   L'espace de travail du dossier affiche une liste des vulnérabilités dans les applications détectées sur les appareils par l'Agent d'administration installé sur ces appareils.

2. Sélectionnez la vulnérabilité pour laquelle vous voulez spécifier un correctif utilisateur.

3. Dans le menu contextuel de la vulnérabilité, sélectionnez **Propriétés**.

   La fenêtre des propriétés de la vulnérabilité s'ouvre.

4. Dans la section **Correctifs utilisateurs et autres**, cliquez sur le bouton **Ajouter**.

   Une liste des paquets d'installation disponibles s'affiche. La liste des paquets d'installation affichés correspond à la liste **Installation à distance** → **Paquets d'installation**. Si vous n'avez pas créé de paquet d'installation contenant un correctif utilisateur pour la vulnérabilité sélectionnée, vous pouvez créer le paquet maintenant en démarrant l'Assistant de création du paquet d'installation.

5. Sélectionnez un ou des paquets d'installation contenant un ou des correctifs utilisateurs pour la vulnérabilité du logiciel tiers.

6. Cliquez sur le bouton **OK**.

Les paquets d'installation contenant les correctifs utilisateur pour la vulnérabilité logicielle sont spécifiés. Lorsque la tâche *Corriger les vulnérabilités* est lancée, le paquet d'installation est installé et la vulnérabilité logicielle est corrigée.

Règles pour l'installation de la mise à jour

Lorsque vous réparez des vulnérabilités dans des applications, vous devez définir les règles d'installation des mises à jour. Ces règles déterminent les mises à jour à installer et les vulnérabilités à corriger.

Les paramètres exacts dépendent de l'objet pour lequel vous créez une règle : pour les mises à jour des applications Microsoft, de produits tiers (applications développées par des éditeurs autres que Kaspersky et Microsoft) ou de toutes les applications. Lors de la création d'une règle pour des applications Microsoft ou des produits tiers, vous pouvez sélectionner des applications spécifiques et les versions de l'application pour lesquelles vous souhaitez installer les mises à jour. Lors de la création d'une règle pour toutes les applications, vous pouvez sélectionner les mises à jour spécifiques que vous souhaitez installer et les vulnérabilités que vous souhaitez éliminer via l'installation des mises à jour.

Pour créer une nouvelle règle pour les mises à jour de toutes les applications :

1. Sur la page **Paramètres** de l'Assistant de création d'une tâche, cliquez sur le bouton **Ajouter**.

   L'Assistant de création de règles se lance. Suivez les étapes de l'Assistant.

2. Sur la page **Type de règle**, sélectionnez **Règle pour toutes les mises à jour**.

3. Sur la page **Critères généraux**, utilisez les listes déroulantes pour définir les paramètres suivants :

   - Définir les mises à jour à installer

     Sélectionnez les mises à jour qui doivent être installées sur les appareils clients :

     - **Installer uniquement les mises à jour confirmées**. Cette option installe uniquement les mises à jour confirmées.
     - **Installer toutes les mises à jour (sauf les mises à jour rejetées)**. Cette option installe les mises à jour avec l'état *Approuvé* ou *Non défini*.
     - **Installer toutes les mises à jour (y compris les mises à jour rejetées)**. Ceci installe toutes les mises à jour, quel que soit leur état d'approbation. Sélectionnez cette option avec prudence. Par exemple, utilisez cette option si vous souhaitez vérifier l'installation de certaines mises à jour rejetées dans une infrastructure d'essai.

   - Corriger les vulnérabilités de niveau de gravité égal ou supérieur à

     Parfois, les mises à jour du logiciel peuvent nuire à l'expérience de l'utilisateur. Dans ce cas, il se peut que vous décidiez d'installer uniquement les mises à jour critiques au fonctionnement du logiciel et d'ignorer les autres.

     Quand cette option est activée, les mises à jour corrigent uniquement les vulnérabilités dont le niveau de gravité tel que défini par Kaspersky est égal ou supérieur à la valeur sélectionnée dans la liste (**Moyenne**, **Élevé** ou **Critique**). Les vulnérabilités dont le niveau de gravité est inférieur à la valeur sélectionnée ne sont pas corrigées.

     Si cette option est désactivée, les mises à jour corrigent toutes les vulnérabilités, quel que soit le niveau de gravité.

     Cette option est Inactif par défaut.

4. Sur la page **Mises à jour**, sélectionnez les mises à jour à installer :

- **Installer toutes les mises à jour convenables**

  Installez toutes les mises à jour du logiciel qui répondent aux critères définis à la page **Critères généraux** de l'assistant. Sélectionné par défaut.

- **Installer uniquement les mises à jour depuis la liste**

  Installer uniquement les mises à jour du logiciel que vous sélectionnez manuellement dans la liste. Cette liste contient toutes les mises à jour du logiciel disponibles.

  Par exemple, vous pouvez sélectionner des mises à jour spécifiques dans les cas suivants : pour vérifier leur installation dans un environnement d'essai, pour mettre à jour uniquement les applications critiques ou pour mettre à jour uniquement certaines applications.

  - **&Installer automatiquement toutes les mises à jour précédentes des applications nécessaires à l'installation des mises à jour sélectionnées**

    Conservez cette option si vous acceptez l'installation de versions de l'application intermédiaires quand l'impose l'installation des mises à jour sélectionnées.

    Si vous désactivez cette option, seules les versions sélectionnées des applications sont installées. Désactivez cette option si vous souhaitez mettre à jour les applications d'une manière directe, sans tenter d'installer les versions successives. S'il est impossible d'installer les mises à jour sélectionnées sans installer les versions antérieures de l'application, la mise à jour de l'application échoue.

    Admettons que la version 3 d'une application est installée sur un appareil et vous souhaitez réaliser la mise à jour jusque la version 5, mais la version 5 de cette application peut être installée uniquement sur la version 4. Quand cette option est installée, le logiciel installe d'abord la version 4, puis la version 5. Si l'option est désactivée, le logiciel ne parvient pas à mettre l'application à jour.

    Cette option est activée par défaut.

5. Sur la page **Vulnérabilités**, sélectionnez les vulnérabilités qui seront corrigées suite à l'installation des mises à jour sélectionnées :

- **Corriger toutes les vulnérabilités qui correspondent aux autres critères**

  Corrigez toutes les vulnérabilités qui satisfont les critères définis à la page **Critères généraux** de l'assistant. Sélectionné par défaut.

- **Corriger uniquement les vulnérabilités depuis la liste**

  Corrigez uniquement les vulnérabilités que vous sélectionnez manuellement dans la liste. Cette liste contient toutes les vulnérabilités détectées.

  Par exemple, vous pouvez sélectionner des vulnérabilités spécifiques dans les cas suivants : pour vérifier les corrections dans un environnement d'essai, pour corriger les vulnérabilités uniquement dans les applications critiques ou pour corriger les vulnérabilités uniquement dans certaines applications.

6. La page **Définition du nom de** permet de renseigner le nom de la tâche créée. Vous pouvez changer ce nom plus tard dans la section **Partenaires** de la fenêtre des propriétés de la tâche créée.

Une fois que l'Assistant de création de règles a terminé, la nouvelle règle est créée et apparaît dans le champ **Définissez les règles d'installation des mises à jour** de l'Assistant de création d'une tâche.

Pour créer une règle pour les mises à jour des applications Microsoft :

1. Sur la page **Paramètres** de l'Assistant de création d'une tâche, cliquez sur le bouton **Ajouter**.

   L'Assistant de création de règles se lance. Suivez les étapes de l'Assistant.

2. Sur la page **Type de règle**, sélectionnez **Règle pour les mises à jour Windows Update**.

3. Dans la fenêtre **Critères généraux**, configurez les paramètres suivants :

   - **Définir les mises à jour à installer**

     Sélectionnez les mises à jour qui doivent être installées sur les appareils clients :

     - **Installer uniquement les mises à jour confirmées**. Cette option installe uniquement les mises à jour confirmées.
     - **Installer toutes les mises à jour (sauf les mises à jour rejetées)**. Cette option installe les mises à jour avec l'état *Approuvé* ou *Non défini*.
     - **Installer toutes les mises à jour (y compris les mises à jour rejetées)**. Ceci installe toutes les mises à jour, quel que soit leur état d'approbation. Sélectionnez cette option avec prudence. Par exemple, utilisez cette option si vous souhaitez vérifier l'installation de certaines mises à jour rejetées dans une infrastructure d'essai.

   - **Corriger les vulnérabilités de niveau de gravité égal ou supérieur à**

     Parfois, les mises à jour du logiciel peuvent nuire à l'expérience de l'utilisateur. Dans ce cas, il se peut que vous décidiez d'installer uniquement les mises à jour critiques au fonctionnement du logiciel et d'ignorer les autres.

     Quand cette option est activée, les mises à jour corrigent uniquement les vulnérabilités dont le niveau de gravité tel que défini par Kaspersky est égal ou supérieur à la valeur sélectionnée dans la liste (**Moyenne**, **Élevé** ou **Critique**). Les vulnérabilités dont le niveau de gravité est inférieur à la valeur sélectionnée ne sont pas corrigées.

     Si cette option est désactivée, les mises à jour corrigent toutes les vulnérabilités, quel que soit le niveau de gravité.

     Cette option est Inactif par défaut.

   - **Corriger les vulnérabilités qui présentent un niveau de gravité selon MSRC égal ou supérieur à**

     Parfois, les mises à jour du logiciel peuvent nuire à l'expérience de l'utilisateur. Dans ce cas, il se peut que vous décidiez d'installer uniquement les mises à jour critiques au fonctionnement du logiciel et d'ignorer les autres.

     Quand cette option est activée, les mises à jour corrigent uniquement les vulnérabilités dont le niveau de gravité tel que défini par Microsoft Security Response Center (MSRC) est égal ou supérieur à la valeur sélectionnée dans la liste (**Bas**, **Moyenne**, **Élevé** ou **Critique**). Les vulnérabilités dont le niveau de gravité est inférieur à la valeur sélectionnée ne sont pas corrigées.

     Si cette option est désactivée, les mises à jour corrigent toutes les vulnérabilités, quel que soit le niveau de gravité.

     Cette option est Inactif par défaut.

4. Sur la page **Applications**, sélectionnez les applications et les versions des applications pour lesquelles vous voulez installer les mises à jour. Toutes les applications sont cochées par défaut.

5. Sur la page **Catégories des mises à jour**, sélectionnez les catégories de mise à jour à installer. Ces catégories sont les mêmes que dans le catalogue Microsoft Update. Toutes les catégories sont cochées par défaut.

6. La page **Définition du nom de** permet de renseigner le nom de la tâche créée. Vous pouvez changer ce nom plus tard dans la section **Partenaires** de la fenêtre des propriétés de la tâche créée.

Une fois que l'Assistant de création de règles a terminé, la nouvelle règle est créée et apparaît dans le champ **Définissez les règles d'installation des mises à jour** de l'Assistant de création d'une tâche.

Pour créer une règle pour les mises à jour des produits tiers :

1. Sur la page **Paramètres** de l'Assistant de création d'une tâche, cliquez sur le bouton **Ajouter**.

   L'Assistant de création de règles se lance. Suivez les étapes de l'Assistant.

2. Sur la page **Type de règle**, sélectionnez **Règles pour les mises à jour tierces**.

3. Dans la fenêtre **Critères généraux**, configurez les paramètres suivants :

   - **Définir les mises à jour à installer**

     Sélectionnez les mises à jour qui doivent être installées sur les appareils clients :

     - **Installer uniquement les mises à jour confirmées**. Cette option installe uniquement les mises à jour confirmées.
     - **Installer toutes les mises à jour (sauf les mises à jour rejetées)**. Cette option installe les mises à jour avec l'état *Approuvé* ou *Non défini*.
     - **Installer toutes les mises à jour (y compris les mises à jour rejetées)**. Ceci installe toutes les mises à jour, quel que soit leur état d'approbation. Sélectionnez cette option avec prudence. Par exemple, utilisez cette option si vous souhaitez vérifier l'installation de certaines mises à jour rejetées dans une infrastructure d'essai.

   - **Corriger les vulnérabilités de niveau de gravité égal ou supérieur à**

     Parfois, les mises à jour du logiciel peuvent nuire à l'expérience de l'utilisateur. Dans ce cas, il se peut que vous décidiez d'installer uniquement les mises à jour critiques au fonctionnement du logiciel et d'ignorer les autres.

     Quand cette option est activée, les mises à jour corrigent uniquement les vulnérabilités dont le niveau de gravité tel que défini par Kaspersky est égal ou supérieur à la valeur sélectionnée dans la liste (**Moyenne**, **Élevé** ou **Critique**). Les vulnérabilités dont le niveau de gravité est inférieur à la valeur sélectionnée ne sont pas corrigées.

     Si cette option est désactivée, les mises à jour corrigent toutes les vulnérabilités, quel que soit le niveau de gravité.

     Cette option est Inactif par défaut.

4. Sur la page **Applications**, sélectionnez les applications et les versions d'applications pour lesquelles vous voulez installer les mises à jour. Toutes les applications sont cochées par défaut.

5. La page **Définition du nom de** permet de renseigner le nom de la tâche créée. Vous pouvez changer ce nom plus tard dans la section **Partenaires** de la fenêtre des propriétés de la tâche créée.

Une fois que l'Assistant de création de règles a terminé, la nouvelle règle est créée et apparaît dans le champ **Définissez les règles d'installation des mises à jour** de l'Assistant de création d'une tâche.

Groupes des applications

Cette section décrit l'utilisation des groupes des applications installées sur les appareils.

Création des catégories d'applications

Kaspersky Security Center permet de créer les catégories d'applications installées sur les appareils.

Il est possible de créer les catégories d'applications à l'aide des moyens suivants :

- L'administrateur indique le dossier dont les fichiers exécutables se trouvent dans la catégorie sélectionnée.
- L'administrateur indique l'appareil dont les fichiers exécutables se trouvent dans la catégorie sélectionnée.
- L'administrateur définit les critères selon lesquels les applications se trouvent dans la catégorie sélectionnée.

Quand une catégorie d'applications est créée, l'administrateur peut définir les règles pour cette catégorie. Les règles définissent le comportement des applications qui sont incluses dans la catégorie indiquée. Par exemple, il est possible d'interdire ou d'autoriser le lancement des applications qui font partie de la catégorie.

Administration du lancement des applications sur les appareils

Kaspersky Security Center permet d'administrer le lancement des applications sur les appareils en mode Liste d'autorisation. La description détaillée est fournie dans l'aide en ligne de Kaspersky Endpoint Security for Windows. Le mode Liste d'autorisation signifie que le lancement uniquement des applications, qui font partie des catégories indiquées, sera autorisé sur les appareils sélectionnés. L'administrateur peut consulter les résultats de l'analyse statique des règles de lancement des applications sur les appareils pour chaque utilisateur.

Inventaire du logiciel installé sur les appareils

Kaspersky Security Center permet de réaliser un inventaire des logiciels sur les appareils tournant sous Windows et Linux. L'Agent d'administration obtient les informations sur toutes les applications installées sur les appareils. Les informations obtenues suite à l'inventaire s'affichent dans l'espace de travail du dossier **Registre des applications**. L'administrateur peut consulter les informations détaillées sur chaque application, y compris la version et l'éditeur.

Le nombre de fichiers exécutables reçus d'un appareil ne peut pas dépasser 150 000. Une fois cette limite atteinte, Kaspersky Security Center ne peut plus accepter de nouveaux fichiers.

Administration des groupes des applications sous licence

Kaspersky Security Center permet de créer les groupes des applications sous licence. Le groupe des applications sous licence inclut les applications qui répondent aux critères définis par l'administrateur. L'administrateur peut indiquer les critères suivants pour les groupes des applications sous licence :

- Nom de l'application
- Version de l'application
- Fabricant
- Tag de l'application

Les applications qui correspondent à un ou plusieurs critères sont placées automatiquement dans le groupe. Pour créer le groupe des applications sous licence, au moins un critère d'inclusion des applications dans ce groupe doit être défini.

Chaque groupe des applications sous licence possède sa clé de licence. La clé de licence du groupe des applications sous licence définit le nombre admissible des installations pour les applications qui font partie du groupe. Si le nombre d'installations dépasse la restriction définie dans la clé de licence, l'événement d'informations s'enregistre sur le Serveur d'administration. L'administrateur peut indiquer la date de fin de validité de la clé de licence. Lorsque cette date survient, l'événement d'informations est enregistré sur le Serveur d'administration.

Consultation des informations sur les fichiers exécutables

Kaspersky Security Center reçoit toutes les informations sur les fichiers exécutables qui ont été lancés sur les appareils dès l'installation du système d'exploitation sur ceux-ci. Les informations collectées sur les fichiers exécutables s'affichent dans la fenêtre principale de l'application, dans l'espace de travail du dossier **Fichiers exécutables**.

Utilisation du Contrôle des applications pour gérer les fichiers exécutables

Vous pouvez utiliser le module Contrôle des applications pour autoriser ou interdire le lancement de fichiers exécutables sur les appareils des utilisateurs. Le module Contrôle des applications prend en charge les systèmes d'exploitation Windows et Linux.

Pour les systèmes d'exploitation basés sur Linux, le composant Contrôle des applications est disponible à partir de Kaspersky Endpoint Security 11.2 pour Linux. Le composant est également disponible pour Kaspersky Embedded Systems Security pour Windows 3.0 ou version ultérieure.

Prérequis

- Kaspersky Security Center est déployé dans votre entreprise.
- La stratégie de Kaspersky Endpoint Security for Windows ou de Kaspersky Endpoint Security for Linux est créée et activée.
- La stratégie de Kaspersky Embedded Systems Security for Windows ou de Kaspersky Embedded Systems Security for Linux est créée et active.

Étapes

Le scénario d'utilisation Contrôle des applications se déroule par étapes :

1. **Formation et consultation de la liste des fichiers exécutables sur les appareils client**

   Cette étape vous permet de découvrir les fichiers exécutables qui figurent sur les appareils administrés. Consultez la liste des fichiers exécutables et comparez-la avec les listes des fichiers exécutables autorisés et interdits. Les restrictions d'utilisation des fichiers exécutables peuvent être liées aux stratégies de sécurité de l'information dans votre entreprise.

   Instructions pour :

   - Console d'administration : inventaire des fichiers exécutables
   - Kaspersky Security Center Web Console : obtention et consultation d'une liste des fichiers exécutables stockés sur les appareils client

2. **Création de catégories pour les fichiers exécutables utilisés dans votre organisation**

   Analysez les listes des fichiers exécutables stockés sur les appareils administrés. En fonction de l'analyse, créez des catégories pour les fichiers exécutables. Il est recommandé de créer une catégorie "Applications de travail" qui englobe l'ensemble standard des fichiers exécutables utilisés dans votre organisation. Si différents groupes de sécurité utilisent leurs propres ensembles de fichiers exécutables dans leur travail, une catégorie distincte peut être créée pour chaque groupe de sécurité.

   Instructions pour :

   - Console d'administration : Création d'une catégorie d'applications dont le contenu est ajouté manuellement, Création d'une catégorie d'applications qui inclut les fichiers exécutables des appareils sélectionnés, Création d'une catégorie d'applications qui inclut les fichiers exécutables du dossier spécifié.
   - Kaspersky Security Center Web Console : Création d'une catégorie d'applications dont le contenu est ajouté manuellement, Création d'une catégorie d'applications qui inclut les fichiers exécutables des appareils sélectionnés, Création d'une catégorie d'applications qui inclut les fichiers exécutables du dossier spécifié.

3. **Configuration du Contrôle des applications dans la stratégie Kaspersky Endpoint Security**

   Configurez le composant Contrôle des applications dans la stratégie Kaspersky Endpoint Security à l'aide des catégories que vous avez créées à l'étape précédente.

   Instructions pour :

   - Console d'administration : configuration d'administration du lancement des applications sur les appareils client
   - Kaspersky Security Center Web Console : configuration du Contrôle des applications dans la stratégie Kaspersky Endpoint Security for Windows

4. **Configuration du Contrôle des applications dans la stratégie de l'application Kaspersky Embedded Systems Security**

   Configurez le composant Contrôle des applications dans la stratégie de Kaspersky Embedded Systems Security for Windows à l'aide des catégories que vous avez créées. Pour plus d'informations sur le composant Contrôle des applications, consultez l'Aide de Kaspersky Embedded Systems Security for Windows ou l'Aide de Kaspersky Embedded Systems Security for Linux.

   Si vous utilisez un grand nombre de règles, une erreur peut se produire lors du chargement de la stratégie. Vous pouvez augmenter la taille maximale de la demande en octets en utilisant les commandes suivantes :

   - Pour la requête JSON :

```
klscflag -fset -pv ".core/.independent" -s KLLIM -n
LP_KLOAPI_MaxSizeOfJsonRequestInBytes -v <max_request_size> -t d
```

- Pour la requête HTTP :

  ```
  klscflag -fset -pv ".core/.independent" -s KLLIM -n
  LP_KLOAPI_MaxSizeOfHttpRequestInBytes -v <max_request_size> -t d
  ```

  Où `<max_request_size>` est une taille de requête maximale en octets (par exemple, `200000000`).

5. **Activation du composant Contrôle des applications en mode test**

   Pour vous assurer que les règles de Contrôle des applications ne bloquent pas les fichiers exécutables nécessaires pour le travail, il est recommandé d'activer le test des règles de Contrôle des applications et d'analyser leur fonctionnement après avoir créé de nouvelles règles. Lorsque les tests sont activés, Kaspersky Endpoint Security for Windows ou Kaspersky Embedded Systems Security ne bloquera pas les fichiers exécutables dont le démarrage est interdit par les règles de Contrôle des applications, mais enverra des notifications relatives à leur démarrage dans le Serveur d'administration.

   Lors du test des règles de Contrôle des applications, il est recommandé d'effectuer les actions suivantes :

   - déterminez la période de test. La période de test peut aller de quelques jours à deux mois.
   - Examinez les événements résultant du test de fonctionnement du Contrôle des applications.

   Instructions pratiques pour Kaspersky Security Center Web Console : Configuration du module Contrôle des applications dans la stratégie Kaspersky Endpoint Security for Windows. Suivez ces instructions et activez l'option **Mode de test** dans le processus de configuration.

6. **Modification des paramètres des catégories du composant Contrôle des applications**

   Si nécessaire, modifiez les paramètres du Contrôle des applications. Selon les résultats des tests, vous pouvez ajouter des fichiers exécutables associés aux événements du composant Contrôle des applications à une catégorie enrichie manuellement.

   Instructions pour :

   - Console d'administration : ajout de fichiers exécutables liés par un événement à la catégorie de l'application
   - Kaspersky Security Center Web Console : ajout de fichiers exécutables liés par un événement à la catégorie de l'application

7. **Appliquer les règles du Contrôle des applications en mode de fonctionnement**

   Une fois les règles du Contrôle des applications testées et la configuration des catégories terminée, vous pouvez appliquer les règles du Contrôle des applications en mode de fonctionnement.

   Instructions pratiques pour Kaspersky Security Center Web Console : Configuration du module Contrôle des applications dans la stratégie Kaspersky Endpoint Security for Windows. Suivez ces instructions et désactivez l'option **Mode de test** dans le processus de configuration.

8. **Vérification de la configuration du Contrôle des applications**

   Assurez-vous d'avoir effectué les tâches suivantes :

   - Catégories créées pour les fichiers exécutables.
   - Configuré le Contrôle des applications en utilisant les catégories.
   - Appliquer les règles du Contrôle des applications en mode de fonctionnement.

Résultats

Une fois le scénario terminé, le démarrage des fichiers exécutables est contrôlé sur les appareils administrés. Les utilisateurs peuvent uniquement exécuter les fichiers exécutables autorisés dans votre organisation et ne peuvent pas exécuter les fichiers exécutables qui y sont interdits.

Pour obtenir des informations détaillées sur le Contrôle des applications, consultez les rubriques d'aide suivantes :

- Aide en ligne de Kaspersky Endpoint Security for Windows
- Aide en ligne de Kaspersky Endpoint Security for Linux
- Kaspersky Security for Virtualization Light Agent
- Aide de Kaspersky Embedded Systems Security for Windows
- Aide de Kaspersky Embedded Systems Security for Linux

Obtention et consultation d'une liste des fichiers exécutables stockés sur les appareils client

Vous pouvez obtenir la liste des fichiers exécutables stockés sur les appareils clients de l'une des manières suivantes :

- Activation des notifications sur le démarrage des applications dans la stratégie de Kaspersky Endpoint Security.
- Création d'une tâche d'inventaire.

Activation des notifications sur le démarrage des applications dans la stratégie de Kaspersky Endpoint Security

Pour activer les notifications relatives au démarrage des applications, procédez comme suit :

1. Ouvrez les paramètres de la stratégie de Kaspersky Endpoint Security, puis accédez à **Paramètres généraux** → **Rapports et stockage**.
2. Dans le groupe de paramètres **Transfert de données au Serveur d'administration**, cochez la case **À propos des applications lancées** et enregistrez les modifications.

Lorsqu'un utilisateur tente de lancer des fichiers exécutables, les informations relatives à ces fichiers sont ajoutées à la liste des fichiers exécutables sur un appareil client. Kaspersky Endpoint Security envoie ces informations à l'Agent d'administration, qui les transmet ensuite au Serveur d'administration.

Création d'une tâche d'inventaire

La fonction d'inventaire des fichiers exécutables est disponible pour les applications suivantes :

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Linux version 11.2 et ultérieure
- Kaspersky Security for Virtualization 4.0 Light Agent et versions ultérieures

Vous pouvez réduire la charge sur la base de données tout en obtenant des informations sur les applications installées. Pour gagner de la place, exécutez une tâche d'inventaire sur les appareils de référence sur lesquels un ensemble standard de logiciels est installé. Il est préférable que le nombre d'appareils soit compris entre 1 et 3.

Nous vous déconseillons fortement d'exécuter la tâche d'inventaire lors de l'utilisation des bases de données suivantes : MySQL, PostgreSQL, SQL Server Express Edition et MariaDB (toutes les éditions).

Pour créer une tâche d'inventaire des fichiers exécutables sur les appareils clients, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le dossier **Tâches**.
2. Dans l'espace de travail du dossier **Tâches**, cliquez sur le bouton **Nouvelle tâche**.

   Ceci permet de lancer l'Assistant de création d'une tâche.
3. Dans la fenêtre **Sélection du type de tâche** de l'Assistant, sélectionnez **Kaspersky Endpoint Security** comme type de tâche, puis sélectionnez le sous-type de tâche **Inventaire**, et cliquez sur **Suivant**.
4. Suivez les étapes ultérieures de l'assistant.

   Une fois que l'Assistant de création d'une tâche a terminé l'opération, la tâche **Inventaire** est créée et configurée. Si vous le souhaitez, vous pouvez modifier les paramètres de la tâche créée. La tâche qui vient d'être créée s'affiche dans la liste des tâches. Si vous le souhaitez, vous pouvez modifier les paramètres de la tâche créée.

Pour obtenir une description détaillée de la tâche d'inventaire, consultez les aides suivantes :

- Aide de Kaspersky Endpoint Security for Windows
- Aide de Kaspersky Endpoint Security for Linux
- Kaspersky Security for Virtualization Light Agent

Une fois la tâche **Inventaire** effectuée, la liste des fichiers exécutables stockés sur les appareils administrés est créée et vous pouvez la consulter.

Lors de l'inventaire, les fichiers exécutables aux formats suivants peuvent être détectés (selon l'option sélectionnée dans les propriétés de la tâche d'inventaire) : MZ, COM, PE, NE, SYS, CMD, BAT, PS1, JS, VBS, REG, MSI, CPL, DLL, JAR et HTML.

Affichage de la liste des fichiers exécutables stockés sur les appareils administrés

Pour consulter la liste de tous les fichiers exécutables stockés sur les appareils client :

Dans l'arborescence de la console, accédez à **Avancé** → **Gestion des applications** → **Fichiers exécutables**.

Si nécessaire, vous pouvez envoyer un fichier exécutable d'un appareil administré vers l'appareil sur lequel la Console d'administration est installée.

Pour envoyer un fichier exécutable, procédez comme suit :

1. Dans l'arborescence de la console, accédez à **Avancé** → **Gestion des applications** → **Fichiers exécutables**.
2. Cliquez sur le lien du fichier exécutable que vous souhaitez envoyer à l'appareil avec la Console d'administration installée.
3. Dans la fenêtre qui s'ouvre, accédez à la section **Appareils**, puis cochez la case correspondant à l'appareil administré à partir duquel vous souhaitez envoyer le fichier exécutable.

   Avant d'envoyer le fichier exécutable, assurez-vous que l'appareil administré dispose d'une connexion directe au Serveur d'administration, en cochant la case **Maintenir la connexion au Serveur d'administration**.
4. Cliquez sur le bouton **Envoyer**, sélectionnez le dossier de destination, puis cliquez sur **OK**.

Le fichier exécutable sélectionné est téléchargé pour être envoyé ultérieurement à l'appareil avec le programme d'installation de la Console d'administration.

Création de catégories d'applications pour les stratégies de Kaspersky Endpoint Security for Windows

Vous pouvez créer des catégories d'applications pour les stratégies de Kaspersky Endpoint Security for Windows au départ du dossier **Catégories d'applications** et depuis la fenêtre **Propriétés** d'une stratégie de Kaspersky Endpoint Security for Windows.

*Pour créer une catégorie d'applications pour une stratégie de Kaspersky Endpoint Security depuis le dossier **Catégories d'applications** :*

1. Dans l'arborescence de la console, sélectionnez **Avancé** → **Gestion des applications** → **Catégories d'applications**.
2. Dans l'espace de travail du dossier **Catégories d'applications**, cliquez sur le bouton **Nouvelle catégorie**.

   L'Assistant de nouvelle catégorie démarre.

3. Sur la page **Type de catégorie**, sélectionnez le type de catégorie utilisateur :

   - **Catégorie complétée à la main**. Indiquez les critères selon lesquels les fichiers exécutables vont être associés à la catégorie créée.

   - **Catégorie complétée automatiquement**. Spécifiez le dossier à partir duquel les fichiers exécutables seront automatiquement attribués à la catégorie créée.

     Lors de la création d'une catégorie enrichie automatiquement, l'application recense les types de fichiers suivants : EXE, COM, DLL, SYS, BAT, PS1, CMD, JS, VBS, REG, MSI, MSC, CPL, HTML, HTM, DRV, OCX et SCR.

   - **Catégorie qui incluent des fichiers exécutables depuis les appareils sélectionnés**. Indiquez l'appareil dont les fichiers exécutables doivent se retrouver automatiquement dans la catégorie.

4. Suivez les instructions de l'assistant.

Une catégorie d'application utilisateur est ainsi créée à l'issue de l'Assistant. Les catégories créées peuvent être consultées dans la liste de catégories de l'espace de travail du dossier **Catégories d'applications**.

Si vous souhaitez exporter une catégorie d'application vers un fichier KLC, faites un clic droit sur le nom de la catégorie, sélectionnez **Exporter** dans le menu, puis dans la fenêtre qui s'ouvre, précisez le nom du fichier et cliquez sur **Enregistrer**.

Vous pouvez également créer une catégorie d'application depuis le dossier **Stratégies**.

*Pour créer une catégorie d'application depuis la fenêtre **Propriétés** d'une stratégie de Kaspersky Endpoint Security for Windows :*

1. Dans l'arborescence de la console, sélectionnez le dossier **Stratégies**.

2. Dans l'espace de travail du dossier **Stratégies**, sélectionnez une stratégie de Kaspersky Endpoint Security pour laquelle vous souhaitez créer une catégorie.

3. Cliquez-droit et sélectionnez l'option **Propriétés**.

4. Dans la fenêtre **Propriétés** qui s'ouvre, dans le volet de gauche **Sections**, sélectionnez **Contrôles de sécurité → Contrôle des applications**.

5. Dans la section **Contrôle des applications**, accédez aux listes déroulantes **Mode de contrôle** et **Action** et réalisez vos sélections pour les listes d'autorisation ou de refus, puis cliquez sur le bouton **Ajouter**.

   La fenêtre **Règle de contrôle des applications** avec la liste de catégories s'ouvre.

6. Cliquez sur le bouton **Nouveau**.

7. Saisissez le nom de la nouvelle catégorie, puis cliquez sur **OK**.

   L'Assistant de nouvelle catégorie démarre.

8. Sur la page **Type de catégorie**, sélectionnez le type de catégorie utilisateur :

   - **Catégorie complétée à la main**. Indiquez les critères selon lesquels les fichiers exécutables vont être associés à la catégorie créée.
   - **Catégorie complétée automatiquement**. Spécifiez le dossier à partir duquel les fichiers exécutables seront automatiquement attribués à la catégorie créée.

     Lors de la création d'une catégorie enrichie automatiquement, l'application recense les types de fichiers suivants : EXE, COM, DLL, SYS, BAT, PS1, CMD, JS, VBS, REG, MSI, MSC, CPL, HTML, HTM, DRV, OCX et SCR.

   - **Catégorie qui incluent des fichiers exécutables depuis les appareils sélectionnés**. Indiquez l'appareil dont les fichiers exécutables doivent se retrouver automatiquement dans la catégorie.

9. Suivez les instructions de l'assistant.

Une catégorie d'application utilisateur est ainsi créée à l'issue de l'Assistant. Vous pouvez voir les nouvelles catégories dans la liste des catégories.

Les catégories d'applications sont utilisées par le module Contrôle des applications, qui fait partie de l'application Kaspersky Endpoint Security for Windows. Grâce au module Contrôle des applications, l'administrateur peut imposer des restrictions sur le lancement des applications sur les appareils client, par exemple, sur la base des applications qui appartiennent à une catégorie déterminée.

Création d'une catégorie d'applications enrichie manuellement

Vous pouvez spécifier un ensemble de critères comme modèle pour les fichiers exécutables dont vous souhaitez autoriser ou bloquer le démarrage dans votre entreprise. En vous basant sur les fichiers exécutables correspondant aux critères, vous pouvez créer une catégorie d'applications et l'utiliser dans la configuration du composant Contrôle des applications.

Pour créer une catégorie d'applications enrichie manuellement, procédez comme suit :

1. Dans l'arborescence de la console, dans le dossier **Avancé** → **Gestion des applications**, sélectionnez le sous-dossier **Catégories d'applications**.
2. Cliquez sur le bouton **Nouvelle catégorie**.

   L'**Assistant de nouvelle catégorie** démarre. Parcourez les étapes de l'Assistant à l'aide du bouton **Suivant**.
3. Sur la page **Type de catégorie** de l'Assistant, sélectionnez le type de la catégorie d'utilisateur **Catégorie créée à la main**.
4. Sur la page de l'Assistant **Saisissez le nom de la catégorie d'applications**, saisissez le nom de la nouvelle catégorie d'applications.
5. Sur la page **Configuration des conditions d'inclusion des applications dans des catégories**, cliquez sur le bouton **Ajouter**.

6. Dans la liste déroulante, spécifiez les paramètres dont vous avez besoin :

- **Depuis la liste des fichiers exécutables**

  Si vous avez choisi cette option, vous pouvez sélectionner les applications à ajouter à une catégorie dans la liste des fichiers exécutables de l'appareil client.

- **Depuis les propriétés du fichier**

  Si cette option a été sélectionnée, vous pouvez indiquer à la main les données détaillées des fichiers exécutables qui seront ajoutés dans une catégorie d'applications définie par l'utilisateur.

- **Données méta des fichiers du dossier**

  Indiquez le dossier sur l'appareil client qui contient les fichiers exécutables. Les données méta des fichiers exécutables, faisant partie du dossier indiqué, seront transmises sur le Serveur d'administration. Les fichiers exécutables, possédant les mêmes données méta, seront ajoutés dans une catégorie d'applications définie par l'utilisateur.

- **Hash des fichiers du dossier**

  Si cette option a été sélectionnée, vous pouvez sélectionner ou créer un dossier sur l'appareil client. Le hash MD5 des fichiers, compris dans le dossier indiqué, sera transmis sur le Serveur d'administration. Les applications, possédant le même hash que les fichiers du dossier indiqué, seront ajoutées dans une catégorie d'applications définie par l'utilisateur.

- **Certificats des fichiers issus du dossier**

  Si cette option a été sélectionnée, vous pouvez indiquer le dossier sur l'appareil client qui contient les fichiers exécutables signés par des certificats. Les certificats des fichiers exécutables sont pris en compte et sont ajoutés aux conditions de catégorie. Les fichiers exécutables signés conformément aux certificats seront ajoutés à la catégorie utilisateur.

- **Métadonnées des fichiers de l'installateur MSI**

  Si cette option a été sélectionnée, vous pouvez indiquer le fichier de l'installateur MSI en tant que la condition d'ajout des applications dans une catégorie d'utilisateur. Les données méta de l'installateur de l'application seront transmises sur le Serveur d'administration. Les applications, dont les données méta de l'installateur coïncident avec l'installateur MSI indiqué, seront ajoutées dans une catégorie d'applications définie par l'utilisateur.

- **Sommes de contrôle des fichiers de l'installateur msi de l'&application**

  Si cette option a été sélectionnée, vous pouvez indiquer le fichier de l'installateur MSI en tant que la condition d'ajout des applications dans une catégorie d'utilisateur. Le hash des fichiers de l'installateur de l'application sera transmis sur le Serveur d'administration. Les applications, dont le hash des fichiers de l'installateur MSI coïncide avec le hash indiqué, seront ajoutées dans une catégorie d'applications définie par l'utilisateur.

- **D'une catégorie K&L**

  Si cette option a été sélectionnée, vous pouvez indiquer la catégorie d'applications de Kaspersky en tant que la condition d'ajout des applications dans une catégorie d'utilisateur. Les applications, faisant partie de la catégorie Kaspersky, seront ajoutées dans une catégorie d'applications définie par l'utilisateur.

- **Définir le chemin d'accès à l'a&pplication (masques pris en charge)**

  Si cette option a été sélectionnée, vous pouvez indiquer le chemin d'accès au fichier ou au dossier sur l'appareil client dont les fichiers exécutables seront ajoutés dans une catégorie d'applications définie par l'utilisateur. Vous pouvez utiliser des expressions régulières, comme *C:\path_to_exe*: C:\Program Files\Internet Explorer*.*

- **Sélectionner un certificat dans le stockage**

  Si cette option a été sélectionnée, vous pouvez indiquer les certificats du stockage. La condition de catégorie correspond uniquement aux fichiers exécutables signés par le certificat spécifié.

- **Type de support**

  Si cette option a été sélectionnée, vous pouvez indiquer le type de support (n'importe lequel ou disque amovible) sur lequel l'application est exécutée. Les applications, lancées sur le moyen de type sélectionné, seront ajoutées dans une catégorie d'applications définie par l'utilisateur.

7. Sur la page de l'assistant **Création de la catégorie d'applications**, cliquez sur le bouton **Terminer**.

Kaspersky Security Center utilise les métadonnées seulement des fichiers qui contiennent la signature numérique. Il est impossible de créer une catégorie sur la base des métadonnées des fichiers qui ne contiennent pas de signature numérique.

L'Assistant débouche sur la création manuelle d'une catégorie utilisateur d'applications. Vous pouvez consulter la catégorie créée dans la liste des catégories de l'espace de travail du dossier **Catégories d'applications**.

Si vous souhaitez exporter une catégorie d'application vers un fichier KLC, faites un clic droit sur le nom de la catégorie, sélectionnez **Exporter** dans le menu, puis dans la fenêtre qui s'ouvre, précisez le nom du fichier et cliquez sur **Enregistrer**.

Création d'une catégorie d'applications incluant des fichiers exécutables provenant des appareils sélectionnés

Vous pouvez utiliser des fichiers exécutables des appareils sélectionnés comme modèle des fichiers exécutables que vous souhaitez autoriser ou bloquer. En vous basant sur les fichiers exécutables des appareils sélectionnés, vous pouvez créer une catégorie d'applications et l'utiliser dans la configuration du composant Contrôle des applications.

Pour récupérer la liste des fichiers exécutables depuis les appareils, procédez comme suit :

1. Assurez-vous que la stratégie de Kaspersky Endpoint Security for Windows ou de Kaspersky Endpoint Security for Linux est créée et active. Activez le module Contrôle des applications dans la stratégie.

2. Obtenez une liste des fichiers exécutables stockés sur les appareils client.

Pour créer une catégorie d'applications incluant des fichiers exécutables provenant des appareils sélectionnés :

1. Dans l'arborescence de la console, dans le dossier **Avancé** → **Gestion des applications**, sélectionnez le sous-dossier **Catégories d'applications**.

2. Cliquez sur le bouton **Nouvelle catégorie**.

   L'**Assistant de nouvelle catégorie** démarre. Parcourez les étapes de l'Assistant à l'aide du bouton **Suivant**.

3. Sur la page de l'assistant **Type de catégorie**, sélectionnez **Catégorie qui inclut les fichiers exécutables des appareils sélectionnés** comme type de catégorie d'utilisateurs.

4. Sur la page de l'Assistant **Saisissez le nom de la catégorie d'applications**, saisissez le nom de la nouvelle catégorie d'applications.

5. Sur la page **Paramètres** de l'Assistant, cliquez sur le bouton **Ajouter**.

6. Sélectionnez un appareil (des appareils) dont les fichiers exécutables seront utilisés pour créer la catégorie d'applications.

7. Définissez les paramètres suivants :

- **Algorithme de calcul de la fonction hash**

  En fonction de la version de l'application de sécurité installée sur les appareils de votre réseau, il faut choisir un algorithme de calcul de la fonction hash par l'application Kaspersky Security Center pour les fichiers de la catégorie. Les informations relatives aux 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 du calcul ne contient pas de vulnérabilités et il est considéré actuellement comme la fonction de chiffrement la plus sûre. Kaspersky Endpoint Security 10 Service Pack 2 for Windows et suivants prennent en charge le calcul de la fonction hash SHA256. Le calcul de la fonction de hach MD5 est pris en charge pour les versions inférieures à Kaspersky Endpoint Security 10 Service Pack 2 for Windows.

  Choisissez une des options du calcul de la fonction hash par l'application Kaspersky Security Center pour les fichiers de la catégorie :

  - Si toutes les instances des applications de sécurité installées sur votre réseau sont Kaspersky Endpoint Security 10 Service Pack 2 for Windows ou des versions ultérieures, cochez la case **SHA256**. Il est déconseillé d'ajouter une catégorie créée selon le critère du hachage SHA256 du fichier exécutable pour les versions de l'application antérieures à Kaspersky Endpoint Security 10 Service Pack 2 for Windows. Cela pourrait entraîner un échec de l'application de sécurité. 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 Service Pack 2 for Windows sont installées sur votre réseau, sélectionnez **Hash MD5**. Il est interdit d'ajouter une catégorie créée selon le critère de la somme de contrôle MD5 du fichier exécutable pour les versions Kaspersky Endpoint Security 10 Service Pack 2 for Windows et suivantes. Dans ce cas vous pouvez utiliser la fonction de hachage cryptographique SHA256 pour les fichiers de la catégorie.

  Si différents appareils de votre réseau utilisent à la fois des versions antérieures et ultérieures de Kaspersky Endpoint Security 10, cochez à la fois la case **SHA256** et la case **Hash MD5**.

  La case **Calculer SHA256 pour les fichiers en la catégorie (pris en charge pour Kaspersky Endpoint Security 10 Service Pack 2 for Windows et versions supérieures)** est cochée par défaut.

  La case **Calculer MD5 pour les fichiers en la catégorie (pris en charge pour les versions inférieures à Kaspersky Endpoint Security 10 Service Pack 2 for Windows)** est décochée.

- **Synchroniser les données avec le stockage du Serveur d'administration**

  Sélectionnez cette option si vous souhaitez que le Serveur d'administration vérifie régulièrement les modifications dans le ou les dossiers spécifiés.

  Cette option est Inactif par défaut.

  Si vous activez cette option, indiquez la période (en heures) pour vérifier les modifications dans le ou les dossiers spécifiés. L'intervalle de l'analyse est de 24 heures par défaut.

8. Sur la page **Filtrer** de l'Assistant, spécifiez les paramètres suivants :

   - Type de fichier

     Dans cette section, vous pouvez spécifier le type de fichier utilisé pour créer la catégorie d'applications.

     Tous les fichiers. Tous les fichiers sont pris en compte lors de la création de la catégorie. Cette option est sélectionnée par défaut.

     Uniquement les fichiers hors des catégories d'applications. Seuls les fichiers hors catégories d'applications sont pris en compte lors de la création de la catégorie.

   - Dossiers

     Dans cette section, vous pouvez spécifier les dossiers de l'appareil (des appareils) sélectionné(s) contenant les fichiers utilisés pour créer la catégorie d'applications.

     Tous les dossiers. Tous les dossiers sont pris en compte pour la catégorie en cours de création. Cette option est sélectionnée par défaut.

     Dossier indiqué. Seul le dossier spécifié est pris en compte pour la catégorie en cours de création. Si vous sélectionnez cette option, vous devez indiquer le chemin d'accès au dossier.

9. Sur la page de l'assistant **Création de la catégorie d'applications**, cliquez sur le bouton **Terminer**.

   Une fois l'Assistant terminé, une catégorie de l'application utilisateur est créée. Vous pouvez consulter la catégorie créée dans la liste des catégories de l'espace de travail du dossier **Catégories d'applications**.

Si vous souhaitez exporter une catégorie d'application vers un fichier KLC, faites un clic droit sur le nom de la catégorie, sélectionnez **Exporter** dans le menu, puis dans la fenêtre qui s'ouvre, précisez le nom du fichier et cliquez sur **Enregistrer**.

Création d'une catégorie d'applications incluant des fichiers exécutables provenant du dossier spécifié

Vous pouvez utiliser des fichiers exécutables provenant d'un dossier sélectionné comme norme de fichiers exécutables que vous souhaitez autoriser ou bloquer dans votre organisation. En vous basant sur les fichiers exécutables provenant du dossier sélectionné, vous pouvez créer une catégorie d'applications et l'utiliser dans la configuration du module Contrôle des applications.

Pour créer une catégorie d'applications incluant des fichiers exécutables provenant du dossier sélectionné :

1. Dans l'arborescence de la console, dans le dossier **Avancé** → **Gestion des applications**, sélectionnez le sous-dossier **Catégories d'applications**.

2. Cliquez sur le bouton **Nouvelle catégorie**.

   L'**Assistant de nouvelle catégorie** démarre. Parcourez les étapes de l'Assistant à l'aide du bouton **Suivant**.

3. Sur la page de l'assistant **Type de catégorie**, sélectionnez **Catégorie qui inclut les fichiers exécutables d'un dossier spécifique** comme type de catégorie d'utilisateurs.

4. Sur la page de l'Assistant **Saisissez le nom de la catégorie d'applications**, saisissez le nom de la nouvelle catégorie d'applications.

5. Sur la page **Dossier de stockage** de l'Assistant, cliquez sur le bouton **Parcourir**.

6. Indiquez le dossier dont les fichiers exécutables seront utilisés pour créer la catégorie d'applications.

7. Configurez les paramètres suivants :

- **Inclure dans la catégorie des bibliothèques connectées de manière dynamique (DLL)**

  Sont intégrées dans la catégorie d'applications les bibliothèques de liens dynamiques (fichiers au format DLL) et le module Contrôle des applications enregistre les actions de ces bibliothèques lancées dans le système. Lors de l'inclusion de fichiers au format DLL dans une catégorie, les performances de Kaspersky Security Center peuvent diminuer.

  Celle-ci est décochée par défaut.

- **Inclure les données relatives aux scripts dans la catégorie**

  Sont intégrées dans la catégorie d'applications les données sur les scripts et les scripts ne sont pas bloqués pas par le module Protection contre les menaces Internet. Lors de l'inclusion des données sur les scripts dans une catégorie, Kaspersky Security Center peut perdre en performance.

  Celle-ci est décochée par défaut.

- **Algorithme de calcul de la fonction hash** : **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) / 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)**

En fonction de la version de l'application de sécurité installée sur les appareils de votre réseau, il faut choisir un algorithme de calcul de la fonction hash par l'application Kaspersky Security Center pour les fichiers de la catégorie. Les informations relatives aux 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 du calcul ne contient pas de vulnérabilités et il est considéré actuellement comme la fonction de chiffrement la plus sûre. Kaspersky Endpoint Security 10 Service Pack 2 for Windows et suivants prennent en charge le calcul de la fonction hash SHA256. Le calcul de la fonction de hach MD5 est pris en charge pour les versions inférieures à Kaspersky Endpoint Security 10 Service Pack 2 for Windows.

Choisissez une des options du calcul de la fonction hash par l'application Kaspersky Security Center pour les fichiers de la catégorie :

- Si toutes les instances des applications de sécurité installées sur votre réseau sont Kaspersky Endpoint Security 10 Service Pack 2 for Windows ou des versions ultérieures, cochez la case **SHA256**. Il est déconseillé d'ajouter une catégorie créée selon le critère du hachage SHA256 du fichier exécutable pour les versions de l'application antérieures à Kaspersky Endpoint Security 10 Service Pack 2 for Windows. Cela pourrait entraîner un échec de l'application de sécurité. 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 Service Pack 2 for Windows sont installées sur votre réseau, sélectionnez **Hash MD5**. Il est interdit d'ajouter une catégorie créée selon le critère de la somme de contrôle MD5 du fichier exécutable pour les versions Kaspersky Endpoint Security 10 Service Pack 2 for Windows et suivantes. Dans ce cas vous pouvez utiliser la fonction de hachage cryptographique SHA256 pour les fichiers de la catégorie.

Si différents appareils de votre réseau utilisent à la fois des versions antérieures et ultérieures de Kaspersky Endpoint Security 10, cochez à la fois la case **SHA256** et la case **Hash MD5**.

La case **Calculer SHA256 pour les fichiers en la catégorie (pris en charge pour Kaspersky Endpoint Security 10 Service Pack 2 for Windows et versions supérieures)** est cochée par défaut.

La case **Calculer MD5 pour les fichiers en la catégorie (pris en charge pour les versions inférieures à Kaspersky Endpoint Security 10 Service Pack 2 for Windows)** est décochée.

- Forcer l'analyse du dossier à la recherche de modifications

Si cette option est activée, l'application effectue régulièrement une analyse forcée du dossier d'ajout de la catégorie pour vérifier la présence de modifications. La fréquence de l'analyse peut être définie en heures dans le champ de saisie situé près de la case. Par défaut, la fréquence des vérifications forcées est de 24 heures.

Si l'option est désactivée, l'application n'imposera pas de vérification du dossier. Le serveur appelle les fichiers du dossier en cas de modification, d'ajout ou de suppression.

Cette option est Inactif par défaut.

8. Sur la page de l'assistant **Création de la catégorie d'applications**, cliquez sur le bouton **Terminer**.

Une fois l'Assistant terminé, une catégorie de l'application utilisateur est créée. Vous pouvez consulter la catégorie créée dans la liste des catégories de l'espace de travail du dossier **Catégories d'applications**.

Si vous souhaitez exporter une catégorie d'application vers un fichier KLC, faites un clic droit sur le nom de la catégorie, sélectionnez **Exporter** dans le menu, puis dans la fenêtre qui s'ouvre, précisez le nom du fichier et cliquez sur **Enregistrer**.

Ajout de fichiers exécutables liés par un événement à la catégorie d'applications

Vous pouvez ajouter des fichiers exécutables liés aux événements **Lancement de l'application interdit** et **Lancement de l'application interdit en mode test** à une catégorie d'applications existante avec un contenu ajouté manuellement, ou à une nouvelle catégorie d'applications.

Pour ajouter des fichiers exécutables liés aux événements de contrôle des applications à la catégorie de l'application :

1. Dans l'arborescence de la console, sélectionnez l'entrée portant le nom du Serveur d'administration requis.
2. Dans l'espace de travail de l'entrée, sélectionnez l'onglet **Événements**.
3. Dans l'onglet **Événements**, sélectionnez les événements souhaités.
4. Dans le menu contextuel de l'événement, sélectionnez l'option **Ajouter dans la catégorie**.

5. Dans la fenêtre **Action sur le fichier exécutable lié à l'événement** qui s'ouvre, définissez les paramètres pertinents :

   Sélectionnez une des options suivantes :

   - **Ajoute une &nouvelle catégorie d'applications**

     Sélectionnez cette option si vous souhaitez créer une nouvelle catégorie d'applications.

     Cliquez sur le bouton **OK** pour lancer l'assistant de nouvelle catégorie. Au terme de l'exécution de l'assistant, une nouvelle catégorie sera créée avec les paramètres indiqués.

     Par défaut, cette option n'est pas sélectionnée.

   - **Ajouter à une &catégorie d'application existante**

     Sélectionnez cette option s'il est nécessaire d'ajouter des règles dans une catégorie d'applications existante. Sélectionnez la catégorie souhaitée dans la liste des catégories d'applications.

     Par défaut, cette option est sélectionnée.

   Dans le groupe **Type de règle**, sélectionnez les paramètres :

   - **Ajouter dans la catégorie**

     Sélectionnez cette option s'il est nécessaire d'ajouter des règles dans les conditions d'une catégorie d'applications.

     Par défaut, cette option est sélectionnée.

   - **Règles pour l'ajout aux &exclusions**

     Sélectionnez cette option si vous souhaitez ajouter des règles dans les exclusions d'une catégorie d'applications.

   Dans le groupe **Type d'informations sur le fichier**, sélectionnez l'un des paramètres :

   - **Détails du certificat (ou hash SHA256 pour les fichiers sans certificat)**

     Les fichiers peuvent être signés par un certificat. De plus un certificat peut signer plusieurs fichiers. Par exemple, différentes versions d'une application peuvent être signées par un certificat ou plusieurs applications différentes d'un même éditeur peuvent être signées par un même certificat. En cas de sélection du certificat, la catégorie peut reprendre plusieurs versions de l'application ou plusieurs applications d'un même éditeur.

     Chaque fichier possède sa propre fonction de hachage SHA256 unique. En cas de sélection de la fonction hash SHA256, la catégorie reprend uniquement un seul fichier correspondant, par exemple, la version définie de l'application.

     Sélectionnez cette option si vous souhaitez ajouter les données du certificat du fichier exécutable (ou la fonction hash SHA256 pour les fichiers sans certificat) aux règles de la catégorie.

     Cette option est sélectionnée par défaut.

   - **Détails du certificat (les fichiers sans certificat sont ignorés)**

Les fichiers peuvent être signés par un certificat. De plus un certificat peut signer plusieurs fichiers. Par exemple, différentes versions d'une application peuvent être signées par un certificat ou plusieurs applications différentes d'un même éditeur peuvent être signées par un même certificat. En cas de sélection du certificat, la catégorie peut reprendre plusieurs versions de l'application ou plusieurs applications d'un même éditeur.

Sélectionnez cette option si vous souhaitez ajouter les données du certificat du fichier exécutable aux règles de la catégorie. Si le fichier exécutable n'a pas de certificat, ce fichier sera ignoré. Les informations le concernant ne seront pas ajoutées dans la catégorie.

- **Uniquement SHA256 (les fichiers sans hachage seront ignorés)**

  Chaque fichier possède sa propre fonction de hachage SHA256 unique. En cas de sélection de la fonction hash SHA256, la catégorie reprend uniquement un seul fichier correspondant, par exemple, la version définie de l'application.

  Sélectionnez cette option si vous souhaitez ajouter uniquement les données de la fonction hash SHA256 du fichier exécutable.

- **MD5 (mode obsolète, seulement pour les versions Kaspersky Endpoint Security 10 Service Pack 1)**

  Chaque fichier possède sa propre fonction de hachage MD5 unique. En cas de sélection de la fonction hash MD5, la catégorie reprend uniquement un seul fichier correspondant, par exemple, la version définie de l'application.

  Sélectionnez cette option si vous souhaitez ajouter uniquement les données de la fonction hash MD5 du fichier exécutable. Le calcul de la fonction de hachage MD5 est pris en charge pour les versions inférieures à Kaspersky Endpoint Security 10 Service Pack 1 for Windows.

6. Cliquez sur le bouton **OK**.

Configuration d'administration du lancement des applications sur les appareils clients

La catégorisation des applications permet d'optimiser le processus d'administration du lancement des applications sur les appareils. Vous pouvez créer une catégorie d'applications et configurer le module Contrôle des applications de la stratégie de telle sorte que seules les applications de la catégories indiquées soient lancées sur les appareils soumis à cette stratégie. Admettons que vous avez créé une catégorie qui contient les applications *Application_1* et *Application_2*. Quand vous ajoutez cette catégorie à une stratégie, seules les applications *Application_1* et *Application_2* peuvent être lancées sur les appareils soumis à cette stratégie. Si l'utilisateur tente de lancer une application qui n'appartient pas à la catégorie, par exemple *Application_3*, le lancement de cette application est bloqué. Un message signale alors à l'utilisateur que le lancement d'*Application_3* est bloqué conformément à la règle de Contrôle des applications. Vous pouvez créer des catégories à remplissage automatique sur la base de différents critères repris dans le dossier indiqué. Dans ce cas, les fichiers sont ajoutés automatiquement à la catégorie depuis le dossier indiqué. Les fichiers exécutables des applications sont copiés dans le dossier indiqué, sont traités automatiquement et leurs données métriques sont ajoutées à la catégorie.

Pour configurer l'administration du lancement des applications sur les appareils clients, procédez comme suit :

1. Dans le dossier **Avancé** → **Gestion des applications** de l'arborescence de la console, sélectionnez le sous-dossier **Catégories d'applications**.

2. Dans l'espace de travail du dossier **Catégories d'applications**, créez une catégorie d'applications que vous voulez administrer pendant leur lancement.

3. Dans le dossier **Appareils administrés**, sur l'onglet **Stratégies**, cliquez sur le bouton **Nouvelle stratégie** pour créer une nouvelle stratégie pour Kaspersky Endpoint Security for Windows, et suivez les instructions de l'Assistant.

   Si une telle stratégie déjà existe, cette étape peut être ignorée. L'administration du lancement des applications dans la catégorie indiquée peut être configurée dans les paramètres de cette stratégie. La stratégie créée s'affiche dans le dossier **Appareils administrés**, sous l'onglet **Stratégies**.

4. Dans le menu contextuel de la stratégie de l'application Kaspersky Endpoint Security for Windows, sélectionnez l'option **Propriétés**.

   La fenêtre des propriétés de la stratégie de Kaspersky Endpoint Security for Windows s'ouvre.

5. Dans la fenêtre des propriétés de la stratégie de Kaspersky Endpoint Security for Windows, **Contrôle de sécurité** → section **Contrôle des applications**, cochez la case **Contrôle des applications**.

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

   La fenêtre **Règle de contrôle des applications** s'ouvre.

7. Dans la fenêtre **Règle de contrôle des applications** dans la liste déroulante **Catégorie**, sélectionnez la catégorie d'applications pour laquelle la règle du lancement sera diffusée. Configurez les paramètres de la règle du lancement pour la catégorie d'applications sélectionnées.

   Pour les versions de Kaspersky Endpoint Security 10 Service Pack 2 et suivantes, les catégories créées selon le critère du hash MD5 du fichier exécutable de l'application ne sont pas affichées.

   Il est déconseillé d'ajouter une catégorie créée selon le critère du hachage SHA256 du fichier exécutable pour les versions de l'application antérieures à Kaspersky Endpoint Security 10 Service Pack 2. Cela pourrait entraîner un échec de l'application.

   Les instructions détaillées pour la configuration des règles de contrôle figurent dans l'Aide en ligne de Kaspersky Endpoint Security for Windows.

8. Cliquez sur le bouton **OK**.

Le lancement des applications sur les appareils qui font partie de la catégorie indiquée sera exécuté conformément à la règle créée. La règle créée s'affiche dans la fenêtre des propriétés de la stratégie de Kaspersky Endpoint Security for Windows dans la section **Contrôle des applications**.

Consultation des résultats de l'analyse statique des règles de lancement des fichiers exécutables

Pour consulter les informations sur le lancement des fichiers exécutables interdits par l'utilisateur, procédez comme suit :

1. Dans l'arborescence de la console du dossier **Appareils administrés**, sélectionnez l'onglet **Stratégies**.
2. Dans le menu contextuel de la stratégie de l'application Kaspersky Endpoint Security for Windows, sélectionnez l'option **Propriétés**.

   La fenêtre des propriétés de la stratégie de l'application s'ouvre.
3. Dans le volet **Sections**, sélectionnez **Contrôles de sécurité**, puis sélectionnez la sous-section **Contrôle des applications**.
4. Cliquez sur le bouton **Analyse statique**.

   La fenêtre **Analyse de la liste des privilèges d'accès** s'ouvre. Dans la partie gauche de la fenêtre, une liste d'utilisateurs basée sur les données Active Directory s'affiche.
5. Sélectionnez l'utilisateur dans la liste.

   La partie droite de la fenêtre affichera les catégories d'applications désignées à cet utilisateur.
6. Pour consulter les fichiers exécutables dont le lancement par l'utilisateur est interdit, dans la fenêtre **Analyse de la liste des privilèges d'accès**, cliquez sur le bouton **Consulter les fichiers**.

   La fenêtre s'ouvre. Cette fenêtre affiche la liste des fichiers exécutables dont le lancement est interdit par l'utilisateur.
7. Pour consulter la liste des fichiers exécutables qui font partie d'une catégorie, sélectionnez la catégorie d'applications et cliquez sur le bouton **Consulter les fichiers de la catégorie**.

   La fenêtre s'ouvre, affiche la liste des fichiers exécutables qui font partie de la catégorie d'applications.

Affichage du registre des applications

Kaspersky Security Center procède à l'inventaire de l'ensemble des logiciels installés sur des appareils administrés.

L'Agent d'administration compile une liste des applications installées sur un appareil Windows ou Linux, puis transmet cette liste au Serveur d'administration. Pour les appareils clients Windows, l'Agent d'administration reçoit la plupart des informations sur les applications installées à partir du registre Windows. Pour les appareils clients Linux, les gestionnaires de paquets fournissent à l'Agent d'administration des informations sur les applications installées.

Pour consulter le registre des applications installées sur les appareils clients,

Dans le dossier **Avancé** → **Gestion des applications** de l'arborescence de la console, sélectionnez le sous-dossier **Registre des applications**.

L'espace de travail du dossier **Registre des applications** affiche une liste des applications installées sur les appareils client et le Serveur d'administration.

Vous pouvez consulter les informations détaillées concernant une application en sélectionnant dans le menu contextuel de cette application l'option **Propriétés**. La fenêtre des propriétés de l'application affiche les informations générales sur l'application et les informations sur les fichiers exécutables de l'application, ainsi que la liste des appareils sur lesquels l'application est installée.

Dans le menu contextuel de chaque application de la liste, vous pouvez:

- Ajouter cette application à une catégorie d'applications.
- Attribuer une balise à l'application.
- Exporter la liste des applications dans un fichier CSV ou TXT.
- Afficher les propriétés de l'application, par exemple, le nom du fournisseur, le numéro de version, la liste des fichiers exécutables, la liste des appareils sur lesquels l'application est installée, la liste des mises à jour logicielles disponibles ou la liste des vulnérabilités logicielles détectées.

Pour consulter les applications qui satisfont les critères définis, vous pouvez utiliser les champs de filtrage dans l'espace de travail du dossier **Registre des applications**.

Dans la fenêtre des propriétés de l'appareil sélectionné, dans la section **Registre des applications**, vous pouvez consulter la liste des applications installées sur l'appareil.

Générer un rapport sur les applications installées

Dans l'espace de travail **Registre des applications**, vous pouvez également cliquer sur le bouton **Consulter le rapport sur les applications installées** pour générer un rapport contenant des statistiques détaillées sur les applications installées, y compris le nombre d'appareils sur lesquels chaque application est installée. Ce rapport, qui s'ouvre sur la page **Rapport sur les applications installées**, contient des informations sur les applications de Kaspersky et les logiciels tiers. Si vous voulez des informations uniquement sur les applications Kaspersky installées sur des appareils clients, dans la liste **Résumé**, sélectionnez AO Kaspersky.

Les informations relatives aux applications de Kaspersky et d'autres éditeurs sur les appareils connectés aux Serveurs d'administration secondaires et virtuels sont également enregistrées dans le registre des applications du Serveur d'administration principal. Une fois que vous avez ajouté des données des Serveurs d'administration secondaires et virtuels, cliquez sur le bouton **Consulter le rapport sur les applications installées** et, sur la page **Rapport sur les applications installées** qui apparaît, vous pouvez consulter ces informations.

Pour ajouter des informations issues des serveurs d'administration secondaires et virtuels au rapport sur les applications installées :

1. Dans l'arborescence de la console, sélectionnez l'entrée portant le nom du Serveur d'administration requis.
2. Dans l'espace de travail de l'entrée, sélectionnez l'onglet **Rapports**.
3. Dans l'onglet **Rapports**, sélectionnez **Rapport sur les applications installées**.
4. Dans le menu contextuel du rapport, sélectionnez l'option **Propriétés**.

   La fenêtre **Propriétés : Rapport sur les applications installées** s'ouvre.
5. Dans la section **Hiérarchie des Serveurs d'administration**, cochez la case **&Inclure les données à partir des Serveurs d'administration secondaires et virtuels**.
6. Cliquez sur le bouton **OK**.

Les informations issues des Serveurs d'administration virtuels et secondaires seront alors incluses dans le **Rapport sur les applications installées**.

Modification de l'heure de début de l'inventaire logiciel

Kaspersky Security Center procède à l'inventaire de l'ensemble des logiciels installés sur les appareils clients administrés exploitation Windows.

L'Agent d'administration constitue une liste des applications installées sur l'appareil et la transmet au Serveur d'administration. L'Agent d'administration reçoit automatiquement des informations sur les applications installées du registre Windows.

Pour enregistrer les ressources de l'appareil, par défaut, l'Agent d'administration comment à recevoir des informations sur les applications installées 10 minutes après le lancement de son service.

Pour changer l'heure de lancement de l'inventaire logiciel, qui s'écoule après l'exécution du service de l'Agent d'administration sur un appareil :

1. Ouvrez le registre système de l'appareil sur lequel l'Agent d'administration est installé, par exemple, à l'aide de la commande regedit dans le menu **Démarrer** → **Exécuter**.
2. Rendez-vous dans la section :
   - Pour les systèmes 32 bits :
     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1103\1.0.0.0\NagentFlags
   - Pour les systèmes 64 bits :
     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1103\1.0.0.0\NagentF
3. Pour la clé KLINV_INV_COLLECTOR_START_DELAY_SEC, cochez la valeur de votre choix en secondes.
   La valeur par défaut est égale à 600 secondes.
4. Relancez le service de l'Agent d'administration.

L'heure de lancement de l'inventaire logiciel, qui s'écoule après l'exécution du service de l'Agent d'administration, est modifiée.

À propos de la gestion des clés de licence d'applications tierces

Kaspersky Security Center vous permet de suivre l'utilisation des clés de licence pour les applications tierces installées sur les appareils administrés. La liste des applications pour lesquelles vous pouvez suivre l'utilisation des clés de licence est extraite du registre des applications. Pour chaque clé de licence, vous pouvez définir et suivre le non-respect des restrictions suivantes :

- Nombre d'appareils sur lesquels l'application, utilisant cette clé de licence, peut être installée
- Date d'expiration de la durée de validité de la clé de licence

Kaspersky Security Center ne vérifie pas si vous définissez une clé de licence réelle. Vous ne pouvez suivre que les restrictions que vous définissez. Si l'une des restrictions que vous imposez à une clé de licence n'est pas respectée, le Serveur d'administration enregistre un événement d'information, d'avertissement ou d'erreur de fonctionnement.

Les clés de licence sont liées à des groupes d'applications. Un groupe d'applications est un groupe d'applications tierces que vous combinez en fonction d'un ou de plusieurs critères. Vous pouvez définir les applications par le nom de l'application, sa version, son fournisseur et sa balise. Une application est ajoutée au groupe si au moins un des critères est rempli. Pour chaque groupe d'applications, vous pouvez lier plusieurs clés de licence, mais chaque clé de licence ne peut être liée qu'à un seul groupe d'applications.

Un autre outil que vous pouvez utiliser pour suivre l'utilisation des clés de licence est le rapport sur l'état des groupes des applications sous licence. Ce rapport fournit des informations sur l'état actuel des groupes des applications sous licence, y compris ce qui suit :

- Nombre d'installations de clés de licence sur chaque groupe d'applications
- Nombre de clés de licence utilisées et clés de licence vacantes
- Liste détaillée des applications sous licence installées sur les appareils administrés

Les outils d'administration des clés de licence d'applications tierces se trouvent dans le sous-dossier **Utilisation des licences tierces** (**Avancé** → **Gestion des applications** → **Utilisation des licences tierces**). Dans ce sous-dossier, vous pouvez créer des groupes d'applications, ajouter des clés de licence et générer le rapport sur les états des groupes des applications sous licence.

Les outils de gestion des clés de licence des applications tierces ne sont disponibles que si vous avez activé l'option Gestion des vulnérabilités et des correctifs dans la fenêtre **Configure interface**.

Création des groupes des applications sous licence

Pour créer un groupe des applications sous licence, procédez comme suit :

1. Dans le dossier **Avancé** → **Gestion des applications** de l'arborescence de la console, sélectionnez le sous-dossier **Utilisation des licences tierces**.
2. Cliquez sur le bouton **Ajouter un groupe des applications sous licence** pour exécuter l'Assistant d'ajout du groupe des applications sous licence.

   L'Assistant d'ajout du groupe des applications sous licence démarre.

3. À l'étape **Informations sur le groupe des applications sous licence**, indiquez les applications que vous souhaitez inclure dans le groupe des applications :

   - **Nom du groupe des applications sous licence**

   - **Suivre la violation des restrictions**

     Si l'une des restrictions que vous imposez à une clé de licence du groupe d'applications n'est pas respectée, le Serveur d'administration enregistre un événement d'information, d'avertissement ou d'erreur de fonctionnement :

     - Événement d'information : **Pour un des groupes des applications sous licence, le nombre d'installations autorisées est épuisé à plus de 95 %**
     - Événement d'avertissement : **La limite des installations sera bientôt dépassée pour l'un des groupes d'applications sous licence**
     - Événement d'erreur de fonctionnement : **Pour un des groupes des applications sous licence, la limite des installations a été dépassée**

       Un événement n'est enregistré qu'une seule fois, lorsque la condition énoncée est remplie. La prochaine fois, le même événement ne peut être enregistré que lorsque le nombre d'installations est revenu à un niveau normal, puis l'événement se reproduit. Un événement ne peut pas être enregistré plus d'une fois par heure.

   - **Critères d'ajout des application détectées dans ce groupe des applications sous licence**

     Précisez les critères permettant de définir les applications que vous souhaitez inclure dans le groupe d'applications. Vous pouvez définir les applications par le nom de l'application, sa version, son fournisseur et sa balise. Vous devez définir au moins un critère. Une application est ajoutée au groupe si au moins un des critères est rempli.

4. À l'étape **Saisissez les données sur les clés de licence existantes**, indiquez les clés de licence que vous souhaitez suivre. Sélectionnez l'option **Contrôler la violation des restrictions définies de la licence**, puis ajoutez les clés de licence :

   a. Cliquez sur le bouton **Ajouter**.

   b. Sélectionnez la clé de licence que vous souhaitez ajouter, puis cliquez sur le bouton **OK**. Si la clé de licence requise ne figure pas dans la liste, cliquez sur le bouton **Ajouter**, puis définissez les propriétés de la clé de licence.

5. À l'étape **Ajout d'un groupe des applications sous licence**, cliquez sur le bouton **Terminer**.

Un groupe des applications sous licence est créé. Ce groupe s'affiche dans le dossier **Utilisation des licences tierces**.

Gestion des clés de licence pour les groupes des applications sous licence

Pour créer une clé de licence pour le groupe des applications sous licence, procédez comme suit :

1. Dans le dossier **Avancé** → **Gestion des applications** de l'arborescence de la console, sélectionnez le sous-dossier **Utilisation des licences tierces**.

2. Dans l'espace de travail du dossier **Utilisation des licences tierces**, cliquez sur le bouton **Administrer les clés de licence des applications sous licence**.

   La fenêtre **Administration des clés de licence des applications sous licence** s'ouvre.

3. Dans la fenêtre **Administration des clés de licence des applications sous licence**, cliquez sur le bouton **Ajouter**.

   Le fenêtre **Clé de licence** s'ouvre.

4. Dans la fenêtre **Clé de licence**, indiquez les propriétés de la clé de licence et les restrictions que cette clé de licence impose sur le groupe des applications sous licence.

   - **Nom**. Le nom de la clé de licence.
   - **Commentaires**. Les remarques de la clé de licence sélectionnée.
   - **Restriction**. Le nombre d'appareils sur lesquels l'application, utilisant cette clé de licence, peut être installée.
   - **Date d'ex&piration**. La date d'expiration de la durée de validité de la clé de licence.

Les clés de licence créées sont affichées dans la fenêtre **Administration des clés de licence des applications sous licence**.

Pour appliquer une clé de licence au groupe des applications sous licence, procédez comme suit :

1. Dans le dossier **Avancé** → **Gestion des applications** de l'arborescence de la console, sélectionnez le sous-dossier **Utilisation des licences tierces**.

2. Dans le dossier **Utilisation des licences tierces**, sélectionnez le groupe des applications sous licence auquel vous souhaitez appliquer une clé de licence.

3. Dans le menu contextuel du groupe des applications sous licence, sélectionnez l'option **Propriétés**.

   La fenêtre des propriétés du groupe des applications sous licence s'ouvre.

4. Dans la fenêtre des propriétés du groupe des applications sous licence, dans la section **Clés de licence**, sélectionnez l'option **Contrôler la violation des restrictions définies de la licence**.

5. Cliquez sur le bouton **Ajouter**.

   La fenêtre **Sélection de la clé de licence** s'ouvre.

6. Dans la fenêtre **Sélection de la clé de licence**, sélectionnez la clé de licence que vous voulez appliquer au groupe des applications sous licence.

7. Cliquez sur le bouton **OK**.

Les restrictions pour le groupe des applications sous licence indiquées dans la clé de licence seront diffusées sur le groupe des applications sous licence sélectionné.

Inventaire des fichiers exécutables

Vous pouvez obtenir une liste des fichiers exécutables stockés sur les appareils administrés. Pour répertorier les fichiers exécutables, vous devrez créer une tâche d'inventaire.

La fonction d'inventaire des fichiers exécutables est disponible pour les applications suivantes :

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Linux
- Kaspersky Security for Virtualization 4.0 Light Agent et versions ultérieures

Le nombre de fichiers exécutables reçus d'un appareil ne peut pas dépasser 150 000. Une fois cette limite atteinte, Kaspersky Security Center ne peut plus accepter de nouveaux fichiers.

Avant de commencer, activez les notifications de lancement des applications dans la stratégie de Kaspersky Endpoint Security et dans la stratégie de l'Agent d'administration, afin de pouvoir transférer les données vers le Serveur d'administration.

Pour activer les notifications relatives au démarrage des applications, procédez comme suit :

- Ouvrez les paramètres de la stratégie de Kaspersky Endpoint Security et procédez comme suit :
  1. Accédez à **Paramètres généraux → Rapports et stockage**.
  2. Dans la section **Transfert des données vers le Serveur d'administration**, cochez la case **À propos des applications lancées**.
  3. Enregistrez vos modifications.
- Ouvrez les paramètres de stratégie de l'Agent d'administration et procédez comme suit :
  1. Passer à la section **Stockages**.
  2. Cochez la case **Détails sur les applications installées**.
  3. Enregistrez vos modifications.

Pour créer une tâche d'inventaire des fichiers exécutables sur les appareils clients, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le dossier **Tâches**.
2. Dans l'espace de travail du dossier **Tâches**, cliquez sur le bouton **Nouvelle tâche**.

   Ceci permet de lancer l'Assistant de création d'une tâche.

3. Dans la fenêtre **Sélection du type de tâche** de l'Assistant, sélectionnez **Kaspersky Endpoint Security** comme type de tâche, puis sélectionnez le sous-type de tâche **Inventaire**, et cliquez sur **Suivant**.

4. Suivez les étapes ultérieures de l'assistant.

   Suite à l'exécution de l'Assistant, une tâche d'inventaire est créée pour Kaspersky Endpoint Security. La tâche créée est affichée dans la liste de tâches de l'espace de travail du dossier **Tâches**.

Suite à l'exécution de l'inventaire, la liste des fichiers exécutables détectés sur les appareils s'affiche dans l'espace de travail **Fichiers exécutables**.

Pendant l'exécution de l'inventaire, l'application détecte les fichiers exécutables des formats suivants : MZ, COM, PE, NE, SYS, CMD, BAT, PS1, JS, VBS, REG, MSI, CPL, DLL, JAR, ainsi que les fichiers HTML.

Consultation des informations sur les fichiers exécutables

Pour consulter la liste de tous les fichiers exécutables détectés sur les appareils clients,

Dans l'arborescence de la console du dossier **Gestion des applications**, sélectionnez le sous-dossier **Fichiers exécutables**.

L'espace de travail du dossier **Fichiers exécutables** affiche la liste des fichiers exécutables qui ont été lancés sur les appareils ou qui ont été détectés pendant le fonctionnement de la tâche d'inventaire de Kaspersky Endpoint Security for Windows.

Pour consulter les données sur les fichiers exécutables qui satisfont les critères définis, vous pouvez utiliser le filtrage.

Pour consulter les propriétés du fichier exécutable,

Dans le menu contextuel du fichier, sélectionnez l'option **Propriétés**.

La fenêtre qui contient les informations sur le fichier exécutable s'ouvre, ainsi que la liste des appareils sur lesquels le fichier exécutable est présent.

Surveillance et rapports

Cette section décrit les capacités de surveillance et d'élaboration de rapports de Kaspersky Security Center. Ces capacités offrent un aperçu de votre infrastructure, des états de la protection et des statistiques.

Une fois Kaspersky Security Center déployé, ou pendant l'opération de déploiement, vous pouvez configurer les fonctions de surveillance et de création de rapports répondant le mieux à vos besoins.

- **Indicateurs de couleur**

  La Console d'administration permet d'évaluer rapidement l'état actuel de Kaspersky Security Center et des appareils administrés grâce à des indicateurs de couleur.

- **Statistiques**

Les statistiques sur l'état du système de protection et des appareils administrés apparaissent dans des panneaux d'informations personnalisables.

- **Rapports**

  Les rapports permettent d'obtenir des informations numériques détaillées sur la sécurité du réseau de votre organisation, d'enregistrer ces informations dans un fichier, de les envoyer par email et les imprimer.

- **Événements**

  Sélections d'événements fournissent une vue à l'écran d'ensembles d'événements nommés stockés dans la base de données du Serveur d'administration. Ces ensembles d'événements sont regroupés selon les catégories suivantes :

  - Par niveau d'importance — **Événements critiques**, **Erreurs de fonctionnement**, **Avertissements** et **Événements d'information**
  - Chronologiquement — **Derniers événements**
  - Par type — **Requêtes des utilisateurs** et **Événements de l'audit**

Vous pouvez créer et voir les sélections d'événements définies par l'utilisateur sur la base des paramètres disponibles, dans l'interface de Kaspersky Security Center Web Console pour configuration.

Scénario : Surveillance et rapports

Cette section fournit un scénario pou configurer la fonction de surveillance et de création de rapports dans Kaspersky Security Center.

Prérequis

Une fois que vous avez déployé Kaspersky Security Center sur le réseau d'une entreprise, vous pouvez commencer à le surveiller et obtenir des rapports opérationnels.

Étapes

La surveillance et la création de rapports dans le réseau d'une organisation se déroulent par étapes :

1. **Configuration de la permutation des états des appareils**

   Familiarisez-vous avec les paramètres qui définissent l'attribution des états des appareils en fonction de conditions spécifiques. En changeant ces paramètres, vous pouvez changer le nombre d'événements de niveau *Critique* ou *Avertissement*.

   Lors de la configuration du changement d'état des appareils, assurez-vous que les nouveaux paramètres n'entrent pas en conflit avec les stratégies de sécurité des informations de votre organisation et que vous êtes en mesure de réagir en temps utile aux événements de sécurité importants sur le réseau de votre organisation.

2. **Configuration des notifications sur les événements survenus sur les appareils clients :**

   Configurez la notification (par email, par SMS ou en exécutant un fichier exécutable) d'événements sur les appareils clients, en fonction des besoins de votre organisation.

3. **Modification de la réaction de votre réseau de sécurité à l'événement Attaque de virus**

Pour régler la réponse du réseau aux nouveaux événements, vous pouvez modifier les seuils spécifiques dans les propriétés du Serveur d'administration. Vous pouvez également créer une stratégie plus stricte qui sera activée ou créer une tâche qui sera exécutée quand l'événement se produira.

4. **Utilisation des données statistiques**

   Configurez l'affichage des statistiques en fonction des besoins de votre organisation.

5. **Vérification de l'état de la sécurité du réseau de votre organisation**

   Pour examiner l'état de sécurité du réseau de votre organisation, vous pouvez effectuer l'une des opérations suivantes :

   - Dans l'espace de travail du nœud **Serveur d'administration**, sous l'onglet **Statistiques**, ouvrez l'onglet de deuxième niveau (page) **État de la protection** et examinez le panneau d'informations **État de la protection en temps réel**
   - Générer et examiner **Rapport sur l'état de la protection**
   - Générer et examiner **Rapport sur les erreurs**

6. **Localisation des appareils clients non protégés**

   Pour localiser les appareils clients qui ne sont pas protégés, accédez à l'espace de travail du nœud **Serveur d'administration**, sous l'onglet **Statistiques**, ouvrez l'onglet de deuxième niveau (page) **État de la protection** et examinez le panneau d'informations **Historique de découverte de nouveaux appareils sur le réseau**. Vous pouvez aussi générer et examiner **Rapport sur le déploiement de la protection**.

7. **Vérification de la protection des appareils clients**

   Pour vérifier la protection des appareils clients, accédez à l'espace de travail du nœud **Serveur d'administration**, sous l'onglet **Statistiques**, ouvrez l'onglet de deuxième niveau (page) **Déploiement** ou **Statistiques des menaces**, et examinez les panneaux d'information appropriés. Vous pouvez aussi commencer et examiner la sélection d'événements **Événements critiques**.

8. **Évaluation et limitation de la charge d'événements sur la base de données.**

   Les informations sur les événements qui se produisent pendant le fonctionnement des applications administrées sont transmises de l'appareil client et enregistrées dans la base de données du Serveur d'administration. Pour réduire la charge sur le Serveur d'administration, évaluez et limitez le nombre maximal d'événements stockables dans la base de données.

   Pour évaluer la charge d'événements sur la base de données, calculez l'espace de la base de données. Vous pouvez aussi limiter le nombre maximum d'événements pour éviter le débordement de la base de données.

9. **Contrôle des informations de licence**

   Pour consulter les informations de licence, accédez à l'espace de travail du nœud **Serveur d'administration**, sous l'onglet **Statistiques**, ouvrez l'onglet de deuxième niveau (page) **Déploiement** et examinez le panneau d'informations **Utilisation de la clé de licence**. Vous pouvez aussi générer et examiner **Rapport sur les clés de licence utilisées**.

Résultats

Une fois le scénario terminé, vous êtes informé de la protection du réseau de votre organisation et pouvez donc planifier des actions pour renforcer la protection.

Surveillance des indicateurs de couleur et des événements consignés dans la Console d'administration

La Console d'administration permet d'évaluer rapidement l'état actuel de Kaspersky Security Center et des appareils administrés grâce à des indicateurs de couleur. Les indicateurs s'affichent dans l'espace de travail de l'entrée **Serveur d'administration** sous l'onglet **Surveillance**. L'onglet affiche six panneaux d'information avec des indicateurs de couleur et les événements enregistrés. Un feu de circulation est une barre verticale colorée sur le côté gauche d'un panneau. Chaque bloc avec un indicateur est consacré à une zone fonctionnelle distincte de Kaspersky Security Center (cf. le tableau ci-dessous).

Zones de responsabilité des indicateurs de couleur dans la Console d'administration

Nom du panneau	Zone de responsabilité de l'indicateur de couleur
Déploiement	Installation de l'Agent d'administration et des applications de sécurité sur les appareils du réseau de l'organisation
Structure d'administration	Structure des groupes d'administration. Sondage de réseau. Règles de déplacement des appareils
Configuration de la protection	Fonctions de l'application de sécurité : état de la protection, analyse des logiciels malveillants
Mise à jour	Mises à jour et correctifs
Surveillance	État de la protection
Serveur d'administration	Fonctions et propriétés du Serveur d'administration

L'indicateur peut être une des cinq couleurs suivantes (cf. le tableau ci-après). La couleur de l'indicateur dépend de l'état actuel de Kaspersky Security Center et des événements enregistrés.

Codes couleur des indicateurs

État	Couleur de l'indicateur	Valeur de la couleur de l'indicateur
Pour information	Vert	L'intervention de l'administrateur n'est pas requise
Avertissement	Jaune	L'intervention de l'administrateur est requise.
Critique	Rouge	Des problèmes importants sont survenus. Leur résolution requiert l'intervention de l'administrateur.
Pour information	Bleu	Enregistrement d'événements non liés à des menaces potentielles ou réelles pour la sécurité des appareils administrés.
Pour information	Gris	Les détails relatifs aux événements ne sont pas disponibles ou n'ont pas encore été récupérés.

L'objectif de l'administrateur est que les témoins de couleur sur tous les panneaux d'informations de l'onglet **Surveillance** soient verts.

Le panneau d'informations affiche également les événements enregistrés ayant un impact sur l'indicateur et l'état de Kaspersky Security Center (cf. le tableau ci-dessous).

Nom, description et couleurs des indicateurs de couleur des événements enregistrés

Couleur de l'indicateur	Nom affiché du type d'événement	Type d'événement	Description
Rouge	**La licence a expiré sur %1 appareil(s)**	IDS_AK_STATUS_LIC_EXPAIRED	Des événements de ce type se produisent lorsque la licence commerciale a expiré. Une fois par jour, Kaspersky Security Center vérifie si la licence n'a pas expiré sur les appareils. À l'expiration de la licence commerciale, Kaspersky Security Center ne fournit que les fonctionnalités de base. Pour continuer à utiliser Kaspersky Security Center, renouvelez la licence commerciale.
Rouge	**Application de sécurité désactivée : %1 appareils**	IDS_AK_STATUS_AV_NOT_RUNNING	Des événements de ce type se produisent lorsque l'application de sécurité installée sur l'appareil ne fonctionne pas. Assurez-vous que Kaspersky Endpoint Security est exécuté sur l'appareil.
Rouge	**La protection n'est pas lancée : %1 appareils**	IDS_AK_STATUS_RTP_NOT_RUNNING	Des événements de ce type se produisent lorsque l'application de sécurité sur l'appareil est désactivée pendant plus longtemps que la durée indiquée. Vérifiez l'état actuel de la protection en temps réel sur l'appareil et assurez-vous que tous les modules de protection dont vous avez besoin sont activés.
Rouge	**Une vulnérabilité a été découverte dans les applications des appareils**	IDS_AK_STATUS_VULNERABILITIES_FOUND	Des événements de ce type se produisent lorsque la tâche *Recherche de vulnérabilités et de mises à jour requises* a détecté des vulnérabilités avec le niveau de gravité indiqué dans les applications installées sur l'appareil. Consultez la liste des mises à jour disponibles dans le sous-dossier **Mises à jour du logiciel** inclus dans le dossier **Gestion des applications**. Ce dossier contient la liste des mises à jour obtenues par le Serveur d'administration des applications de Microsoft et d'autres éditeurs du logiciel qui peuvent être diffusées sur les appareils. Après la consultation des informations sur les mises à jour disponibles, installez-les sur l'appareil.
Rouge	**Des événements critiques ont été enregistrés sur le Serveur d'administration**	IDS_AK_STATUS_EVENTS_OCCURED	Les événements de ce type se produisent en cas d'événements critiques du Serveur d'administration détectés. Consultez la liste des événements enregistrée sur le Serveur d'administration, puis corrigez les événements critiques un par un.
Rouge	**Des erreurs ont été enregistrées dans des événements sur le Serveur d'administration**	IDS_AK_STATUS_ERROR_EVENTS_OCCURED	Des événements de ce type se produisent lorsque des erreurs inattendues sont enregistrées du côté du Serveur d'administration. Consultez la liste des événements enregistrée sur le Serveur d'administration, puis corrigez les erreurs une par une.
Rouge	**La connexion avec %1 appareils est perdue**	IDS_AK_STATUS_ADM_LOST_CONTROL1	Des événements de ce type se produisent lorsque la connexion entre le Serveur d'administration et l'appareil est perdue. Consultez la liste des appareils déconnectés et essayez de les reconnecter.

Couleur de l'indicateur	Nom affiché du type d'événement	Type d'événement	Description
Rouge	**%1 appareil(s) n'ont pas connecté(s) au Serveur d'administration depuis longtemps**	IDS_AK_STATUS_ADM_NOT_CONNECTED1	Des événements de ce type se produisent lorsque l'appareil ne s'est pas connecté au Serveur d'administration dans l'intervalle de temps indiqué, car l'appareil était éteint. Assurez-vous que l'appareil est sous tension et que l'Agent d'administration est en cours d'exécution.
Rouge	**Il existe %1 appareils avec l'état différent de OK**	IDS_AK_STATUS_HOST_NOT_OK	Des événements de ce type se produisent lorsque l'état *OK* de l'appareil connecté au Serveur d'administration devient *Critique* ou *Avertissement*. Vous pouvez résoudre le problème à l'aide de l'utilitaire de diagnostic à distance de Kaspersky Security Center.
Rouge	**Les bases sont dépassées sur : %1 appareil(s)**	IDS_AK_STATUS_UPD_HOSTS_NOT_UPDATED	Des événements de ce type se produisent lorsque les bases antivirus n'ont pas été mises à jour sur l'appareil dans les intervalles de temps indiqués. Suivez les instructions pour mettre à jour les bases de Kaspersky.
Rouge	**Appareil(s) sur lesquels la vérification des mises à jour Windows Update n'a pas été effectuée depuis longtemps : %1**	IDS_AK_STATUS_WUA_DATA_OBSOLETE	Des événements de ce type se produisent lorsque la tâche *Synchronisation des mises à jour Windows Update* n'a pas été exécutée dans l'intervalle de temps spécifié. Suivez les instructions pour synchroniser les mises à jour de Windows Update avec le Serveur d'administration.
Rouge	**L'installation de %1 plug-in(s) pour Kaspersky Security Center est requise**	IDS_AK_STATUS_PLUGINS_REQUIRED2	Des événements de ce type se produisent lorsque vous devez installer des plug-ins supplémentaires pour les applications de Kaspersky. Téléchargez et installez les plug-ins d'administration de l'application Kaspersky nécessaires à partir du site du Support Technique de Kaspersky.

Utilisation des rapports, des statistiques et des notifications

Cette section reprend les informations sur l'utilisation des rapports, les statistiques et les sélections d'événements et d'appareils dans Kaspersky Security Center, ainsi que sur la configuration des notifications du Serveur d'administration.

Utilisation des rapports

Les rapports dans Kaspersky Security Center contiennent les informations sur l'état des appareils administrés. Les rapports se forment à partir des informations enregistrées sur le Serveur d'administration. Vous pouvez créer les rapports pour les objets suivants :

- Pour les sélections d'appareils créés selon des paramètres définis.
- Pour les groupes d'administration.
- Pour les ensembles d'appareils issus de divers groupes d'administration.
- Pour tous les appareils dans le réseau (dans le rapport de déploiement).

L'application comporte un ensemble de modèles standard de rapport. La possibilité de créer des modèles de rapports d'utilisateurs. Les rapports s'affichent dans la fenêtre principale de l'application, dans le dossier de l'arborescence de la console **Serveur d'administration**.

Créer le nouveau rapport

Pour créer un modèle de rapport, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez l'entrée portant le nom du Serveur d'administration requis.
2. Dans l'espace de travail de l'entrée, sélectionnez l'onglet **Rapports**.
3. Cliquez sur le bouton **Nouveau modèle de rapport**.

Finalement, l'Assistant de création du modèle du rapport se lancera. Suivez les instructions de l'assistant.

A la fin du fonctionnement de l'Assistant, le modèle formé du rapport sera ajouté dans le dossier sélectionné **Serveur d'administration** de l'arborescence de la console. Ce modèle peut être utilisé pour créer et afficher des rapports.

Consultation et modification des propriétés du modèle de rapport

Vous pouvez consulter et modifier les propriétés de base d'un modèle de rapport par exemple, le nom du modèle de rapport ou les champs affichés dans le rapport.

Pour consulter et modifier les propriétés d'un modèle de rapport :

1. Dans l'arborescence de la console, sélectionnez l'entrée portant le nom du Serveur d'administration requis.
2. Dans l'espace de travail de l'entrée, sélectionnez l'onglet **Rapports**.
3. Dans la liste des modèles de rapport, sélectionnez le modèle de rapport requis.

4. Dans le menu contextuel du modèle de rapport sélectionné, sélectionnez **Propriétés**.

   Vous pouvez aussi commencer par générer le rapport, puis cliquer soit sur le bouton **Ouvrir les propriétés du modèle de rapport**, soit sur le bouton **Configurer les colonnes du rapport**.

5. Dans la fenêtrer qui s'ouvre, modifiez les propriétés du modèle de rapport. Il se peut que les propriétés de chaque rapport ne contiennent que quelques-unes des sections décrites ci-après.

   - Section **Général** :

     - Nom du modèle de rapport

     - Nombre maximal d'entrées affichées

       Quand cette option est activée, le nombre d'entrées affichées dans le tableau contenant les données détaillées du rapport ne peut être supérieur à la valeur indiquée.

       Les entrées du rapport sont tout d'abord classées en fonction des règles définies dans la section **Champs → Champs d'informations** des propriétés des modèles de rapport, puis seule la première des entrées obtenues est conservée. L'en-tête du tableau contenant les données détaillées du rapport reprend le nombre d'entrées affichées et le nombre total d'entrées disponible qui correspondent aux autres paramètres du modèle de rapport.

       Quand cette option est désactivée, le tableau contenant les données détaillées du rapport affiche toutes les entrées disponibles. Nous déconseillons de désactiver cette option. La restriction du nombre d'entrées affichées dans le rapport réduit la charge sur le système de gestion de base de données (SGBD) et réduit le temps requis pour la création et l'exportation du rapport. Certains rapports contiennent trop d'entrées. Dans ce cas, il peut être difficile de les lire et de les analyser tous. Aussi, votre appareil pourrait épuiser sa mémoire lors de la création de ces rapports et vous empêcher de les visualiser.

       Cette option est activée par défaut. La valeur par défaut est égale à 1000.

     - Imprimer la version

       La présentation du rapport est optimalisée pour l'impression : des espaces sont ajoutés entre certaines valeurs afin de simplifier la lecture.

       Cette option est activée par défaut.

   - Section **Champs**.

     Sélectionnez les champs qui seront repris dans le rapport et l'ordre d'affichage de ces champs, puis décidez si les informations dans le rapport doivent être triées et filtrées selon chaque champ.

   - Section **Période**.

     Modifiez la période du rapport. Les valeurs disponibles sont les suivantes :

     - Entre deux dates définies

     - Depuis la date définie jusqu'à la date de création du rapport

     - Depuis la date de création du rapport moins le nombre de jours indiqué avant la date de création du rapport

   - **Groupe**, section **Sélection d'appareils** ou **Appareils**.

     Modifiez la sélection d'appareils clients pour laquelle un rapport est créé. Seule une de ces sections peut être présente, en fonction des paramètres définis lors de la création du modèle de rapport.

- Section **Paramètres**.

  Modifiez les paramètres du rapport. L'ensemble exacte de paramètres dépend de chaque rapport.

- Section **Sécurité**. Hériter des paramètres du &Serveur d'administration

  Quand cette option est activée, les paramètres de sécurité du rapport sont hérités du Serveur d'administration.

  Quand cette option est désactivée, vous pouvez configurez les paramètres de sécurité pour le rapport. Vous pouvez affecter un rôle à un utilisateur ou à un groupe d'utilisateurs ou attribuer des permissions à un utilisateur ou à un groupe d'utilisateurs, tel qu'appliqué au rapport.

  Cette option est activée par défaut.

  La section **Sécurité** est disponible lorsque la case **Afficher les sections avec les paramètres de sécurité** est cochée dans la fenêtre de configuration de l'interface.

- Section **Hiérarchie des Serveurs d'administration** :

  - &Inclure les données à partir des Serveurs d'administration secondaires et virtuels

    Quand cette option est activée, le rapport reprend les informations des Serveurs d'administration secondaires et virtuels placés sous le Serveur d'administration pour lequel le modèle de rapport est créé.

    Désactivez cette option si vous souhaitez voir les données uniquement pour le Serveur d'administration actuel.

    Cette option est activée par défaut.

  - Jusqu'au niveau d'imbrication

    Le rapport contient les données des Serveurs d'administration secondaires et virtuels placés sous le Serveur d'administration actuel à un niveau d'imbrication inférieur ou égal à la valeur indiquée.

    La valeur par défaut est de 1. Vous pouvez modifier cette valeur si vous devez obtenir des informations des Serveurs d'administration secondaires situés à des niveaux inférieurs dans l'arborescence.

  - Intervalle d'attente des données (min.)

    Avant de créer le rapport, le Serveur d'administration pour lequel le modèle de rapport est créé attend les données des Serveurs d'administration secondaires pendant le nombre de minutes indiqué. Si le Serveur d'administration secondaire n'a envoyé aucune donnée à l'issue de cette période, le rapport est créé malgré tout. Au lieu des données réelles, le rapport affiche des données tirées du cache (si l'option **Mettre en cache les données des Serveurs d'administration** secondaires est activée) ou **N/A** (non disponible) dans le cas contraire.

    La valeur par défaut est de 5 (minutes).

  - Mettre en &cache les données des Serveurs d'administration secondaires

Les Serveurs d'administration secondaires transmettent régulièrement des données au Serveur d'administration pour lequel le rapport est créé. Là, les données transmises sont placées dans le cache.

Quand le Serveur d'administration actuel ne peut recevoir les données d'un Serveur d'administration secondaire lors de la création du rapport, le rapport affiche les données tirées du cache. La date de placement des données dans le cache est également affichée.

L'activation de cette option permet de consulter les informations de Serveurs d'administration secondaires même lorsqu'il est impossible de récupérer les données à jour. Les données affichées peuvent toutefois être obsolètes.

Cette option est Inactif par défaut.

- **Fréquence de mise à jour des données en cache (h.)**

  Les Serveurs d'administration secondaires transmettent à intervalles réguliers des données au Serveur d'administration pour lequel le rapport est créé. Vous pouvez spécifier cette période en heures. Une valeur égale à 0 signifie que les données sont transférées uniquement lorsque le rapport est créé.

  La valeur par défaut est égale à 0.

- **Transmettre des informations &détaillées à partir des Serveurs d'administration secondaires**

  Dans le rapport généré, le tableau contenant les données détaillées du rapport reprend les données des Serveurs d'administration secondaires du Serveur d'administration pour lequel le modèle de rapport est créé.

  L'activation de cette option ralentit la création du rapport et augment le trafic entre les Serveurs d'administration. Toutefois, elle permet de consulter toutes les données dans un rapport.

  Au lieu d'activer cette option, vous pouvez analyser les données détaillées de rapport afin de détecter un Serveur d'administration secondaire défectueux, puis générer le même rapport uniquement pour celui-ci.

  Cette option est Inactif par défaut.

Format de filtre étendu dans les modèles de rapport

Dans Kaspersky Security Center 15.1, vous pouvez appliquer le format de filtre étendu à un modèle de rapport. Le format de filtre étendu offre davantage de flexibilité que le format par défaut. Vous pouvez créer des conditions de filtrage complexes à l'aide d'un ensemble de filtres qui seront appliqués au rapport au moyen de l'opérateur logique OU lors de la création du rapport, comme indiqué ci-dessous :

Filtre [1] (Champ[1] ET Champ[2]... ET Champ [n]) OU Filtre[2] (Champ[1] ET Champ[2]... ET Champ [n]) OU... Filtre [n] (Champ[1] ET Champ[2]... ET Champ[n])

En outre, avec le format de filtre étendu, vous pouvez définir une valeur d'intervalle de temps dans un format d'heure relative (par exemple, en utilisant une condition « Pour les N derniers jours ») à appliquer à des champs spécifiques dans un filtre. La disponibilité et l'ensemble des conditions d'intervalle de temps dépendent du type de modèle de rapport.

Conversion du filtre au format étendu

Le format de filtre étendu pour les modèles de rapport n'est pris en charge que dans Kaspersky Security Center 12 et les versions ultérieures. Après la conversion du filtre par défaut au format étendu, le modèle de rapport devient incompatible avec les Serveurs d'administration du réseau sur lesquels des versions antérieures de Kaspersky Security Center sont installées. Les informations de ces Serveurs d'administration ne seront pas reçues pour le rapport.

Pour convertir le filtre par défaut du modèle de rapport au format étendu :

1. Dans l'arborescence de la console, sélectionnez l'entrée portant le nom du Serveur d'administration requis.
2. Dans l'espace de travail de l'entrée, sélectionnez l'onglet **Rapports**.
3. Dans la liste des modèles de rapport, sélectionnez le modèle de rapport requis.
4. Dans le menu contextuel du modèle de rapport sélectionné, sélectionnez **Propriétés**.
5. Dans la fenêtre des propriétés qui s'ouvre, sélectionnez la section **Champs**.
6. Dans l'onglet **Champs d'informations**, cliquez sur le lien **Convertir le filtre**.
7. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **OK**.

   La conversion au format de filtre étendu est irréversible pour le modèle de rapport auquel elle est appliquée. Si vous avez cliqué accidentellement sur le lien **Convertir le filtre**, vous pouvez annuler les modifications en cliquant sur le lien **Annuler** dans la fenêtre des propriétés du modèle de rapport.

8. Pour appliquer les modifications, fermez la fenêtre des propriétés du modèle de rapport en cliquant sur le bouton **OK**.

   Lorsque la fenêtre des propriétés du modèle de rapport s'ouvre à nouveau, la section des **Filtres** mise à disposition est affichée. Dans cette section, vous pouvez configurer le filtre étendu.

Configuration du filtre étendu

Pour configurer le filtre étendu dans les propriétés du modèle de rapport :

1. Dans l'arborescence de la console, sélectionnez l'entrée portant le nom du Serveur d'administration requis.
2. Dans l'espace de travail de l'entrée, sélectionnez l'onglet **Rapports**.
3. Dans la liste des modèles de rapport, sélectionnez le modèle de rapport précédemment converti au format de filtre étendu.
4. Dans le menu contextuel du modèle de rapport sélectionné, sélectionnez **Propriétés**.
5. Dans la fenêtre des propriétés qui s'ouvre, sélectionnez la section **Filtres**.

   La section **Filtres** n'est pas affichée si le modèle de rapport n'a pas été précédemment converti au format de filtre étendu.

   Dans la section **Filtres** de la fenêtre des propriétés du modèle de rapport, vous pouvez consulter et modifier la liste des filtres appliqués au rapport. Chaque filtre de la liste a un nom unique et représente un ensemble de filtres pour les champs correspondants dans le rapport.

6. Ouvrez la fenêtre des paramètres de filtre en utilisant l'un des moyens suivants :

   - Pour créer un nouveau filtre, cliquez sur le bouton **Ajouter**.
   - Pour modifier le filtre existant, sélectionnez le filtre requis et cliquez sur le bouton **Modifier**.

7. Dans la fenêtre qui s'ouvre, sélectionnez et spécifiez les valeurs des champs obligatoires du filtre.
8. Cliquez sur le bouton **OK** pour enregistrer les modifications et fermer la fenêtre.

   Si vous créez un nouveau filtre, le nom du filtre doit être spécifié dans le champ **Nom de filtre** avant de cliquer sur le bouton **OK**.

9. Fermez la fenêtre des propriétés du modèle de rapport en cliquant sur le bouton **OK**.

   Le filtre étendu du modèle de rapport est configuré. Vous pouvez maintenant créer des rapports à l'aide de ce modèle de rapport.

Génération et affichage des rapports

Pour former et consulter le rapport, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez l'entrée portant le nom du Serveur d'administration requis.
2. Dans l'espace de travail de l'entrée, sélectionnez l'onglet **Rapports**.
3. Dans la liste des modèles de rapport, double-cliquez sur le modèle de rapport dont vous avez besoin.

   Un rapport pour le modèle sélectionné s'affiche.

Le rapport affiche les données suivantes :

- Le type et le nom du rapport, une brève description et la période couverte, ainsi que les informations sur la création d'un rapport créée pour un groupe d'appareils.
- Graphique présentant les données les plus représentatives du rapport.
- Tableau récapitulatif avec les indices énumérés du rapport.
- Tableau avec les données détaillées du rapport.

Enregistrement du rapport

Afin de sauvegarder un rapport formé, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez l'entrée portant le nom du Serveur d'administration requis.
2. Dans l'espace de travail de l'entrée, sélectionnez l'onglet **Rapports**.
3. Dans la liste des modèles de rapport, sélectionnez le modèle de rapport dont vous avez besoin.
4. Dans le menu contextuel du modèle de rapport sélectionné, sélectionnez l'option **Enregistrer**.

L'Assistant d'enregistrement du rapport démarre. Suivez les instructions de l'assistant.

Quand l'Assistant a terminé, le dossier avec le fichier du rapport enregistré s'ouvre.

Lorsque vous enregistrez un rapport au format XLS, toutes les images associées, telles que le logo et le datagramme, sont enregistrées dans des fichiers distincts.

Création d'une tâche d'envoi du rapport

Les rapports peuvent être diffusés par email. La diffusion des rapports dans Kaspersky Security Center s'effectue à l'aide de la tâche de diffusion du rapport.

Pour créer une tâche de diffusion pour un seul rapport, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez l'entrée portant le nom du Serveur d'administration requis.
2. Dans l'espace de travail de l'entrée, sélectionnez l'onglet **Rapports**.
3. Dans la liste des modèles de rapport, sélectionnez le modèle de rapport dont vous avez besoin.
4. Dans le menu contextuel du modèle sélectionné du rapport, sélectionnez l'option **Envoi de rapports**.

   L'Assistant de création de la tâche d'envoi du rapport démarre. Suivez les instructions de l'assistant.

Pour créer une tâche de diffusion de plusieurs rapports, procédez comme suit :

1. Dans l'arborescence de la console, dans l'entrée portant le nom du Serveur d'administration requis, sélectionnez le dossier **Tâches**.
2. Dans l'espace de travail du dossier **Tâches**, cliquez sur le bouton **Créer une tâche**.

   Ceci permet de lancer l'Assistant de création d'une tâche. Suivez les instructions de l'assistant.

   La tâche de diffusion du rapport créée s'affiche dans le dossier de l'arborescence de la console **Tâches**.

La tâche de diffusion du rapport est créée automatiquement si les paramètres de l'email ont été spécifiés lors de l'installation de Kaspersky Security Center.

Étape 1. Sélectionner le type de tâche

Dans la fenêtre **Sélection du type de tâche**, dans la liste des tâches, sélectionnez **Envoi de rapports** comme type de tâche.

Pour passer à l'étape suivante, cliquez sur le bouton **Suivant**.

Étape 2. Sélection du type de rapport

Dans la fenêtre **Sélection du type de rapport**, dans la liste des modèles de création de la tâche, sélectionnez le type de rapport.

Pour passer à l'étape suivante, cliquez sur le bouton **Suivant**.

Étape 3. Actions sur un rapport

Dans la fenêtre **Action à appliquer aux rapports**, indiquez les paramètres suivants :

- **Envoyer les rapports par email**

  Si l'option est activée, l'application envoie les rapports créés par Email.

  Les paramètres d'envoi du rapport par email peuvent être configurés à l'aide du lien **Paramètres d'envoi par email**. Le lien est disponible si l'option est activée.

  Si l'option est désactivée, l'application enregistre les rapports dans le dossier prévu à cet effet.

  Cette option est Inactif par défaut.

- **Enregistrer les rapports dans un dossier partagé**

  Si l'option est activée, l'application enregistre les rapports dans le dossier indiqué dans le champ figurant sous la case. Pour enregistrer les rapports dans le dossier partagé, indiquez le chemin d'accès UNC à ce dossier. Dans ce cas, il faut définir le compte utilisateur et le mot de passe d'accès à ce dossier dans la fenêtre **Sélection du compte utilisateur pour télécharger une tâche**.

  Si l'option est désactivée, l'application n'enregistre pas les rapports dans le dossier, mais les envoie par Email.

  Cette option est Inactif par défaut.

- **Remplacer les rapports précédents du même type**

  Si l'option est activée, au démarrage de chaque tâche, un nouveau fichier de rapport remplace le fichier enregistré lors de l'exécution précédente.

  Si l'option est désactivée, les fichiers de rapports ne sont pas remplacés. Lors de chaque exécution de la tâche, un fichier de rapports distinct est sauvegardé dans le dossier.

  Une case à cocher est disponible si l'option **Enregistrer le rapport dans un dossier** est sélectionnée.

  Cette option est Inactif par défaut.

- **Créer un compte utilisateur pour accéder au dossier partagé**

  Si l'option est activée, il est possible d'indiquer le compte sous lequel le rapport est enregistré dans le dossier. Si dans la fenêtre **Manipulations du rapport**, le paramètre **Enregistrer le rapport dans un dossier** affiche comme valeur le chemin d'accès UNC au dossier partagé, il faut indiquer le compte utilisateur et le mot de passe d'accès à ce dossier.

  Si l'option est désactivée, le rapport est enregistré dans le dossier sous le compte du Serveur d'administration.

  Une case à cocher est disponible si l'option **Enregistrer le rapport dans un dossier** est sélectionnée.

  Cette option est Inactif par défaut.

Lorsque vous enregistrez ou envoyez un rapport au format XLS, toutes les images associées, telles que le logo et le datagramme, sont enregistrées dans des fichiers séparés.

Pour passer à l'étape suivante, cliquez sur le bouton **Suivant**.

Étape 4. Sélection du compte utilisateur pour télécharger une tâche

La fenêtre **Sélection du compte utilisateur pour exécuter la tâche** permet d'indiquer le compte utilisateur sous lequel la tâche va être exécutée. Sélectionnez l'une des options ci-dessous :

- **Compte par défaut**

  La tâche sera lancée sous le même compte utilisateur sous lequel l'application, exécutant cette tâche, a été installée et lancée.

  Cette option est sélectionnée par défaut.

- **Indiquer un compte**

  Remplissez les champs **Compte utilisateur** et **Mot de passe** pour définir les détails d'un compte à partir duquel la tâche est exécutée. Le compte doit disposer de droits suffisants pour cette tâche.

  - **Compte utilisateur**

    Le compte utilisateur au nom duquel la tâche sera lancée.

  - **Mot de passe**

    Mot de passe du compte utilisateur au nom duquel la tâche sera lancée.

Pour passer à l'étape suivante, cliquez sur le bouton **Suivant**.

Étape 5. Planification d'une tâche

La page de l'Assistant **Planifier la tâche** permet de programmer le lancement de la tâche. Le cas échéant, définissez les paramètres suivants :

- **Lancement planifié :**

  Sélectionnez la programmation de l'exécution de la tâche, puis configurez la programmation sélectionnée.

  - **Toutes les N heures**

    La tâche s'exécute régulièrement, selon l'intervalle défini en heures, à partir de la date et heure définis.

    La tâche s'exécute par défaut toutes les six heures à partir de la date et de l'heure actuelles du système.

  - **Tous les N jours**

    La tâche s'exécute régulièrement, selon l'intervalle défini en jours. En outre, vous pouvez spécifier la date et l'heure de la première exécution de la tâche. Ces options supplémentaires deviennent disponibles si elles sont prises en charge par l'application pour laquelle vous créez la tâche.

    La tâche s'exécute par défaut chaque jour, à partir de la date et de l'heure actuelle du système.

  - **Toutes les N semaines**

    La tâche s'exécute régulièrement, selon l'intervalle défini en semaines, le jour indiqué de la semaine et à l'heure indiquée.

    La tâche s'exécute par défaut chaque lundi à l'heure système actuelle.

  - **Toutes les N minutes**

    La tâche s'exécute régulièrement, à l'intervalle défini en minutes, à partir de l'heure indiquée le jour de la création de la tâche.

    La tâche s'exécute par défaut toutes les 30 minutes, à partir de l'heure actuelle du système.

  - **Chaque jour (passage à l'heure d'été non pris en charge)**

    La tâche s'exécute régulièrement, selon l'intervalle défini en jours. Cette programmation ne tient pas compte du passage à l'heure d'été. Cela signifie que lorsque les horloges sont avancées ou reculées d'une heure au début ou à la fin de l'été, l'heure de lancement réelle de la tâche ne change pas.

    Nous déconseillons d'adopter cette programmation. Elle est requise pour la rétrocompatibilité avec Kaspersky Security Center.

    La tâche démarre par défaut chaque jour à l'heure système actuelle.

  - **Chaque semaine**

    La tâche s'exécute chaque semaine, le jour défini et à l'heure indiquée.

  - **Par jours de la semaine**

La tâche s'exécute régulièrement les jours définis de la semaine, à l'heure indiquée.

Par défaut, la tâche s'exécute chaque vendredi à 18h00.

- **Chaque mois**

  La tâche s'exécute régulièrement le jour du mois défini, à l'heure indiquée.

  Si le jour en question ne figure pas dans le mois, la tâche s'exécute le dernier jour.

  La tâche s'exécute par défaut le premier jour de chaque mois, à l'heure système actuelle.

- **Manuel**

  La tâche ne s'exécute pas automatiquement. Vous pouvez uniquement la lancer manuellement.

  Cette option est sélectionnée par défaut.

- **Chaque mois, les jours indiqués des semaines sélectionnées**

  La tâche s'exécute régulièrement les jours du mois définis, à l'heure indiquée.

  Par défaut, aucun jour du mois n'est sélectionné. L'heure de début par défaut est 18:00.

- **Lors de la détection d'une attaque de virus**

  La tâche s'exécute après un événement *Attaque de virus* de virus. Sélectionnez les types d'application qui vont surveiller les propagations de virus. Les types suivants de Application sont présent :

  - Antivirus pour postes de travail et serveurs de fichiers
  - Antivirus de protection du périmètre
  - Antivirus pour systèmes de messagerie

  Tous les types d'application sont cochés par défaut.

  Il se peut que vous souhaitiez exécuter différentes tâches en fonction du type d'application de sécurité qui signale une propagation de virus. Dans ce cas, supprimez la sélection des types d'application dont vous n'avez pas besoin.

- **Après l'exécution d'une autre tâche**

La tâche actuelle démarre à la fin d'une autre tâche. Cette option ne fonctionne que si les deux tâches sont affectées aux mêmes appareils. Par exemple, vous pouvez exécuter la tâche *Administration des appareils* avec l'option **&Activer l'appareil** et, une fois celle-ci terminée, exécuter la tâche de *recherche de virus* comme tâche de déclenchement.

Il faut sélectionner la tâche de déclenchement dans le tableau et l'état avec lequel cette tâche doit se terminer (**Terminée avec succès** ou **Échec**).

Si nécessaire, vous pouvez rechercher, trier et filtrer les tâches dans le tableau comme suit :

- Saisissez le nom de la tâche dans le champ de recherche pour rechercher une tâche par son nom.
- Cliquez sur l'icône de tri pour trier les tâches par nom.

  Par défaut, les tâches sont triées par ordre alphabétique croissant.
- Cliquez sur l'icône du filtre, et dans la fenêtre qui s'ouvre, filtrez les tâches par groupe, puis cliquez sur le bouton **Appliquer**.

- **Lancer les tâches non exécutées**

  Cette option détermine le comportement d'une tâche si un appareil client n'est pas visible sur le réseau quand la tâche est sur le point de démarrer.

  Si la case est Activé, lors du lancement suivant de l'application de Kaspersky sur cet appareil client, une tentative de lancement de la tâche sera faite. Si la programmation de la tâche est **Manuel**, **Une fois** ou **Immédiatement**, la tâche est immédiatement lancée dès que l'appareil apparaît sur le réseau ou immédiatement après l'inclusion de l'appareil dans la zone d'action de la tâche.

  Si cette option est désactivée, seules les tâches planifiées s'exécutent sur les appareils clients. Pour les planifications **Manuel**, **Une fois** et **Immédiatement**, les tâches s'exécutent uniquement sur les appareils clients qui sont visibles sur le réseau. Par exemple, vous pouvez désactiver cette option pour une tâche qui consomme des ressources que vous voulez exécuter uniquement en dehors des heures de bureau.

  Cette option est Inactif par défaut.

- Adopter un décalage aléatoire automatique pour les lancements de tâche

  Si cette option est activée, la tâche est lancée sur les appareils clients de manière aléatoire au cours d'un intervalle défini. C'est ce qu'on appelle un *lancement échelonné d'une tâche*. Un lancement échelonné de tâche permet d'éviter la communication simultanée d'un nombre important d'appareils clients avec le Serveur d'administration lors du lancement de la tâche programmée.

  Le temps du lancement aléatoire est automatiquement calculée lors de la création d'une tâche selon le nombre d'appareils clients sur lesquels la tâche est diffusée. Par la suite, la tâche démarre toujours à l'heure de lancement calculée. Toutefois, quand les paramètres de la tâche sont modifiés ou si la tâche est lancée manuellement, la valeur calculée de l'heure de lancement de la tâche est modifiée.

  Si la case n'est pas cochée, le lancement de la tâche sur les appareils clients s'opère selon la planification.

- Décaler aléatoirement le lancement de la tâche dans un intervalle de (min.)

  Si cette option est activée, la tâche est lancée sur les appareils clients de manière aléatoire au cours de l'intervalle défini. Un lancement échelonné de tâche permet d'éviter la communication simultanée d'un nombre important d'appareils clients avec le Serveur d'administration lors du lancement de la tâche programmée.

  Si la case n'est pas cochée, le lancement de la tâche sur les appareils clients s'opère selon la planification.

  Cette option est Inactif par défaut. Par défaut, la valeur de cet intervalle est de une minute.

Étape 6. Définition du nom de la tâche

La fenêtre **Définition du nom de la tâche** permet de renseigner le nom de la tâche que vous créez. Le nom de la tâche ne peut pas contenir plus de 100 symboles et contenir de symboles spéciaux (`"*<>?\:|`).

Pour passer à l'étape suivante, cliquez sur le bouton **Suivant**.

Étape 7. Fin de la création d'une tâche

Dans la fenêtre **Fin de la création de la tâche**, cliquez sur le bouton **Terminé** pour quitter l'Assistant.

Si vous souhaitez que la tâche démarre directement à la fin de l'Assistant, cochez la case **&Lancer la tâche à la fin de l'Assistant**

Utilisation des données statistiques

Les statistiques sur l'état du système de protection et des appareils administrés apparaissent dans des panneaux d'informations personnalisables. Les statistiques sont affichées dans l'espace de travail de l'entrée **Serveur d'administration** sur l'onglet **Statistiques**. L'onglet contient plusieurs onglets de deuxième niveau (pages). Des panneaux d'informations contenant des statistiques ainsi que des liens vers des actualités et d'autres contenus de la société Kaspersky s'affichent sur chaque page d'onglet. Les données statistiques sont présentées sur les panneaux d'informations sous forme de tableaux ou de diagrammes camemberts ou colonnes. Les données dans les panneaux d'informations sont actualisées lors du fonctionnement de l'application et reflètent l'état actuel de l'application de sécurité.

Vous pouvez modifier l'ensemble des onglets de deuxième niveau sous l'onglet **Statistiques**, l'ensemble de panneaux d'informations sur chaque page d'onglets, ainsi que le mode d'affichage des données dans les panneaux d'informations.

*Pour ajouter un nouvel onglet de second niveau avec des panneaux d'informations, dans l'onglet **Statistiques**, procédez comme suit :*

1. Cliquez sur le bouton **Configurer l'apparence** en haut à droite de l'onglet **Statistiques**.

   La fenêtre des propriétés des statistiques s'ouvre. Cette fenêtre contient une liste des pages d'onglets actuellement affichées dans l'onglet **Statistiques**. Dans la fenêtre, vous pouvez modifier l'ordre d'apparition des pages dans l'onglet, ajouter et supprimer des pages, procéder à la configuration des propriétés des pages via le bouton **Propriétés**.

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

   La fenêtre de propriétés de la nouvelle page s'affiche.

3. Configurez la nouvelle page :

   - Dans la section **Général**, indiquez le nom de la page.

   - Dans la section **Panneaux d'informations**, cliquez sur le bouton **Ajouter** pour ajouter des panneaux d'informations qui doivent s'afficher sur la page.

     Cliquez sur le bouton **Propriétés** dans la section **Panneaux d'informations** pour configurer les propriétés des panneaux d'informations que vous avez ajoutés : nom, type et affichage du diagramme sur les panneaux, ainsi que les données qui ont servi à tracer le diagramme.

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

La page d'onglets ajoutée et les panneaux d'informations apparaissent dans l'onglet **Statistiques**. Cliquez sur l'icône (⚙) des paramètres pour aller directement à la configuration de la page ou du panneau d'informations sélectionné sur celle-ci.

Configuration des paramètres de notification sur les événements

Kaspersky Security Center permet de sélectionner le mode de notification de l'administrateur sur les événements survenus sur les appareils client et de configurer les paramètres de ces notifications :

- Email. Quand un événement se produit, l'application envoie une notification à l'adresse email indiquée. Vous pouvez configurer le texte de la notification.

- SMS. Quand un événement se produit, l'application envoie la notification aux numéros de téléphone indiqués. Vous pouvez configurer l'envoi des notifications SMS via la passerelle de messagerie.

- Fichier exécutable. Quand un événement se produit sur l'appareil, le fichier exécutable est lancé sur le poste de travail de l'administrateur. Le fichier exécutable permet à l'administrateur d'obtenir les paramètres de l'événement survenu.

Pour configurer les notifications sur les événements survenus sur les appareils clients, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez l'entrée portant le nom du Serveur d'administration requis.

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

3. Cliquez sur le lien **Configurer les paramètres des notifications et d'exportation des événements**, puis dans la liste déroulante, sélectionnez la valeur **Configurer les notifications**.

   Cela permet d'ouvrir la fenêtre **Propriétés : Événements**.

4. Dans la section **Notification**, sélectionnez le mode de notification (email, SMS, fichier exécutable à lancer) et configurez les paramètres des notifications.

   - **Email**

L'onglet **Email** vous permet de configurer les notifications d'événement par email.

Dans le champ **Destinataires (adresses email)**, indiquez les adresses e-mail auxquelles l'application enverra des notifications. Vous pouvez spécifier plusieurs adresses dans ce champ, en les séparant par un point-virgule.

Dans le champ **Serveurs SMTP**, spécifiez les adresses du serveur de messagerie, en les séparant par un point-virgule. Vous pouvez utiliser les valeurs suivantes du paramètre :

- Adresse IPv4 ou IPv6
- Nom de réseau Windows (nom NetBIOS) de l'appareil
- Nom complet du serveur SMTP

Dans le champ **Port du serveur SMTP**, spécifiez le numéro d'un port de communication du serveur SMTP. Le numéro de port par défaut est 25.

Si vous activez l'option **Utiliser la recherche MX de DNS**, vous pouvez utiliser plusieurs enregistrements MX des adresses IP pour le même nom DNS du serveur SMTP. Le même nom DNS peut avoir plusieurs enregistrements MX avec des priorités différentes pour la réception des emails. Le Serveur d'administration tente d'envoyer des notifications par email au serveur SMTP par ordre croissant de priorité des enregistrements MX. Cette option est Inactif par défaut.

Si vous activez l'option **Utiliser la recherche MX de DNS** et n'activez pas l'utilisation des paramètres TLS, nous vous recommandons d'utiliser les paramètres DNSSEC sur votre appareil serveur comme mesure supplémentaire de protection pour l'envoi des notifications par email.

Cliquez sur le lien **Paramètres** pour définir des paramètres de notification supplémentaires :

- Nom de l'objet (nom de l'objet d'un message électronique)
- Adresse email de l'expéditeur
- Paramètres d'authentification ESMTP

Vous devez indiquer un compte pour l'authentification sur un serveur SMTP si l'option d'authentification ESMTP est activée pour un serveur SMTP.

- Paramètres TLS pour le serveur SMTP :
  - **Ne pas utiliser TLS**

    Vous pouvez choisir cette option si vous désactivez le chiffrement des emails.
  - **Utiliser TLS si pris en charge par le serveur SMTP**

    Vous pouvez choisir cette option si vous voulez utiliser une connexion TLS pour un serveur SMTP. Si le serveur SMTP n'est pas compatible avec TLS, le Serveur d'administration connecte le serveur SMTP sans utiliser TLS.
  - **Toujours utiliser TLS, vérifier la validité du certificat de serveur**

    Vous pouvez choisir cette option si vous voulez utiliser les paramètres d'authentification TLS. Si le serveur SMTP n'est pas compatible avec TLS, le Serveur d'administration ne peut pas connecter le serveur SMTP.

Nous vous recommandons d'utiliser cette option pour améliorer la protection de la connexion avec un serveur SMTP. Si vous choisissez cette option, vous pouvez définir les paramètres d'authentification pour une connexion TLS.

Si vous choisissez la valeur **Toujours utiliser TLS, vérifier la validité du certificat de serveur**, vous pouvez spécifier un certificat pour l'authentification du serveur SMTP et choisir si vous souhaitez activer la communication via n'importe quelle version de TLS ou uniquement via TLS 1.2 ou les versions ultérieures. Vous pouvez également spécifier un certificat pour l'authentification du client sur le serveur SMTP.

Vous pouvez spécifier les paramètres TLS pour le serveur SMTP :

- Recherchez un fichier de certificat de serveur SMTP :

Vous pouvez recevoir un fichier avec la liste des certificats de l'autorité de certification de confiance et charger le fichier sur le Serveur d'administration. Kaspersky Security Center vérifie si le certificat d'un serveur SMTP est également signé par une autorité de certification de confiance ou non. Kaspersky Security Center ne peut pas se connecter à un serveur SMTP si le certificat du serveur SMTP ne provient pas d'une autorité de certification de confiance.

- Recherchez un fichier de certificat client :

Vous pouvez utiliser un certificat que vous avez reçu de n'importe quelle source, par exemple, de n'importe quelle autorité de certification de confiance. Vous devez spécifier le certificat et sa clé privée en utilisant l'un des types de certificats suivants :

- Certificat X-509 :

Vous devez spécifier un fichier avec le certificat et un fichier avec la clé privée. Les deux fichiers ne dépendent pas l'un de l'autre, et l'ordre de chargement des fichiers est sans importance. Lorsque les deux fichiers sont chargés, vous devez spécifier le mot de passe pour décoder la clé privée. Le mot de passe peut présenter une valeur vide si la clé privée n'est pas encodée.

- Conteneur pkcs12 :

Vous devez charger un seul fichier contenant le certificat et sa clé privée. Lorsque le fichier est chargé, vous devez ensuite indiquer le mot de passe pour décoder la clé privée. Le mot de passe peut présenter une valeur vide si la clé privée n'est pas encodée.

Le champ **Message de notification** contient du texte standard avec des informations sur l'événement que l'application envoie lors d'un événement. Ce texte inclut des paramètres de remplacement, comme le nom de l'événement, le nom de l'appareil et le nom de domaine. Vous pouvez modifier le texte du message en ajoutant d'autres paramètres de remplacement avec des détails plus pertinents de l'événement. La liste des paramètres de remplacement est disponible en cliquant sur le bouton à droite du champ.

Si le texte de notification contient un caractère en pourcentage (%), vous devez l'indiquer deux fois de suite pour autoriser l'envoi du message. Par exemple, « La charge du processeur est de 100 %% ».

Cliquez sur le lien **Configurer la limite du nombre de notifications** pour indiquer le nombre maximum de notifications que l'application peut envoyer pendant l'intervalle de temps spécifié.

Cliquez sur le bouton **&Envoyer un message d'essai** pour vérifier si vous avez correctement configuré les notifications. L'application envoie une notification de test aux adresses email que vous avez indiquées.

- SMS

L'onglet **SMS** vous permet de configurer la transmission de notifications par SMS des divers événements à un téléphone portable. Les messages SMS sont envoyés via une passerelle de messagerie.

Dans le champ **Destinataires (adresses email)**, indiquez les adresses email auxquelles l'application enverra des notifications. Vous pouvez spécifier plusieurs adresses dans ce champ, en les séparant par un point-virgule. Les notifications seront envoyées aux numéros de téléphone associés aux adresses email spécifiées.

Dans le champ **Serveurs SMTP**, spécifiez les adresses du serveur de messagerie, en les séparant par un point-virgule. Vous pouvez utiliser les valeurs suivantes du paramètre :

- Adresse IPv4 ou IPv6
- Nom de réseau Windows (nom NetBIOS) de l'appareil
- Nom complet du serveur SMTP

Dans le champ **Port du serveur SMTP**, spécifiez le numéro d'un port de communication du serveur SMTP. Le numéro de port par défaut est 25.

Cliquez sur le lien **Paramètres** pour définir des paramètres de notification supplémentaires :

- Nom de l'objet (nom de l'objet d'un message électronique)
- Adresse email de l'expéditeur
- Paramètres d'authentification ESMTP

Au besoin, vous pouvez spécifier un compte pour l'authentification sur un serveur SMTP si l'option d'authentification ESMTP est activée pour un serveur SMTP.

- Paramètres TLS pour le serveur SMTP

Vous pouvez désactiver l'utilisation de TLS, utiliser TLS si le serveur SMTP prend en charge ce protocole ou vous pouvez forcer l'utilisation de TLS uniquement. Si vous choisissez d'utiliser uniquement TLS, vous pouvez spécifier un certificat pour l'authentification du serveur SMTP et choisir si vous souhaitez activer la communication via n'importe quelle version de TLS ou uniquement via TLS 1.2 ou les versions ultérieures. De plus, si vous choisissez d'utiliser uniquement TLS, vous pouvez spécifier un certificat pour l'authentification du client sur le serveur SMTP.

- Rechercher un fichier de certificat de serveur SMTP

Vous pouvez recevoir un fichier avec la liste des certificats des autorités de certification de confiance et charger le fichier dans Kaspersky Security Center. Kaspersky Security Center vérifie si le certificat du serveur SMTP est également signé par une autorité de certification de confiance ou non. Kaspersky Security Center ne peut pas se connecter au serveur SMTP si le certificat du serveur SMTP ne provient pas d'une autorité de certification de confiance.

Vous devez charger un seul fichier contenant le certificat et sa clé privée. Lorsque le fichier est chargé, vous devez ensuite indiquer le mot de passe pour décoder la clé privée. Le mot de passe peut être vide si la clé privée n'est pas encodée. Le champ **Message de notification** contient un texte standard avec des informations sur l'événement que l'application envoie lorsqu'un événement se produit. Ce texte inclut des paramètres de remplacement, comme le nom de l'événement, le nom de l'appareil et le nom de domaine. Vous pouvez modifier le texte du message en ajoutant d'autres paramètres de remplacement avec des détails plus pertinents de l'événement. La liste des paramètres de remplacement est disponible en cliquant sur le bouton à droite du champ.

Si le texte de notification contient un caractère en pourcentage (%), vous devez l'indiquer deux fois de suite pour autoriser l'envoi du message. Par exemple, « La charge du processeur est de 100 %% ».

Cliquez sur le lien **Configurer la limite de notification numérique** pour indiquer le nombre maximum de notifications que l'application peut envoyer au cours de l'intervalle de temps spécifié.

Cliquez sur le bouton **Envoyer un message d'essai** pour vérifier si vous avez bien configuré les notifications. L'application envoie une notification de test au destinataire que vous avez indiqué.

- Fichier exécutable à exécuter

  Si cette méthode de notification est sélectionnée, dans le champ de saisie, vous pouvez indiquer quelle application démarre selon l'événement qui se produit.

  Cliquez sur le lien **Configurer la limite du nombre de notifications** pour indiquer le nombre maximum de notifications que l'application peut envoyer sur l'intervalle de temps spécifié.

  Cliquez sur le bouton **Envoyer un message d'essai** pour vérifier si vous avez bien configuré les notifications : l'application envoie une notification d'essai aux adresses électroniques que vous avez indiquées.

5. Dans le champ **Message de notification**, saisissez le texte que l'application enverra lorsqu'un événement se produira.

   Dans la liste déroulante située à droite du champ de texte, choisissez les paramètres prédéfinis avec les détails de l'événement à ajouter au texte (par exemple, la description de l'événement, l'heure à laquelle il s'est produit, etc.).

   Si le texte de la notification contient le caractère %, il faut le saisir deux fois pour que le message puisse être envoyé. Par exemple, « La charge du processeur est de 100 %% ».

6. Cliquez sur le bouton **&Envoyer un message d'essai** pour vérifier si la notification a été correctement configurée.

   L'application envoie la notification au destinataire indiqué.

7. Cliquez sur le bouton **OK** afin d'enregistrer les modifications.

Les paramètres configurés de notification sont diffusés sur tous les événements survenus sur les appareils clients.

Vous pouvez remplacer les paramètres de notification de certains événements dans la section **Configuration de l'événement** des Paramètres du Serveur d'administration, des paramètres d'une stratégie, ou des paramètres d'une application.

Création d'un certificat pour le serveur SMTP

Pour créer un certificat pour le serveur SMTP, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez l'entrée portant le nom du Serveur d'administration requis.
2. Dans l'espace de travail de l'entrée, sélectionnez l'onglet **Événements**.
3. Cliquez sur le lien **Configurer les paramètres des notifications et d'exportation des événements**, puis dans la liste déroulante, sélectionnez la valeur **Configurer les notifications**.

   La fenêtre de propriétés des événements s'affiche.

4. Dans l'onglet **Email**, cliquez sur le lien **Paramètres** pour ouvrir la fenêtre **Paramètres**.

5. Dans la fenêtre **Paramètres**, cliquez sur le lien **Indiquer le certificat** pour ouvrir la fenêtre **Certificat pour la signature**.

6. Dans la fenêtre **Certificat pour la signature**, cliquez sur le bouton **Parcourir**.

   La fenêtre **Certificat** s'ouvre.

7. Dans la liste déroulante **Type de certificat**, sélectionnez le type de certificat ouvert ou fermé :

   - Si le certificat sélectionné est de type fermé (**Conteneur PKCS#12**), indiquez le fichier de certificat et le mot de passe.

   - Si le certificat sélectionné est de type ouvert (**Certificat X.509**) :

     a. indiquez un fichier clé privée (avec l'extension prk ou pem).

     b. Indiquez le mot de passe de la clé privée.

     c. Indiquez un fichier clé publique (avec l'extension cer).

8. Cliquez sur le bouton **OK**.

Suite à cette action, un certificat pour serveur SMTP est créé.

Sélections d'événements

Les informations relatives aux événements dans le fonctionnement de Kaspersky Security Center et des applications administrées sont enregistrées dans la base de données du Serveur d'administration et dans le journal système de Microsoft Windows. Vous pouvez consulter des informations de la base de données du Serveur d'administration dans l'espace de travail de l'entrée **Serveur d'administration** dans l'onglet **Événements**.

Les informations de l'onglet **Événements** sont présentées sous forme de liste de sélections d'événements. Chaque sélection inclut seulement les événements d'un certain type. Par exemple, la sélection « L'appareil est en état critique » contient uniquement les enregistrements du passage des appareils à l'état « Critique ». Après l'installation de l'application, l'onglet **Événements** contient certaines sélections d'événements standard. Vous pouvez créer des sélections complémentaires (d'utilisateurs) d'événements et exporter les informations sur les événements dans un fichier.

Consultation d'une sélection d'événements

Pour consulter une sélection d'événements, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez l'entrée portant le nom du Serveur d'administration requis.

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

3. Dans la liste déroulante **Sélections d'événements**, choisissez la sélection d'événements concernée.

   Si vous souhaitez que les événements de cette sélection s'affichent en permanence dans l'espace de travail, cliquez sur l'icône étoile (☆) en regard de la sélection.

L'espace de travail reprend la liste des événements du type sélectionné enregistrés sur le Serveur d'administration.

Vous pouvez trier les informations dans la liste des événements par ordre croissant ou décroissant des données dans n'importe quelle colonne de la liste.

Configuration d'une sélection d'événements

Pour configurer une sélection d'événements, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez l'entrée portant le nom du Serveur d'administration requis.
2. Dans l'espace de travail de l'entrée, sélectionnez l'onglet **Événements**.
3. Ouvrez la sélection d'événements concernée sous l'onglet **Événements**.
4. Cliquez sur le bouton **Propriétés de la sélection**.

   Dans la fenêtre ouverte des propriétés de la sélection d'événements, vous pouvez configurer les paramètres de la sélection.

Création d'une sélection d'événements

Pour créer une sélection d'événements, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez l'entrée portant le nom du Serveur d'administration requis.
2. Dans l'espace de travail de l'entrée, sélectionnez l'onglet **Événements**.
3. Cliquez sur le bouton **Créer une sélection**.
4. Dans la fenêtre ouverte **Nouvelle sélection d'événements**, indiquez le nom de la sélection créée et cliquez sur le bouton **OK**.

   Suite à cette action, une section portant le nom que vous avez indiqué est créée dans la liste déroulante **Sélections d'événements**.

Par défaut, la sélection d'événements créée contient tous les événements enregistrés sur le Serveur d'administration. Pour que la sélection d'événements affiche uniquement les événements qui vous intéressent, il faut configurer les paramètres de la sélection.

Exportation d'une sélection d'événements dans le fichier texte

Pour exporter la sélection d'événements dans un fichier texte, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez l'entrée portant le nom du Serveur d'administration requis.
2. Dans l'espace de travail de l'entrée, sélectionnez l'onglet **Événements**.
3. Cliquez sur le bouton **Importation/Exportation**.
4. Dans la liste affichée, sélectionnez **Exporter les événements dans un fichier**.

L'Assistant d'exportation des événements démarre. Suivez les instructions de l'assistant.

Suppression des événements depuis la sélection

Pour supprimer des événements de la sélection, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez l'entrée portant le nom du Serveur d'administration pertinent.
2. Dans l'espace de travail de l'entrée, sélectionnez l'onglet **Événements**.
3. Sélectionnez les événements à supprimer à l'aide de la souris et des touches **SHIFT** ou **CTRL**.
4. Supprimez les événements sélectionnés par un des moyens suivants :
   - En sélectionnant **Supprimer** dans le menu contextuel de n'importe lequel des événements sélectionnés.

     Lors de la sélection de l'option du menu contextuel **Supprimer tout**, tous les événements affichés seront supprimés de la sélection, quelle que soit votre sélection d'événements à supprimer.
   - En cliquant sur le lien **Supprimer l'événement** (si un événement a été sélectionné), ou sur le lien **Supprimer les événements** (si plusieurs événements ont été sélectionnés) dans la zone d'informations correspondant à ces événements.

Suite à cette action, les événements sélectionnés sont supprimés.

Ajout d'applications aux exclusions sur requêtes des utilisateurs

Lorsque vous recevez des requêtes des utilisateurs pour débloquer des applications bloquées par erreur, vous pouvez créer une exclusion pour les règles de la Sécurité évolutive appliquées à ces applications. Par la suite, les applications ne seront plus bloquées sur les appareils des utilisateurs. Vous pouvez suivre le nombre de requêtes des utilisateurs sous l'onglet **Surveillance** du Serveur d'administration.

Pour ajouter des applications bloquées par Kaspersky Endpoint Security à la liste des exclusions sur requêtes des utilisateurs :

1. Dans l'arborescence de la console, sélectionnez l'entrée portant le nom du Serveur d'administration requis.
2. Dans l'espace de travail de l'entrée, sélectionnez l'onglet **Événements**.
3. Dans la liste déroulante **Sélections d'événements**, sélectionnez **Requêtes des utilisateurs**.
4. Cliquez-droit sur la ou les requêtes des utilisateurs qui contiennent les application à ajouter aux exclusions, puis choisissez l'option **Ajouter une exclusion**.

   Cela lance l'assistant d'ajout d'une exclusion. Suivez-en les instructions.

Les applications sélectionnées seront exclues de la liste **Déclenchements de règles dans l'état Apprentissage intelligent** (sous **Stockages** dans l'arborescence de la console) après la prochaine synchronisation de l'appareil client avec le Serveur d'administration, et elles ne figureront plus dans la liste.

Sélections d'appareils

Les informations sur l'état des appareils se trouvent dans le dossier **Sélections d'appareils** dans l'arborescence de la console.

Les informations dans le dossier de **Sélections d'appareils** sont présentées sous forme de liste de sélections d'appareils. Chaque sélection comprend les appareils répondant aux conditions définies. Par exemple, la sélection **Appareils avec l'état Critique** contient uniquement des appareils avec l'état *Critique*. Une fois que l'application a été installée, le dossier **Sélections d'appareils** contient diverses sélections standard. Vous pouvez créer des sélections d'appareils complémentaires (définies par l'utilisateur), exporter les paramètres des sélections dans un fichier, et créer des sélections avec les paramètres importés depuis un fichier.

Affichage d'une sélection d'appareils

Pour afficher une sélection d'appareils, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le dossier **Sélections d'appareils**.
2. Dans l'espace de travail du dossier, dans la liste déroulante **Appareils de la sélection**, choisissez la sélection d'appareils concernée.
3. Cliquez sur le bouton **Lancer la sélection**.
4. Cliquez sur l'onglet **Résultats de la sélection**.

Finalement, l'espace de travail présentera la liste des appareils qui répondent aux paramètres de la sélection.

Vous pouvez trier les informations dans la liste des appareils en ordre croissant ou décroissant et dans n'importe quelle colonne.

Configuration d'une sélection d'appareils

Pour configurer la sélection d'appareils, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le dossier **Sélections d'appareils**.
2. Dans l'espace de travail, cliquez sur l'onglet **Sélection**, puis sélectionnez la sélection d'appareils concernée dans la liste des sélections d'utilisateurs.
3. Cliquez sur le bouton **Propriétés de la sélection**.
4. Dans la fenêtre des propriétés qui s'ouvre, définissez les paramètres suivants :
   - Propriétés de la sélection générales.
   - Conditions à remplir pour inclure les appareils de la sélection. Vous pouvez configurer les conditions après avoir sélectionné un nom de condition et cliqué sur le bouton **Propriétés**.
   - Paramètres de sécurité.
5. Cliquez sur le bouton **OK**.

Les paramètres sont appliqués et enregistrés.

Les paramètres des conditions d'ajout des appareils à une sélection sont décrits ci-dessous. Les conditions sont combinées à l'aide de l'opérateur logique " ou " : la sélection reprend les appareils qui répondent au moins à une des conditions présentées.

Général

La section **Général** permet de modifier le nom de la condition de la sélection et d'indiquer si cette condition doit être intervertie :

Inverser la condition de sélection

Cette option est Inactif par défaut.

Si vous activez cette option, la condition de sélection définie sera inversée. Tous les appareils qui ne correspondent pas à la condition feront partie de la sélection.

L'exemple suivant montre la logique du travail d'inversion :

- **Condition** : sur votre appareil, il y a un système d'exploitation avec le type Linux et le numéro de build 00.0.000.
- **Condition inversée** : sur votre appareil, il existe un système d'exploitation avec NOT (le type de version Linux et le numéro de build 00.0.000), ce qui équivaut à ce qui suit :

  Il existe un système d'exploitation de type NOT Linux OU numéro de build NOT 00.0.000.

Ainsi, la sélection inclura les appareils équipés d'un système d'exploitation, par exemple, de type Windows et dont le numéro de build est 00.0.000, ou de type Linux et dont le numéro de build est différent de 00.0.000.

Réseau

La section **Réseau** permet de configurer les critères d'inclusion des appareils dans une sélection sur la base de leurs données de réseau.

- **Nom de l'appareil ou adresse IP**

  Nom de réseau Windows (nom NetBIOS) de l'appareil ou adresse IPv4 ou IPv6.

- **Domaine Windows**

  Les appareils faisant partie du domaine Windows indiqué seront affichés.

- **Groupe d'administration**

  Les appareils faisant partie du groupe d'administration seront affichés.

- **Description**

  Texte apparaissant dans la fenêtre des propriétés de l'appareil : dans le champ **Description** de la section **Général**.

  Pour décrire le texte dans le champ **Description**, vous pouvez utiliser les caractères suivants :

  - A l'intérieur d'un seul mot :

    - *****. Remplace n'importe quelle ligne quel que soit le nombre de caractères.

    Exemple :

    Pour décrire les mots **Serveur**, **Serveurs** ou de serveur, il est possible d'utiliser la ligne **Serveur***.

    - **?.** Remplace un n'importe quel caractère.

    Exemple :

    Pour décrire les mots **Fenêtre** ou **Fenêtres**, il est possible d'utiliser la ligne **Fenêtr?**.

    Caractère ***** ou **?** ne peut pas être utilisé en tant que premier caractère dans la description du texte.

  - Pour lier plusieurs mots :

    - Espace. Affiche l'ensemble des appareils dont la description contient l'un des mots de la liste.

    Exemple :

    Pour décrire la phrase contenant le mot **Secondaire** ou **Virtuel**, il est possible d'utiliser la ligne **Secondaire Virtuel**.

    - **+**. Avant le mot signifie la présence obligatoire du mot dans le texte.

    Exemple :

    Pour décrire la phrase contenant le mot **Secondaire**, et le mot **Virtuel**, il est possible de saisir la demande **+Secondaire+Virtuel**.

    - **-**. Avant le mot signifie l'absence obligatoire du mot dans le texte.

    Exemple :

    Pour décrire la phrase avec le mot **Secondaire** et sans le mot **Virtuel**, il est possible de saisir la demande **+Secondaire-Virtuel**.

    - **"<le texte>"**. Le fragment du texte entre guillemets doit être entièrement présent dans le texte.

    Exemple :

    Pour décrire la phrase contenant le groupe de mots **Serveur secondaire**, il est possible de saisir la demande **"Serveur secondaire"**.

- **Plage IP**

  Si l'option est activée, vous pouvez saisir les adresses IP de début et de fin de la plage IP à laquelle les appareils concernés doivent appartenir.

  Cette option est Inactif par défaut.

Tags

La section **Tags** permet de configurer les critères d'inclusion des appareils dans une sélection sur la base des mots clés (tags) ajoutés au préalable aux descriptions des appareils administrés :

- **Appliquer si au moins un tag sélectionné coïncide**

  Si l'option est activée, les appareils dont la description contient au moins l'un des tags sélectionnés figureront dans les résultats de la recherche.

  Si l'option est désactivée, seuls les appareils dont la description contient l'ensemble des tags sélectionnés figureront dans les résultats de la recherche.

  Cette option est Inactif par défaut.

- **Le tag doit être inclus**

  Si vous avez choisi cette option, les résultats de la recherche reprennent les appareils dont la description contient le tag sélectionné. Dans le cadre de la recherche d'appareils, vous pouvez utiliser le caractère * qui remplace n'importe quelle chaîne quel que soit le nombre de caractères.

  Cette option est sélectionnée par défaut.

- **Le tag doit être exclus**

  Si vous avez choisi cette option, les résultats de la recherche reprennent les appareils dont la description ne contient pas le tag sélectionné. Dans le cadre de la recherche d'appareils, vous pouvez utiliser le caractère * qui remplace n'importe quelle chaîne quel que soit le nombre de caractères.

Active Directory

La section **Active Directory** permet de configurer les critères d'inclusion d'appareils dans une sélection sur la base de leurs données Active Directory :

- **L'appareil se trouve dans une unité &organisationnelle Active Directory**

  Si l'option est activée, la sélection inclura les appareils de l'unité d'organisation Active Directory indiquée dans le champ de saisie.

  Cette option est Inactif par défaut.

- **Inclure les unités organisationnelles enfants**

  Si l'option est activée, la sélection inclut les appareils appartenant aux unités organisationnelles enfants de l'unité organisationnelle de domaine spécifiée.

  Cette option est Inactif par défaut.

- **L'appareil est un membre du &groupe Active Directory**

  Si l'option est activée, la sélection inclut les appareils issus du groupe Active Directory indiqué dans le champ de saisie.

  Cette option est Inactif par défaut.

Activité réseau

La section **Activité réseau** permet de configurer les critères d'inclusion des appareils dans une sélection sur la base de leur activité réseau :

- L'appareil est un point de distribution

  La liste déroulante permet de sélectionner les critères d'inclusion des appareils dans la sélection dans le cadre d'une recherche :

  - **Oui**. La sélection contient les appareils qui ne sont pas des points de distribution.
  - **Non**. Les appareils qui sont les points de distribution ne seront pas inclus dans la sélection.
  - **La valeur n'est pas sélectionnée**. Les critères ne sont pas appliqués.

- Maintenir la connexion au Serveur d'administration

  La liste déroulante permet de sélectionner les critères d'inclusion des appareils dans la sélection dans le cadre d'une recherche :

  - **Activé**. La sélection comportera des appareils sur lesquels la case **Maintenir la connexion au Serveur d'administration** est cochée.
  - **Désactivé**. La sélection comprendra des appareils sur lesquels la case **Maintenir la connexion au Serveur d'administration** est décochée.
  - **La valeur n'est pas sélectionnée**. Les critères ne sont pas appliqués.

- Changement du profil de connexion

  La liste déroulante permet de sélectionner les critères d'inclusion des appareils dans la sélection dans le cadre d'une recherche :

  - **Oui**. La sélection inclura les appareils connectés au Serveur d'administration suite au changement du profil de connexion.
  - **Non**. La sélection n'inclura pas les appareils connectés au Serveur d'administration suite au changement du profil de connexion.
  - **La valeur n'est pas sélectionnée**. Les critères ne sont pas appliqués.

- Dernière connexion au Serveur d'administration

  Cette case permet de définir les critères de recherche d'appareils selon la date et l'heure de la dernière connexion au Serveur d'administration.

  Si la case est cochée, le champ de saisie permet d'indiquer les valeurs de l'intervalle de temps (date et heure), durant lequel la dernière connexion de l'Agent d'administration installé sur l'appareil client avec le Serveur d'administration a été effectuée. La sélection contient les appareils qui s'inscrivent dans l'intervalle défini.

  Si la case est décochée, le critère ne sera pas appliqué.

  Celle-ci est décochée par défaut.

- Nouveaux appareils détectés lors d'un sondage du réseau

  Recherche de nouveaux appareils détectés lors du sondage du réseau au cours des derniers jours.

  Si l'option est activée, la sélection inclut seulement les nouveaux appareils détectés lors de la recherche d'appareils au cours du nombre de jours défini dans le champ **Période de détection (jours)**.

  Si l'option est désactivée, la sélection inclut tous les appareils détectés lors de la recherche d'appareils.

  Cette option est Inactif par défaut.

- Appareil visible

  La liste déroulante permet de sélectionner les critères d'inclusion des appareils dans la sélection dans le cadre d'une recherche :

  - **Oui**. L'application est reprise dans la sélection d'appareils visibles sur le réseau à l'heure actuelle.
  - **Non**. L'application est reprise dans la sélection d'appareils qui ne sont pas visibles sur le réseau à l'heure actuelle.
  - **La valeur n'est pas sélectionnée**. Les critères ne sont pas appliqués.

Application

La section **Application** permet de configurer les critères d'inclusion des appareils dans une sélection sur la base de l'application administrée sélectionnée :

- Nom de l'application

  Liste déroulante qui permet de sélectionner les critères d'inclusion des appareils dans la sélection dans le cadre d'une recherche selon le nom de l'application de Kaspersky.

  La liste ne fournit que le nom des applications disposant de plug-ins d'administration installés sur le poste de travail de l'administrateur.

  Si l'application n'est pas sélectionnée, les critères ne sont pas appliqués.

- Version de l'application

  Champ qui permet de saisir les critères d'inclusion des appareils dans la sélection lors de la recherche par numéro de version de l'application de Kaspersky.

  Si le numéro de version n'est pas indiqué, les critères ne sont pas appliqués.

- Nom de la mise à jour critique

  Champ de saisie qui permet de saisir les critères d'inclusion des appareils dans la sélection lors de la recherche du paquet de mise à jour installé pour l'application par nom ou numéro.

  Si le champ n'est pas rempli, les critères ne sont pas appliqués.

- **Dernière mise à jour des modules**

  Cette option permet de définir les critères de recherche d'appareils selon l'heure de la dernière mise à jour des modules des applications installées sur les appareils.

  Si la case est cochée, le champ de saisie permet d'indiquer les valeurs de l'intervalle de temps (date et heure), durant lequel la dernière mise à jour des modules des applications installées sur les appareils a été effectuée.

  Si la case est décochée, le critère ne sera pas appliqué.

  Celle-ci est décochée par défaut.

- **L'appareil est administré par Kaspersky Security Center**

  La liste déroulante permet d'inclure les appareils qui sont administrés via Kaspersky Security Center dans la sélection d'appareils :

  - **Oui**. L'application ajoute les appareils administrés via Kaspersky Security Center à la sélection d'appareils.
  - **Non**. L'application inclut les appareils dans la sélection s'ils ne sont pas administrés via Kaspersky Security Center.
  - **La valeur n'est pas sélectionnée**. Les critères ne sont pas appliqués.

- **L'application de sécurité est installée**

  La liste déroulante permet d'ajouter à la sélection d'appareils ceux sur lesquels l'application de sécurité est installée :

  - **Oui**. L'application inclut les appareils sur lesquels l'application de sécurité est installée dans la sélection d'appareils.
  - **Non**. L'application inclut les appareils sur lequel l'application de sécurité n'est pas installée dans la sélection d'appareils.
  - **La valeur n'est pas sélectionnée**. Les critères ne sont pas appliqués.

Système d'exploitation

La section **Système d'exploitation** permet de configurer les critères d'inclusion d'appareils dans une sélection en fonction du type de système d'exploitation installé.

- **Version du système d'exploitation**

  Si la case est cochée, la liste permet de sélectionner les systèmes d'exploitation. Les appareils avec les systèmes d'exploitation indiqués installés sont inclus dans les résultats de recherche.

- **Taille de bit du système d'exploitation**

  Dans la liste déroulante, vous pouvez sélectionner l'architecture du système d'exploitation qui détermine la manière dont la règle de déplacement est appliquée à l'appareil (**Inconnu**, **x86**, **AMD64** ou **IA64**). Par défaut, aucune option n'est sélectionnée dans la liste, l'architecture du système d'exploitation n'est pas définie.

- **Version du service pack du système d'exploitation**

  Dans ce champ, vous pouvez indiquer la version du paquet du système d'exploitation installé (au format X.Y) en présence de laquelle la règle de déplacement s'applique à l'appareil. Par défaut, la version n'est pas indiquée.

- **Build du système d'exploitation**

  Ce paramètre concerne uniquement les systèmes d'exploitation Windows.

  Le numéro de version du système d'exploitation. Vous pouvez indiquer si le système d'exploitation sélectionné doit avoir un numéro de version égal, antérieur ou supérieur. Vous pouvez également configurer la recherche de tous les numéros de version à l'exception du numéro indiqué.

- **ID de version du système d'exploitation**

  Ce paramètre concerne uniquement les systèmes d'exploitation Windows.

  L'identifiant de version du système d'exploitation. Vous pouvez indiquer si le système d'exploitation sélectionné doit avoir un ID de version égal, antérieur ou supérieur. Vous pouvez également configurer la recherche de tous les ID de version à l'exception du numéro indiqué.

État de l'appareil

La section **État de l'appareil** permet de configurer les critères d'inclusion des appareils dans une sélection sur la base de la description de l'état de l'appareil envoyé par une application administrée :

- **État de l'appareil**

  Liste déroulante qui permet de sélectionner l'un des états de l'appareil : *OK*, *Critique* ou *Avertissement*.

- **Description d'état de l'appareil**

  Ce champ permet de cocher les cases en regard des conditions qui, lorsqu'elles sont remplies, affectent l'un des états suivants à l'appareil : *OK, Critique* ou *Avertissement*.

- **État de l'appareil défini par l'application**

  Liste déroulante vous permettant de sélectionner l'état de la protection en temps réel. Les appareils avec l'état indiqué de la protection en temps réel seront inclus dans la sélection.

Modules de protection

La section **Modules de protection** permet de configurer les critères d'inclusion d'appareils dans une sélection sur la base de leur état de la protection :

- **Les bases de données sont publiées**

  Si l'option est activée, la recherche d'appareils clients s'exécute selon la date de publication des bases antivirus. Les champs de saisies permettent d'indiquer l'intervalle de temps sur la base duquel la recherche aura lieu.

  Cette option est Inactif par défaut.

- **Dernière analyse**

  Si l'option est activée, la recherche d'appareils clients s'exécute en fonction de l'heure de la dernière analyse des logiciels malveillants. Les champs de saisie permettent d'indiquer l'intervalle durant lequel la dernière analyse des logiciels malveillants a été exécutée.

  Cette option est Inactif par défaut.

- **Nombre total de détections de menaces**

  Si l'option est activée, la recherche d'appareils clients s'exécute en fonction du nombre de virus sélectionné. Les champs de saisie permettent d'indiquer les valeurs inférieures et supérieures du nombre de virus découverts.

  Cette option est Inactif par défaut.

Registre des applications

La section **Registre des applications** permet de configurer les critères d'inclusion d'appareils dans une sélection sur la base des applications installées :

- **Nom de l'application**

  La liste déroulante qui permet de sélectionner l'application. Les appareils avec l'application indiquée installée seront inclus dans la sélection.

- **Version de l'application**

  Le champ de saisie à indiquer la version de l'application sélectionnée.

- **Éditeur**

  La liste déroulante qui permet de sélectionner l'éditeur de l'application installée sur l'appareil.

- **État de l'application**

  La liste déroulante qui permet de sélectionner l'état de l'application (*Installé*, *Non installé*). Les appareils sur lesquels l'application indiquée est installée ou non sont inclus dans la sélection en fonction de l'état sélectionné.

- **Rechercher selon la mise à jour**

  Si l'option est activée, la recherche sera exécutée selon les informations présentes dans les mises à jour des applications installées sur les appareils concernés. Une fois que vous avez sélectionné la case à cocher, les champs **Nom de l'application**, **Version de l'application** et **État de l'application** se changent respectivement en **Nom de la mise à jour**, **Version de la mise à jour** et **État**.

  Cette option est Inactif par défaut.

- **Nom de l'application de sécurité incompatible**

  La liste déroulante qui permet de sélectionner les applications antivirus des éditeurs tiers. Les appareils avec l'application sélectionnée installée seront inclus dans la sélection pendant la recherche.

- Tag de l'application

  La liste déroulante permet de sélectionner le tag de l'application. Tous les appareils sur lesquels sont installés des applications dont la description contient le tag sélectionné, sont repris dans la sélection d'appareils.

- Appliquer aux appareils sans les tags sélectionnés

  Si cette option est activée, la sélection inclut des appareils ne contenant aucun des tags sélectionnés.

  Si l'option est désactivée, les critères ne sont pas appliqués.

  Cette option est Inactif par défaut.

Registre du matériel

La section **Registre du matériel** permet de configurer les critères d'inclusion des appareils dans une sélection sur la base du matériel installé :

- Appareil

  La liste déroulante permet de sélectionner le type d'unité. Tous les appareils avec cette unité sont inclus dans les résultats de la recherche.

  Le champ prend en charge la recherche en texte intégral.

- Éditeur

  La liste déroulante permet de sélectionner le fabricant de la machine virtuelle. Tous les appareils avec cette unité sont inclus dans les résultats de la recherche.

  Le champ prend en charge la recherche en texte intégral.

- Nom de l'appareil

  Nom de l'appareil dans le réseau Windows. L'appareil portant le nom indiqué est repris dans la sélection.

- Description

  Description de l'appareil ou du matériel. Les appareils dont la description figure dans le champ seront inclus dans la sélection.

  La description de l'appareil peut être librement saisie dans la fenêtre des propriétés. Le champ prend en charge la recherche en texte intégral.

- Fabricant d'appareil

  Nom du fabricant de l'appareil. Les appareils du fabricant figurant dans le champ seront inclus dans la sélection.

  Le nom du fabricant peut être saisi dans la fenêtre des propriétés de l'appareil.

- **Numéro de série**

  Le matériel dont le numéro de série figure dans le champ sera inclus dans la sélection.

- **Numéro d'inventaire**

  Le matériel dont le numéro d'inventaire figure dans le champ sera inclus dans la sélection.

- **Utilisateur**

  Le matériel de l'utilisateur figurant dans le champ sera inclus dans la sélection.

- **Emplacement**

  Emplacement de l'appareil ou du matériel (par exemple dans le bureau ou dans la filiale). Les ordinateurs ou les autres appareils dont l'emplacement figure dans le champ seront inclus dans la sélection.

  L'emplacement de l'appareil peut être librement saisi dans la fenêtre des propriétés du matériel.

- **Fréquence du processeur, en MHz**

  Plage de fréquence du processeur. Les appareils dont la fréquence du processeur est comprise dans la plage figurant dans les champs de saisie (inclus) seront inclus dans la sélection.

- **Noyaux virtuels**

  Plage de noyaux virtuels du processeur. Les appareils dont le nombre de processeurs est compris dans la plage figurant dans les champs de saisie (inclus) seront inclus dans la sélection.

- **Volume du disque dur (Go)**

  Plage de volumes du disque dur de l'appareil. Les appareils dont le volume du disque dur est compris dans la plage figurant dans les champs de saisie (inclus) seront inclus dans la sélection.

- **Taille de la mémoire RAM (Mo)**

  Plage de valeur du volume de mémoire RAM de l'appareil. Les appareils dont le volume de mémoire RAM est compris dans la plage figurant dans les champs de saisie (inclus) seront inclus dans la sélection.

Machines virtuelles

La section **Machines virtuelles** permet de configurer les critères d'inclusion des appareils dans une sélection selon qu'il s'agit de machines virtuelles ou d'appareils inclus dans une infrastructure de type Virtual Desktop Infrastructure (VDI) :

- **Est une machine virtuelle**

  La liste déroulante permet de sélectionner les éléments suivants :

  - **Ignorer**.
  - **Non**. Les appareils recherchés ne doivent pas être des machines virtuelles.
  - **Oui**. Les appareils recherchés doivent être des machines virtuelles.

- **Type de machine virtuelle**

  La liste déroulante permet de sélectionner le fabricant de la machine virtuelle.

  Cette liste déroulante est disponible si les valeurs **Oui** ou **Ignorer** sont sélectionnées dans la liste déroulante **Est une machine virtuelle**.

- **Membre d'une Virtual Desktop Infrastructure**

  La liste déroulante permet de sélectionner les éléments suivants :

  - **Ignorer**.
  - **Non**. Les appareils recherchés ne doivent pas faire partie de Virtual Desktop Infrastructure.
  - **Oui**. Les appareils recherchés doivent faire partie de Virtual Desktop Infrastructure (VDI).

Vulnérabilités et mises à jour

La section **Vulnérabilités et mises à jour** permet de définir les critères d'inclusion d'appareils dans une sélection sur la base de leur source de mise à jour Windows Update :

WUA est transféré sur le Serveur d'administration

Dans la liste déroulante, vous pouvez sélectionner une des options de recherche suivantes :

- **Oui**. Si cette option a été sélectionnée, les appareils qui reçoivent les mises à jour Windows Update depuis le Serveur d'administration sont inclus dans les résultats de recherche.
- **Non**. Si cette option a été sélectionnée, les appareils qui reçoivent les mises à jour Windows Update depuis une autre source sont inclus dans les résultats de recherche.

Utilisateurs

La section **Utilisateurs** permet de configurer les critères d'inclusion des appareils dans une sélection sur la base des comptes utilisateurs utilisés pour ouvrir la session dans le système d'exploitation.

- **Dernier utilisateur ayant accédé au système**

  Si l'option est activée, cliquez sur le bouton **Parcourir** pour définir un compte utilisateur. Les résultats de recherche comprennent les appareils dont le dernier accès au système d'exploitation a été effectué par l'utilisateur indiqué.

- **Utilisateur ayant accédé au moins une fois au système**

  Si l'option est activée, cliquez sur le bouton **Parcourir** pour définir un compte utilisateur. Les résultats de recherche comprennent les appareils sur lesquels l'utilisateur indiqué a déjà accédé au système.

Problèmes ayant une incidence sur l'état dans les applications administrées

La section **Problèmes ayant une incidence sur l'état dans les applications administrées** permet de spécifier les critères d'inclusion des appareils dans une sélection sur la base de la liste des problèmes potentiels détectés par une application administrée. Si au moins un des problèmes que vous avez sélectionné existe sur un appareil, l'appareil est repris dans la sélection. Quand vous sélectionnez un problème repris pour plusieurs applications, vous avez la possibilité de sélectionner ce problème dans toutes les listes automatiquement.

Description d'état de l'appareil

Vous pouvez cocher les cases pour les descriptions des états de l'application administrée dont la réception entraînera l'inclusion de l'appareil dans la sélection. Quand vous sélectionnez un état repris pour plusieurs applications, vous avez la possibilité de sélectionner cet état dans toutes les listes automatiquement.

État des modules des applications administrées

La section **État des modules des applications administrées** permet de configurer les critères d'inclusion des appareils dans une sélection sur la base de l'état des modules dans les applications administrées :

- **État de la protection contre les fuites de données**

  Recherchez des appareils sur la base de l'état de la Protection contre les fuites de données (*Inconnu, Arrêté(e), En cours de démarrage, Suspendu(e), En cours d'exécution, Échec*).

- **État de la protection des serveurs de collaboration**

  Recherchez des appareils sur la base de l'état de la protection de collaboration du serveur (*Inconnu, Arrêté(e), En cours de démarrage, Suspendu(e), En cours d'exécution, Échec*).

- **État de Endpoint Protection des serveurs de messagerie**

  Recherchez des appareils sur la base de l'état de la protection du Serveur de messagerie (*Inconnu, Arrêté(e), En cours de démarrage, Suspendu(e), En cours d'exécution, Échec*).

- **État de Endpoint Sensor**

  Recherchez des appareils sur la base de l'état du module Endpoint Sensor (*Inconnu, Arrêté(e), En cours de démarrage, Suspendu(e), En cours d'exécution, Échec*).

Chiffrement

Algorithme de chiffrement

Standard d'algorithme de chiffrement symétrique par bloc Advanced Encryption Standard (AES). La liste déroulante permet de sélectionner la taille de la clé de chiffrement (56, 128, 192 ou 256 bits).

Les valeurs possibles sont *AES56*, *AES128*, *AES192*, *AES256*.

Segments dans le cloud

La section **Segments dans le cloud** permet de configurer les critères d'inclusion des appareils dans une sélection sur la base de leur appartenance aux segments dans le Cloud :

- **L'appareil se trouve dans un segment dans le cloud**

  Si l'option est activée, vous pouvez cliquer sur le bouton **Parcourir** pour indiquer le segment dans lequel rechercher.

  Si l'option **Inclure les objets enfants** est également activée, la recherche est exécutée sur l'ensemble des objets enfants du segment indiqué.

  Seuls les appareils du segment choisi figurent dans les résultats de la recherche.

- **Appareil &découvert à l'aide de l'API**

  La liste déroulante permet de choisir s'vous pouvez détecter un appareil à l'aide des outils de l'API :

  - **AWS**. L'appareil est détecté via l'utilisation de l'API AWS, autrement dit, l'appareil est bel et bien dans l'environnement cloud AWS.
  - **Azure**. L'appareil est détecté via l'utilisation de l'API Azure, autrement dit, l'appareil est bel et bien dans l'environnement cloud Azure.
  - **Google Cloud.** L'appareil est détecté via l'utilisation de l'API Google, autrement dit, l'appareil est bel et bien dans le cloud Google.
  - **Non**. L'appareil n'est pas détecté à l'aide de l'API AWS, Azure ou Google, c'est-à-dire qu'il se trouve soit en dehors de l'environnement Cloud, soit dans l'environnement Cloud, mais il ne peut pas être détecté à l'aide d'une API.
  - **Pas de valeur**. Cette condition ne s'applique pas.

Modules de l'application

Cette section contient la liste des modules des applications dont le plug-in d'administration correspondant est installé dans la Console d'administration.

La section **Modules de l'application** permet de définir les critères d'inclusion des appareils dans une sélection sur la base des états et des numéros de version des modules faisant référence à l'application que vous avez sélectionnée :

- **État**

  Recherchez les appareils selon les états des modules renvoyés par une application au Serveur d'administration. Vous avez le choix entre les états suivants : *Aucune donnée de l'appareil*, *Arrêté*, *En cours de démarrage*, *Suspendu*, *En cours d'exécution*, *Dysfonctionnement* ou *Non installé*. Si le module sélectionné de l'application installée sur un appareil administré possède l'état indiqué, l'appareil est repris dans la sélection d'appareils.

  États envoyés par les applications :

  - *En cours de démarrage* : l'initialisation du module est actuellement en cours.
  - *En cours d'exécution* : le module est activé et fonctionne correctement.
  - *Suspendu* : le module est suspendu, par exemple, après que l'utilisateur a suspendu la protection dans l'application administrée.
  - *Dysfonctionnement* : une erreur s'est produite lors du fonctionnement du module.
  - *Arrêté* : le module est désactivé et ne fonctionne pas pour l'instant.
  - *Non installé* : l'utilisateur n'a pas sélectionné le module en vue de l'installer lors de la configuration de l'installation personnalisée de l'application.

  A la différence des autres états, l'état *Aucune donnée de l'appareil* n'est pas envoyé par les applications. Cette option indique que les applications n'ont aucune information sur l'état du module sélectionné. Cela peut se produire, par exemple, quand le module sélectionné n'appartient à aucune des applications installées sur l'appareil ou quand l'appareil est éteint.

- **Version**

  Recherchez les appareils en fonction du numéro de version du module que vous avez sélectionné dans la liste. Vous pouvez taper un numéro de version, par exemple `3.4.1.0`, puis indiquez si le numéro de version du module sélectionné doit être égal, antérieur ou postérieur. Vous pouvez également configurer la recherche de toutes les versions à l'exception du numéro indiqué.

Exportation des paramètres de la sélection d'appareils dans un fichier

Pour exporter les paramètres de la sélection d'appareils dans le fichier texte, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le dossier **Sélections d'appareils**.
2. Dans l'espace de travail, sous l'onglet **Sélection**, cliquez sur la sélection d'appareils concernée dans la liste des sélections d'utilisateurs.

   Les paramètres peuvent être exportés uniquement à partir des sélections d'appareils créées par un utilisateur.

3. Cliquez sur le bouton **Lancer la sélection**.

4. Sous l'onglet **Résultats de la sélection**, cliquez sur le bouton **Exporter les paramètres**.

5. Dans la fenêtre ouverte **Enregistrer sous**, définissez le nom du fichier d'exportation des paramètres de la sélection, sélectionnez le dossier dans lequel le fichier sera enregistré et cliquez sur le bouton **Enregistrer**.

Les paramètres de la sélection d'appareils seront enregistrés dans le fichier indiqué.

Création d'une sélection d'appareils

Pour créer une sélection d'appareils, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le dossier **Sélections d'appareils**.

2. Dans l'espace de travail du dossier, cliquez sur **Avancé**, et, dans la liste déroulante, sélectionnez **Créer une sélection**.

3. Dans la fenêtre ouverte **Nouvelle sélection d'appareils** qui s'ouvre, indiquez le nom de la nouvelle sélection et cliquez sur le bouton **OK**.

Un nouveau dossier portant le nom que vous avez indiqué apparaîtra dans l'arborescence de la console, dans le dossier **Sélections d'appareils**. Par défaut, la sélection d'appareils créée contient tous les appareils inclus dans les groupes d'administration du Serveur d'administration pour lequel la sélection a été créée. Pour que la sélection d'événements affiche uniquement les appareils qui vous intéressent, vous devez configurer la sélection en appuyant sur le bouton **Propriétés de la sélection**.

Création d'une sélection d'appareils selon les paramètres importés

Pour créer une sélection d'appareils selon les paramètres importés, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le dossier **Sélections d'appareils**.

2. Dans l'espace de travail du dossier, cliquez sur le bouton **Avancé**, et, dans la liste déroulante, sélectionnez **Importer une sélection depuis un fichier**.

3. Dans la fenêtre qui s'ouvre, indiquez le chemin d'accès au fichier depuis lequel vous souhaitez importer les paramètres de la sélection. Cliquez sur **Ouvrir**.

Une **Nouvelle sélection** entrée est créée dans le dossier **Sélections d'appareils**. Les paramètres de la nouvelle sélection sont importés depuis le fichier que vous avez défini.

Si une sélection portant le nom **Nouvelle sélection** existe déjà dans le dossier **Sélections d'appareils**, un suffixe de type **(<next sequence number>)** est ajouté au nom de la sélection créée, par exemple : **(1)**, **(2)**.

Suppression des appareils depuis les groupes d'administration dans la sélection

Lors de l'utilisation de la sélection d'appareils, vous pouvez supprimer les appareils des groupes d'administration directement dans la sélection sans avoir à supprimer les appareils des groupes d'administration.

Pour supprimer les appareils depuis les groupes d'administration, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le dossier **Sélections d'appareils**.
2. Sélectionnez les appareils à supprimer à l'aide des touches **Maj** ou **Ctrl**.
3. Supprimez les appareils sélectionnés depuis les groupes d'administration à l'aide d'un des moyens suivants :
   - Sélectionnez **Supprimer** dans le menu contextuel d'un des appareils sélectionnés.
   - Cliquez le bouton **Exécuter l'action** et, dans la liste déroulante, sélectionnez **Supprimer du groupe**.

Finalement, les appareils sélectionnés seront supprimés depuis les groupes d'administration dont ils faisaient partie.

Surveillance de l'installation et de la désinstallation des applications

Vous pouvez surveiller l'installation et la désinstallation d'applications spécifiques sur des appareils administrés (par exemple, un navigateur spécifique). Pour utiliser cette fonction, vous pouvez ajouter des applications du registre des applications à la liste des applications surveillées. Lorsqu'une application surveillée est installée ou désinstallée, l'Agent d'administration publie les événements respectifs :**L'application contrôlée a été installée** ou **L'application contrôlée a été désinstallée**. Vous pouvez surveiller ces événements à l'aide, par exemple, de sélections d'événements ou de rapports.

Vous ne pouvez surveiller ces événements que s'ils sont stockés dans la base de données du Serveur d'administration.

Pour ajouter une application à la liste des applications surveillées :

1. Dans le dossier **Avancé** → **Gestion des applications** de l'arborescence de la console, sélectionnez le sous-dossier **Registre des applications**.
2. Au-dessus de la liste des applications qui s'affiche, cliquez sur le bouton **Ouvrir la fenêtre des propriétés du registre des applications**.
3. Dans la fenêtre **Applications contrôlées** affichée, cliquez sur le bouton **Ajouter**.
4. Dans la fenêtre **Sélectionnez le nom de l'application** qui s'affiche, sélectionnez les applications dans le Registre des applications dont vous souhaitez surveiller l'installation ou la désinstallation.
5. Dans la fenêtre **Sélectionnez le nom de l'application**, cliquez sur le bouton **OK**.

Après avoir configuré la liste des applications surveillées et installé ou désinstallé une application surveillée sur des appareils administrés de votre organisation, vous pouvez surveiller les événements respectifs, par exemple à l'aide de la sélection d'événements récents Derniers événements.

Événements des modules de Kaspersky Security Center

Chaque module de Kaspersky Security Center possède son propre ensemble de types d'événements. Cette section reprend les types d'événements qui se produisent dans le Serveur d'administration de Kaspersky Security Center, l'Agent d'administration et le Serveur MDM iOS. Les types d'événements qui surviennent dans les applications de Kaspersky ne sont pas répertoriés dans cette section.

Pour chaque événement pouvant être généré par une application, vous pouvez spécifier les paramètres de notification et les paramètres de stockage sous l'onglet **Configuration des événements** dans la stratégie de l'application. Pour le Serveur d'administration, vous pouvez également consulter et configurer la liste des événements dans les propriétés du Serveur d'administration. Si vous souhaitez configurer les paramètres de notification pour tous les événements à la fois, configurez les paramètres de notification généraux dans les propriétés du Serveur d'administration.

Structure des données de la description du type d'événement

Pour chaque type d'événement, le nom affiché, l'identifiant (ID), le code alphabétique, la description et la durée de stockage par défaut sont fournis.

- **Nom affiché du type d'événement**. Ce texte est affiché dans Kaspersky Security Center lorsque vous configurez les événements et lorsqu'ils se produisent.
- **ID de type d'événement**. Ce code numérique est utilisé lorsque vous traitez des événements à l'aide d'outils tiers en vue d'une analyse.
- **Type d'événement** (code alphabétique). Ce code est utilisé lorsque vous naviguez parmi les événements et les traitez à l'aide des représentations publiques fournies dans la base de données de Kaspersky Security Center et lorsque les événements sont exportés dans un système SIEM.
- **Description**. Ce texte décrit les situations où l'événement se produit et ce qu'il faut faire dans ce cas.
- **Durée de stockage par défaut**. Il s'agit du nombre de jours pendant lesquels l'événement est conservé dans la base de données du Serveur d'administration et affiché dans la liste des événements sur le Serveur d'administration. A l'issue de cette période, l'événement est supprimé. Si la valeur du paramètre de conservation des événements est de 0, les événements sont détectés, mais ils ne sont pas affichés dans la liste des événements du Serveur d'administration. Si votre configuration prévoit l'enregistrement de ces événements dans le journal des événements du système d'exploitation, c'est là qu'il faudra les chercher.

  Vous pouvez modifier la durée de conservation pour les événements :

  - Console d'administration : définition de la condition de stockage pour un événement
  - Kaspersky Security Center Web Console : définition de la condition de stockage pour un événement

Les autres données peuvent inclure les champs suivants :

- **event_id** : numéro unique de l'événement dans la base de données, généré et attribué automatiquement ; à ne pas confondre avec l'**identifiant de type d'événement**.
- **task_id** : l'identifiant de la tâche qui a provoqué l'événement (le cas échéant)
- **severity** : l'un des niveaux de gravité suivants (dans l'ordre croissant de gravité) :

  0) Niveau de gravité incorrect

  1) Informations

  2) Avertissement

  3) Erreur

  4) Critique

Événements du Serveur d'administration

Cette section contient des informations sur les événements liés au serveur d'administration.

Événements critiques du Serveur d'administration

Le tableau ci-dessous indique les types d'événements du Serveur d'administration de Kaspersky Security Center, regroupés par niveau de gravité **Critique**.

Pour chaque événement pouvant être généré par une application, vous pouvez spécifier les paramètres de notification et les paramètres de stockage sous l'onglet **Configuration des événements** dans la stratégie de l'application. Pour le Serveur d'administration, vous pouvez également consulter et configurer la liste des événements dans les propriétés du Serveur d'administration. Si vous souhaitez configurer les paramètres de notification pour tous les événements à la fois, configurez les paramètres de notification généraux dans les propriétés du Serveur d'administration.

Si vous avez indiqué le port dans la fenêtre des propriétés du Serveur d'administration de la Console d'administration, **Kaspersky Security Center publie ses métriques** et ses événements critiques afin que le système de surveillance et d'alerte puisse les obtenir par Prometheus. Prometheus obtient les métriques et les événements critiques, puis génère des alertes pour chaque événement.

// KL.KSC.Common—Kaspersky Security Center common counters

"xdr_klserver_errors", "counter", "klserver errors"

"xdr_klserver_api_calls_time", "counter", "klserver api calls time"

// KL.KSC.Transport—Transport counters set

"ksc_Transport__Number_of_all_connections", "counter", "number of all connections"

"ksc_Transport__Number_of_all_nagent_connection", "counter", "number of all Network Agent connection"

"ksc_Transport__Number_of_controlled_nagent_connections", "counter", "number of controlled Network Agent connections"

"ksc_Transport__Total_active_hosts_count", "gauge", "total active devices count"

"ksc_Transport__Number_of_pings_processed", "counter", "number of pings processed"

"ksc_Transport__Number_of_pings_rejected", "counter", "number of pings rejected"

"ksc_Transport__Number_of_ping_processing_errors", "counter", "number of ping processing errors"

"ksc_Transport__Number_of_TCP_connections_accepted", "counter", "number of TCP connections accepted"

"ksc_Transport__Number_of_failed_TCP_connections", "counter", "number of failed TCP connections"

"ksc_Transport__Bytes_sent_by_TCP", "counter", "bytes sent by TCP"

"ksc_Transport__Bytes_received_by_TCP", "counter", "bytes received by TCP"

"ksc_Transport__Number_of_GetNextFileChunk_requests", "counter", "number of GetNextFileChunk requests"

"ksc_Transport__Number_of_GetNextFileChunk_rejected", "counter", "number of GetNextFileChunk rejected"

"ksc_Transport__Bytes_transmitted_through_GetNextFileChunk", "counter", "bytes transmitted through GetNextFileChunk"

// KL.KSC.Events—Events delivery counters set

"ksc_Events__Number_of_event_bulks_processed", "counter", "number of event bulks processed"

"ksc_Events__Number_of_event_bulks_rejected", "counter", "number of event bulks rejected"

"ksc_Events__Number_of_event_bulks_processing_errors", "counter", "number of event bulks processing errors"

"ksc_Events__Number_of_event_bulks_processing_just_now", "gauge", "number of event bulks processing just now"

"ksc_Events__Number_of_events_processed", "counter", "number of events processed"

"ksc_Events__Number_of_events_rejected", "counter", "number of events rejected"

"ksc_Events__Number_of_events_processing_errors", "counter", "number of events processing errors"

"ksc_Events__Number_of_events_processing_just_now", "gauge", "number of events processing just now"

// KL.KSC.Resources—Kaspersky Security Center resources usage

"ksc_Resources__CPU_time_in_user_mode", "counter", "CPU time in user mode"

"ksc_Resources__CPU_time_in_kernel_mode", "counter", "CPU time in kernel mode"

"ksc_Resources__PID_of_klserver_process", "gauge", "process ID of klserver"

"ksc_Resources__PID_of_klnagent_process", "gauge", "process ID of klnagent"

"ksc_Resources__Available_disk_user_quota_for_server_data", "gauge", "available disk user quota for server data"

"ksc_Resources__Available_disk_user_quota_for_packages", "gauge", "available disk user quota for packages"

"ksc_Resources__Current_OpenAPI_threads_count", "counter", "current OpenAPI threads count

"ksc_Resources__Maximum_OpenAPI_threads_count", "counter", "maximum OpenAPI threads count"

// KL.KSC.NLST

// KL.KSC.NLST.Trans.Common—List of server transactions

"ksc_NLST__Common__Current_transactions_count", "gauge", "current transactions count

"ksc_NLST__Common__Transactions_queue_ful", "gauge", "transactions queue full"

"ksc_NLST__Common__Transactions_queue_near_to_ful", "gauge", "transactions queue near to full"

// KL.KSC.NLST.InvAppCtrlLink—Application Control link

"ksc_NLST__Application_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Application_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Application_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Application_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Application_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Application_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Application_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Application_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Application_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.InvSoft—Software Inventory

"ksc_NLST__Software_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Software_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Software_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Software_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Software_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Software_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Software_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Software_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Software_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.InvHard—Hardware Inventory

"ksc_NLST__Hardware_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Hardware_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Hardware_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Hardware_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Hardware_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Hardware_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Hardware_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Hardware_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Hardware_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.DevCtrl—Device Control

"ksc_NLST__Device_control__items_changed", "gauge", "items changed"

"ksc_NLST__Device_control__items_deleted", "gauge", "items deleted"

"ksc_NLST__Device_control__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Device_control__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Device_control__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Device_control__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Device_control__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Device_control__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Device_control__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.MDM—Mobile Device Management

"ksc_NLST__Mobile_device_management__items_changed", "gauge", "items changed"

"ksc_NLST__Mobile_device_management__items_deleted", "gauge", "items deleted"

"ksc_NLST__Mobile_device_management__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Mobile_device_management__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Mobile_device_management__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Mobile_device_management__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Mobile_device_management__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Mobile_device_management__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Mobile_device_management__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.MDMmails—Device management emails

"ksc_NLST__Device_management_emails__items_changed", "gauge", "items changed"

"ksc_NLST__Device_management_emails__items_deleted", "gauge", "items deleted"

"ksc_NLST__Device_management_emails__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Device_management_emails__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Device_management_emails__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Device_management_emails__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Device_management_emails__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Device_management_emails__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Device_management_emails__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.AppCtrl—Application Control

"ksc_NLST__Application_control__items_changed", "gauge", "items changed"

"ksc_NLST__Application_control__items_deleted", "gauge", "items deleted"

"ksc_NLST__Application_control__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Application_control__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Application_control__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Application_control__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Application_control__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Application_control__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Application_control__transactions_in_queue", "gauge", "transactions in queue"

"ksc_NLST__Application_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Application_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Application_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Application_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Application_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Application_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Application_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Application_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Application_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.DPEErrors—Data protection errors

"ksc_NLST__Data_protection_errors__items_changed", "gauge", "items changed"

"ksc_NLST__Data_protection_errors__items_deleted", "gauge", "items deleted"

"ksc_NLST__Data_protection_errors__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Data_protection_errors__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Data_protection_errors__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Data_protection_errors__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Data_protection_errors__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Data_protection_errors__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Data_protection_errors__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.iOsMDM—iOS Mobile Device Management

"ksc_NLST__iOS_mobile_device_management__items_changed", "gauge", "items changed"

"ksc_NLST__iOS_mobile_device_management__items_deleted", "gauge", "items deleted"

"ksc_NLST__iOS_mobile_device_management__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__iOS_mobile_device_management__change_item_operations", "gauge", "change item operations"

"ksc_NLST__iOS_mobile_device_management__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__iOS_mobile_device_management__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__iOS_mobile_device_management__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__iOS_mobile_device_management__list_is_pending", "gauge", "list is pending"

"ksc_NLST__iOS_mobile_device_management__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.Vapm—Vulnerability assessment and patch management

"ksc_NLST__Vulnerability_assesment_and_patch_management__items_changed", "gauge", "items changed"

"ksc_NLST__Vulnerability_assesment_and_patch_management__items_deleted", "gauge", "items deleted"

"ksc_NLST__Vulnerability_assesment_and_patch_management__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Vulnerability_assesment_and_patch_management__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Vulnerability_assesment_and_patch_management__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Vulnerability_assesment_and_patch_management__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Vulnerability_assesment_and_patch_management__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Vulnerability_assesment_and_patch_management__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Vulnerability_assesment_and_patch_management__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.Va—Vulnerability assessment

"ksc_NLST__Vulnerability_assesment__items_changed", "gauge", "items changed"

"ksc_NLST__Vulnerability_assesment__items_deleted", "gauge", "items deleted"

"ksc_NLST__Vulnerability_assesment__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Vulnerability_assesment__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Vulnerability_assesment__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Vulnerability_assesment__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Vulnerability_assesment__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Vulnerability_assesment__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Vulnerability_assesment__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.VM—Virtual machines

"ksc_NLST__Virtual_machines__items_changed", "gauge", "items changed"

"ksc_NLST__Virtual_machines__items_deleted", "gauge", "items deleted"

"ksc_NLST__Virtual_machines__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Virtual_machines__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Virtual_machines__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Virtual_machines__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Virtual_machines__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Virtual_machines__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Virtual_machines__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.WUS—Windows Update

"ksc_NLST__Windows_update__items_changed", "gauge", "items changed"

"ksc_NLST__Windows_update__items_deleted", "gauge", "items deleted"

"ksc_NLST__Windows_update__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Windows_update__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Windows_update__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Windows_update__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Windows_update__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Windows_update__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Windows_update__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.CIP_PLC—CIP PLC

"ksc_NLST__CIP_PLC__items_changed", "gauge", "items changed"

"ksc_NLST__CIP_PLC__items_deleted", "gauge", "items deleted"

"ksc_NLST__CIP_PLC__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__CIP_PLC__change_item_operations", "gauge", "change item operations"

"ksc_NLST__CIP_PLC__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__CIP_PLC__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__CIP_PLC__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__CIP_PLC__list_is_pending", "gauge", "list is pending"

"ksc_NLST__CIP_PLC__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.NagentNetScan—Network Agent Network Scan

"ksc_NLST__Network_scan__items_changed", "gauge", "items changed"

"ksc_NLST__Network_scan__items_deleted", "gauge", "items deleted"

"ksc_NLST__Network_scan__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Network_scan__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Network_scan__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Network_scan__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Network_scan__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Network_scan__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Network_scan__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.AS—Adaptive Security

"ksc_NLST__Adaptive_security__items_changed", "gauge", "items changed"

"ksc_NLST__Adaptive_security__items_deleted", "gauge", "items deleted"

"ksc_NLST__Adaptive_security__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Adaptive_security__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Adaptive_security__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Adaptive_security__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Adaptive_security__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Adaptive_security__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Adaptive_security__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.ASS—Adaptive Security State

"ksc_NLST__Adaptive_security_state__items_changed", "gauge", "items changed"

"ksc_NLST__Adaptive_security_state__items_deleted", "gauge", "items deleted"

"ksc_NLST__Adaptive_security_state__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Adaptive_security_state__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Adaptive_security_state__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Adaptive_security_state__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Adaptive_security_state__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Adaptive_security_state__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Adaptive_security_state__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.KillChain—Kill Chain

"ksc_NLST__Kill_chain__items_changed", "gauge", "items changed"

"ksc_NLST__Kill_chain__items_deleted", "gauge", "items deleted"

"ksc_NLST__Kill_chain__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Kill_chain__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Kill_chain__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Kill_chain__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Kill_chain__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Kill_chain__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Kill_chain__transactions_in_queue", "gauge", "transactions in queue"

Nom affiché du type d'événement	ID de type d'événement	Type d'événement	Description	Durée de stockage par défaut
La restriction de la licence a été dépassée	4099	KLSRV_EV_LICENSE_CHECK_MORE_110	Une fois par jour, Kaspersky Security Center vérifie si une limite de licence est dépassée. Ce type d'événements se produit si le serveur d'administration détecte que certaines limites de licence sont dépassées par les applications Kaspersky installées sur les appareils clients et si le nombre d'unités de licence actuellement utilisé sous licence unique est supérieur à 110 % du nombre total d'unités sous licence. Même lorsque cet événement se produit, les appareils clients sont protégés. Vous pouvez répondre à l'événement des manières suivantes : • Parcourez la liste des appareils administrés. Supprimez les appareils inutilisés. • Fournissez une licence pour plusieurs appareils (ajoutez un code d'activation valide ou un fichier clé au serveur d'administration). Kaspersky Security Center définit les règles de génération d'événements lorsqu'une limite de la licence est dépassée.	180 jours
Attaque de virus	26 (pour la Protection contre les fichiers malicieux)	GNRL_EV_VIRUS_OUTBREAK	Ce type d'événements se produit lorsque le nombre d'objets malveillants détectés sur plusieurs appareils administrés dépasse le seuil sur une courte durée. Vous pouvez répondre à l'événement des manières suivantes : • Vous pouvez configurer le seuil dans les propriétés du Serveur d'administration. • Vous pouvez aussi créer une stratégie plus stricte qui sera activée ou créer une tâche qui sera exécutée quand l'événement se produit.	180 jours
Attaque de virus	27 (pour la Protection contre les menaces par emails)	GNRL_EV_VIRUS_OUTBREAK	Ce type d'événements se produit lorsque le nombre d'objets malveillants détectés sur plusieurs appareils administrés dépasse le seuil sur une courte durée. Vous pouvez répondre à l'événement des manières suivantes : • Vous pouvez configurer le seuil dans les propriétés du Serveur d'administration. • Vous pouvez aussi créer une stratégie plus stricte qui sera activée ou créer une tâche qui sera exécutée quand l'événement se produit.	180 jours
Attaque de virus	28 (pour le pare-feu)	GNRL_EV_VIRUS_OUTBREAK	Ce type d'événements se produit lorsque le nombre d'objets malveillants détectés sur plusieurs appareils administrés dépasse le seuil sur une courte durée. Vous pouvez répondre à l'événement des manières suivantes : • Vous pouvez configurer le seuil dans les propriétés du Serveur d'administration. • Vous pouvez aussi créer une stratégie plus stricte qui sera activée ou créer une tâche qui sera exécutée quand l'événement se produit.	180 jours

Nom affiché du type d'événement	ID de type d'événement	Type d'événement	Description	Durée de stockage par défaut
L'appareil n'est plus administré	4111	KLSRV_HOST_OUT_CONTROL	Des événements de ce type se produisent si un appareil administré est visible sur le réseau mais n'est pas connecté au Serveur d'administration pendant une certaine durée. Trouvez ce qui empêche le fonctionnement normal de l'Agent d'administration sur l'appareil. Les causes possibles sont des problèmes de réseau et la suppression de l'agent d'administration de l'appareil.	180 jours
L'appareil est en état Critique	4113	KLSRV_HOST_STATUS_CRITICAL	Ce type d'événements se produit lorsqu'un appareil administré a reçu l'état *Critique*. Vous pouvez configurer les conditions dans lesquelles l'état de l'appareil devient *Critique*.	180 jours
Le fichier clé a été ajouté à la liste de refus	4124	KLSRV_LICENSE_BLACKLISTED	Des événements de ce type se produisent lorsque Kaspersky a ajouté le code d'activation ou le fichier clé que vous utilisez à la liste de refus. Pour en savoir plus, contactez le Support technique.	180 jours
Mode limité	4130	KLSRV_EV_LICENSE_SRV_LIMITED_MODE	Ce type d'événements se produit lorsque Kaspersky Security Center commence à fonctionner avec les fonctionnalités de base, sans les fonctionnalités de Gestion des vulnérabilités et des correctifs et d'administration des appareils mobiles. Les causes de l'événement et les réponses appropriées sont indiquées ci-après : • La durée de validité de la licence a expiré. Fournissez une licence pour utiliser le mode de fonctionnalité complète de Kaspersky Security Center (ajoutez un code d'activation valide ou un fichier clé au Serveur d'administration). • Le serveur d'administration gère plus d'appareils que spécifié par la limite de licence. Déplacez les appareils des groupes d'administration d'un serveur d'administration vers les groupes d'un autre serveur d'administration (si permis pas la limite de licence de l'autre serveur d'administration).	180 jours

Nom affiché du type d'événement	ID de type d'événement	Type d'événement	Description	Durée de stockage par défaut
La licence expire bientôt	4129	KLSRV_EV_LICENSE_SRV_EXPIRE_SOON	Des événements de ce type se produisent lorsque la date de fin de la durée de validité de la licence commerciale approche. Une fois par jour, Kaspersky Security Center vérifie si la date de fin de la durée de validité de la licence approche. Les événements de ce type sont publiés 30 jours, 15 jours, 5 jours et 1 jour avant la date de fin de la durée de validité de la licence. Vous ne pouvez pas modifier le nombre de jours. Si le Serveur d'administration est désactivé le jour défini avant la date de fin de la durée de validité de la licence, l'événement ne sera pas publié avant le jour suivant. À l'expiration de la licence commerciale, Kaspersky Security Center ne fournit que les fonctionnalités de base. Vous pouvez répondre à l'événement des manières suivantes : • Assurez-vous qu'une clé de licence de réserve est ajoutée au Serveur d'administration. • Si vous utilisez un abonnement, assurez-vous de le renouveler. Un abonnement illimité est renouvelé automatiquement s'il a été prépayé auprès du prestataire de services à la date d'échéance.	180 jours
Le certificat a expiré	4132	KLSRV_CERTIFICATE_EXPIRED	Des événements de ce type se produisent lorsque le certificat client sur les appareils mobiles expire.	180 jours
Le certificat du Serveur d'administration a expiré.	6129	Certificat de serveur expiré	Des événements de ce type se produisent lorsque les certificats du Serveur d'administration pour les appareils mobiles et les appareils UEFI expirent. Vous devez mettre à jour le certificat expiré.	180 jours
Les mises à jour des modules des applications Kaspersky ont été rappelées	4142	KLSRV_SEAMLESS_UPDATE_REVOKED	Ce type d'événements se produit si des mises à jour continues ont été révoquées (l'état *Révoqué* est affiché pour ces mises à jour) par des spécialistes techniques de Kaspersky ; par exemple, ils doivent être mis à jour vers une version plus récente. L'événement concerne les correctifs de Kaspersky Security Center et non les modules d'applications administrés par Kaspersky. L'événement indique que les mises à jour continues ne sont pas installées.	180 jours
Audit : l'exportation vers le SIEM a échoué	5130	KLAUD_EV_SIEM_EXPORT_ERROR	Les événements de ce type se produisent lorsque l'exportation d'événements vers le système SIEM a échoué en raison d'une erreur de connexion avec le système SIEM.	180 jours

Événements liés à des erreurs de fonctionnement du Serveur d'administration

Le tableau ci-dessous indique les types d'événements du Serveur d'administration de Kaspersky Security Center au niveau de gravité **Erreur de fonctionnement**.

Pour chaque événement pouvant être généré par une application, vous pouvez spécifier les paramètres de notification et les paramètres de stockage sous l'onglet **Configuration des événements** dans la stratégie de l'application. Pour le Serveur d'administration, vous pouvez également consulter et configurer la liste des événements dans les propriétés du Serveur d'administration. Si vous souhaitez configurer les paramètres de notification pour tous les événements à la fois, configurez les paramètres de notification généraux dans les propriétés du Serveur d'administration.

Événements liés à des erreurs de fonctionnement du Serveur d'administration

Nom affiché du type d'événement	ID de type d'événement	Type d'événement	Description	Durée de stockage par défaut
Erreur du temps d'exécution	4125	KLSRV_RUNTIME_ERROR	Ce type d'événements se produit à cause de problèmes inconnus. Ce sont le plus souvent des problèmes de SGBD, de réseau et d'autres problèmes logiciels et matériels. Les détails de l'événement peuvent se trouver dans la description de l'événement.	180 jours
Pour un des groupes des applications sous licence, la limite des installations a été dépassée	4126	KLSRV_INVLICPROD_EXCEDED	Le serveur d'administration génère ce type d'événements périodiquement (toutes les heures). Ce type d'événements se produit si dans Kaspersky Security Center, vous administrez les clés d'applications tierces et si le nombre d'installations a dépassé la limite définie par la clé de licence de l'application tierce. Vous pouvez répondre à l'événement des manières suivantes : • Parcourez la liste des appareils administrés. Supprimez l'application tierce des appareils où l'application n'est pas utilisée. • Utiliser une licence tierce pour plusieurs appareils. Vous pouvez gérer les clés de licence d'applications tierces à l'aide des fonctionnalités des groupes des applications sous licence. Un groupe des applications sous licence inclut les applications tierces qui répondent aux critères que vous avez définis.	180 jours
Échec du sondage du segment dans le cloud	4143	KLSRV_KLCLOUD_SCAN_ERROR	Des événements de ce type se produisent lorsque le Serveur d'administration ne parvient pas à interroger un segment de réseau dans un environnement cloud. Lisez les détails dans la description de l'événement et répondez en conséquence.	Non stocké
Échec de la copie des mises à jour vers le dossier indiqué	4123	KLSRV_UPD_REPL_FAIL	Ce type d'événements se produit lorsque les mises à jour logicielles sont copiées dans un ou plusieurs dossier(s) partagés. Vous pouvez répondre à l'événement des manières suivantes : • Vérifiez si le compte d'utilisateur utilisé pour accéder au(x) dossier(s) est autorisé en écriture. • Vérifiez si un nom d'utilisateur et / ou un mot de passe du ou des dossiers a changé. • Vérifiez la connexion Internet, car elle peut être à l'origine de l'événement. Suivez les instructions pour mettre à jour les bases de données et es modules logiciels.	180 jours

Nom affiché du type d'événement	ID de type d'événement	Type d'événement	Description	Durée de stockage par défaut
Plus d'espace disponible sur le disque	4107	KLSRV_DISK_FULL	Des événements de ce type se produisent lorsque le disque dur de l'appareil sur lequel le Serveur d'administration est installé ne dispose plus d'espace libre. Libérez de l'espace disque sur l'appareil.	180 jours
Le dossier en accès public n'est pas disponible	4108	KLSRV_SHARED_FOLDER_UNAVAILABLE	Ce type d'événements se produit si le dossier partagé du Serveur d'administration n'est pas disponible. Vous pouvez répondre à l'événement des manières suivantes : • Vérifiez si le Serveur d'administration (où se trouve le dossier partagé) est sous tension et disponible. • Vérifiez si un nom d'utilisateur et / ou un mot de passe du dossier a changé. • Vérifiez la connexion réseau.	180 jours

Nom affiché du type d'événement	ID de type d'événement	Type d'événement	Description	Durée de stockage par défaut
La base de données du Serveur d'administration n'est pas disponible	4109	KLSRV_DATABASE_UNAVAILABLE	Ce type d'événements se produit si le Serveur d'administration n'est pas disponible. Vous pouvez répondre à l'événement des manières suivantes : • Vérifiez si le serveur distant sur lequel est installé SQL Server est disponible. • Affichez les journaux du SGBD pour trouver la raison de l'indisponibilité de la base de données du Serveur d'administration. Par exemple, un serveur distant sur lequel est installé SQL Server peut ne pas être disponible à cause de la maintenance préventive.	180 jours
Espace insuffisant dans la base de données du Serveur d'administration	4110	KLSRV_DATABASE_FULL	Ce type d'événements se produit lorsque la base de données du Serveur d'administration n'a plus d'espace libre. Le Serveur d'administration ne fonctionne pas lorsque sa base de données a atteint sa capacité maximale et que la base de données ne peut plus recevoir d'enregistrement. Les causes de cet événement, en fonction du SGBD utilisé, et les réponses appropriées à l'événement sont indiquées ci-après : • Vous utilisez le SGBD de SQL Server édition Express : Dans la documentation SQL Server Express, contrôlez la taille limite de la base de données pour la version que vous utilisez. La base de données de votre Serveur d'administration a probablement dépassé la taille limite. Limiter le nombre d'événements à stocker dans la base de données du Serveur d'administration. La base de données du Serveur d'administration contient trop d'événements envoyés par le module Contrôle des applications. Vous pouvez modifier les paramètres de la stratégie Kaspersky Endpoint Security for Windows concernant le stockage des événements du Contrôle des applications dans la base de données du Serveur d'administration. • Vous utilisez un SGBD autre que SQL Server Express Edition : Ne pas limiter le nombre d'événements à stocker dans la base de données du Serveur d'administration. Réduire la liste d'événements à stocker dans la base de données du Serveur d'administration. Consulter les informations sur la sélection du SGBD.	180 jours

Événements d'avertissement du Serveur d'administration

Le tableau ci-dessous montre les événements du Serveur d'administration de Kaspersky Security Center au niveau de gravité **Avertissement**.

Pour chaque événement pouvant être généré par une application, vous pouvez spécifier les paramètres de notification et les paramètres de stockage sous l'onglet **Configuration des événements** dans la stratégie de l'application. Pour le Serveur d'administration, vous pouvez également consulter et configurer la liste des événements dans les propriétés du Serveur d'administration. Si vous souhaitez configurer les paramètres de notification pour tous les événements à la fois, configurez les paramètres de notification généraux dans les propriétés du Serveur d'administration.

Événements d'avertissement du Serveur d'administration

Nom affiché du type d'événement	ID de type d'événement	Type d'événement	Description	Durée de stockage par défaut
Un événement fréquent a été détecté		KLSRV_EVENT_SPAM_EVENTS_DETECTED	Des événements de ce type se produisent lorsque le Serveur d'administration détecte un événement fréquent sur l'appareil administré. Pour en savoir plus sur la section suivante : Blocage des événements fréquents.	90 jours
La restriction de la licence a été dépassée	4098	KLSRV_EV_LICENSE_CHECK_100_110	Une fois par jour, Kaspersky Security Center vérifie si une limite de licence est dépassée. Ce type d'événements se produit si le serveur d'administration détecte que certaines limites de licence sont dépassées par les applications Kaspersky installées sur les appareils clients et si le nombre d'unités de licence actuellement utilisé sous licence unique représente 100 % à 110 % du nombre total d'unités sous licence. Même lorsque cet événement se produit, les appareils clients sont protégés. Vous pouvez répondre à l'événement des manières suivantes : • Parcourez la liste des appareils administrés. Supprimez les appareils inutilisés. • Fournissez une licence pour plusieurs appareils (ajoutez un code d'activation valide ou un fichier clé au serveur d'administration). Kaspersky Security Center définit les règles de génération d'événements lorsqu'une limite de la licence est dépassée.	90 jours
L'appareil est resté inactif sur le réseau depuis longtemps	4103	KLSRV_EVENT_HOSTS_NOT_VISIBLE	Des événements de ce type se produisent lorsqu'un appareil administré est inactif pendant un certain temps. Le plus souvent, cela se produit lorsqu'un appareil administré est mis hors service. Vous pouvez répondre à l'événement des manières suivantes : • Supprimez manuellement l'appareil de la liste des appareils administrés. • Spécifiez l'intervalle de temps après lequel l'événement **L'appareil est resté inactif sur le réseau depuis longtemps** est créé à l'aide de la Console d'administration ou de Kaspersky Security Center Web Console. • Spécifiez l'intervalle de temps après lequel l'appareil est automatiquement supprimé du groupe à l'aide de la Console d'administration ou de Kaspersky Security Center Web Console.	90 jours

Nom affiché du type d'événement	ID de type d'événement	Type d'événement	Description	Durée de stockage par défaut
Noms d'appareil en conflit	4102	KLSRV_EVENT_HOSTS_CONFLICT	Des événements de ce type se produisent lorsque le Serveur d'administration considère deux ou plusieurs appareils administrés comme un seul appareil. La plupart du temps, cela se produit lorsqu'un disque dur cloné a été utilisé pour déployer des logiciels sur des appareils administrés et sans que l'Agent d'administration ne passe en mode de clonage de disque dédié sur un appareil de référence. Pour éviter ce problème, passez l'Agent d'administration en mode de clonage de disque sur un appareil de référence avant de cloner le disque dur de cet appareil.	90 jours
L'appareil est en état Avertissement	4114	KLSRV_HOST_STATUS_WARNING	Ce type d'événements se produit lorsqu'un appareil administré a reçu l'état *Avertissement*. Vous pouvez configurer les conditions dans lesquelles l'état de l'appareil devient *Avertissement*.	90 jours
La limite des installations sera bientôt dépassée pour l'un des groupes d'applications sous licence	4127	KLSRV_INVLICPROD_FILLED	Des événements de ce type se produisent lorsque le nombre d'installations pour des applications tierces incluses dans un groupe des applications sous licence atteint 90 % de la valeur maximale autorisée indiquée dans les propriétés de la clé de licence. Vous pouvez répondre à l'événement des manières suivantes : • Si l'application tierce n'est pas utilisée sur certains des appareils administrés, supprimez l'application de ces appareils. • Si vous prévoyez que le nombre d'installations pour l'application tierce dépassera le nombre maximum autorisé prochainement, envisagez d'obtenir à l'avance une licence tierce pour un plus grand nombre d'appareils. Vous pouvez gérer les clés de licence d'applications tierces à l'aide des fonctionnalités des groupes des applications sous licence.	90 jours
Le certificat a été demandé	4133	KLSRV_CERTIFICATE_REQUESTED	Des événements de ce type se produisent lorsqu'un certificat pour l'administration des appareils mobiles ne parvient pas à être réémis automatiquement. Les causes et les réponses appropriées à cet événement peuvent être les suivantes : • La réémission automatique a été lancée pour un certificat pour lequel l'option **Réémettre automatiquement le certificat si possible** est désactivée. Cela peut être dû à une erreur qui s'est produite lors de la création du certificat. Il peut être nécessaire d'émettre à nouveau le certificat manuellement. • Si vous utilisez une intégration avec une infrastructure à clé publique, la cause peut être l'absence d'un attribut SAM-Account-Name du compte utilisé pour l'intégration avec PKI et pour l'émission du certificat. Vérifiez les propriétés du compte.	90 jours

Nom affiché du type d'événement	ID de type d'événement	Type d'événement	Description	Durée de stockage par défaut
Le certificat a été supprimé	4134	KLSRV_CERTIFICATE_REMOVED	Des événements de ce type se produisent lorsqu'un administrateur supprime tout type de certificat (général, email, VPN) pour l'Administration des appareils mobiles. Une fois qu'un certificat aura été supprimé, les appareils mobiles connectés via ce certificat ne parviendront pas à se connecter au Serveur d'administration. Cet événement pourrait être utile lors d'une enquête sur les dysfonctionnements liés à l'administration des appareils mobiles.	90 jours
Le certificat expire	6128	Le certificat du serveur expire bientôt	Des événements de ce type se produisent lorsque les certificats du Serveur d'administration pour les appareils mobiles et les appareils UEFI expirent. Vous devez mettre à jour le certificat expiré.	90 jours
La durée de validité du certificat APNs a expiré	4135	KLSRV_APN_CERTIFICATE_EXPIRED	Des événements de ce type se produisent lorsqu'un certificat APNs expire. Vous devez renouveler manuellement le certificat APNs et l'installer sur un serveur MDM iOS.	Non stocké
La durée de validité du certificat APNs expire bientôt	4136	KLSRV_APN_CERTIFICATE_EXPIRES_SOON	Les événements de ce type se produisent lorsqu'il reste moins de 14 jours avant l'expiration du certificat APNs. Lorsque le certificat APNs expire, vous devez renouveler manuellement le certificat APNs et l'installer sur un serveur MDM iOS. Nous vous recommandons de planifier le renouvellement du certificat APNs avant la date d'expiration.	Non stocké
Échec de l'envoi d'un message FCM sur l'appareil mobile	4138	KLSRV_GCM_DEVICE_ERROR	Des événements de ce type se produisent lorsque l'Administration des appareils mobiles est configurée de façon à utiliser Firebase Cloud Messaging (FCM) pour se connecter aux appareils mobiles administrés avec un système d'exploitation Android et que le serveur FCM ne parvient pas à traiter certaines des requêtes reçues de la part du Serveur d'administration. Cela signifie que certains des appareils mobiles administrés ne recevront aucune notification push. Lisez le code HTTP dans les détails de la description de l'événement et répondez en conséquence. Pour en savoir plus sur les codes HTTP reçus de la part du serveur FCM et sur les erreurs qui y sont liées, veuillez consulter la documentation du service Firebase (voir le chapitre « Codes de réponse d'erreur aux messages en aval »).	90 jours

Nom affiché du type d'événement	ID de type d'événement	Type d'événement	Description	Durée de stockage par défaut
Erreur HTTP lors de l'envoi d'un message FCM sur le serveur FCM	4139	KLSRV_GCM_HTTP_ERROR	Des événements de ce type se produisent lorsque l'Administration des appareils mobiles est configurée de façon à utiliser Firebase Cloud Messaging (FCM) pour connecter les appareils mobiles administrés avec le système d'exploitation Android et que le serveur FCM revient à la requête du Serveur d'administration avec un code HTTP différent de 200 (OK). Les causes et les réponses appropriées à cet événement peuvent être les suivantes : • Problèmes du côté du serveur FCM. Lisez le code HTTP dans les détails de la description de l'événement et répondez en conséquence. Pour en savoir plus sur les codes HTTP reçus de la part du serveur FCM et sur les erreurs qui y sont liées, veuillez consulter la documentation du service Firebase (voir le chapitre « Codes de réponse d'erreur aux messages en aval »). • Problèmes du côté du serveur proxy (si vous utilisez un serveur proxy). Lisez le code HTTP dans les détails de la description de l'événement et répondez en conséquence.	90 jours
Échec de l'envoi d'un message FCM sur le serveur FCM	4140	KLSRV_GCM_GENERAL_ERROR	Des événements de ce type se produisent en raison d'erreurs inattendues du côté du Serveur d'administration lors de l'utilisation du protocole HTTP de Firebase Cloud Messaging. Lisez les détails dans la description de l'événement et répondez en conséquence. Si vous ne pouvez pas trouver la solution à un problème par vous-même, nous vous recommandons de contacter le Support Technique de Kaspersky.	90 jours
Espace libre insuffisant sur le disque dur	4105	KLSRV_NO_SPACE_ON_VOLUMES	Des événements de ce type se produisent lorsque le disque dur de l'appareil sur lequel le Serveur d'administration est installé ne dispose presque plus d'espace libre. Libérez de l'espace disque sur l'appareil.	90 jours

Nom affiché du type d'événement	ID de type d'événement	Type d'événement	Description	Durée de stockage par défaut
Trop peu d'espace disponible dans la base de données du Serveur d'administration	4106	KLSRV_NO_SPACE_IN_DATABASE	Ce type d'événements se produit si l'espace de la base de données du Serveur d'administration est trop limité. Si vous ne corrigez pas la situation, quand la base de données du Serveur d'administration atteindra sa pleine capacité, le Serveur d'administration ne fonctionnera plus. Les causes de cet événement, en fonction du SGBD utilisé, et les réponses appropriées à l'événement sont indiquées ci-après. Vous utilisez le SGBD de SQL Server édition Express : • Dans la documentation SQL Server Express, contrôlez la taille limite de la base de données pour la version que vous utilisez. La base de données de votre Serveur d'administration est probablement tout près d'atteindre la taille limite. • Limiter le nombre d'événements à stocker dans la base de données du Serveur d'administration. • La base de données du Serveur d'administration contient trop d'événements envoyés par le module Contrôle des applications. Vous pouvez modifier les paramètres de la stratégie Kaspersky Endpoint Security for Windows concernant le stockage des événements du Contrôle des applications dans la base de données du Serveur d'administration. Vous utilisez un SGBD autre que SQL Server Express Edition : • Ne pas limiter le nombre d'événements à stocker dans la base de données du Serveur d'administration • Réduire la liste d'événements à stocker dans la base de données du Serveur d'administration Consulter les informations sur la sélection du SGBD.	90 jours
La connexion au Serveur d'administration secondaire a été perdue	4116	KLSRV_EV_SLAVE_SRV_DISCONNECTED	Des événements de ce type se produisent lorsqu'une connexion au Serveur d'administration secondaire est interrompue. Lisez le journal des événements Kaspersky sur l'appareil où le Serveur d'administration secondaire est installé et répondez en conséquence.	90 jours
La connexion au Serveur d'administration principal a été interrompue	4118	KLSRV_EV_MASTER_SRV_DISCONNECTED	Des événements de ce type se produisent lorsqu'une connexion au Serveur d'administration principal est interrompue. Lisez le journal des événements Kaspersky sur l'appareil où le Serveur d'administration principal est installé et répondez en conséquence.	90 jours

Nom affiché du type d'événement	ID de type d'événement	Type d'événement	Description	Durée de stockage par défaut
Les nouvelles mises à jour des modules des applications Kaspersky ont été enregistrées	4141	KLSRV_SEAMLESS_UPDATE_REGISTERED	Des événements de ce type se produisent lorsque le Serveur d'administration enregistre de nouvelles mises à jour pour le logiciel Kaspersky installé sur des appareils administrés dont l'installation nécessite une autorisation. Approuvez ou refusez les mises à jour à l'aide de la Console d'administration ou de Kaspersky Security Center Web Console.	90 jours
La limite du nombre d'événements dans la base de données est dépassée, la suppression des événements a commencé	4145	KLSRV_EVP_DB_TRUNCATING	Ce type d'événements se produit lorsque la suppression des anciens événements de la base de données du Serveur d'administration commence une fois que la base de données du Serveur d'administration a atteint sa capacité. Vous pouvez répondre à l'événement des manières suivantes : • Modifiez le nombre maximal d'événements stockés dans la base de données du Serveur d'administration • Réduire la liste d'événements à stocker dans la base de données du Serveur d'administration	Non stocké
La limite du nombre d'événements dans la base de données est dépassée, les événements ont été supprimés	4146	KLSRV_EVP_DB_TRUNCATED	Ce type d'événements se produit lorsque d'anciens événements ont été supprimés de la base de données du Serveur d'administration une fois que la base de données du Serveur d'administration a atteint sa capacité. Vous pouvez répondre à l'événement des manières suivantes : • Modifiez le nombre maximal autorisé d'événements stockés dans la base de données du Serveur d'administration • Réduire la liste d'événements à stocker dans la base de données du Serveur d'administration	Non stocké
Audit (échec du test de connexion au serveur SIEM)	5120	KLAUD_EV_SIEM_TEST_FAILED	Les événements de ce type se produisent lorsqu'un test de connexion au serveur SIEM a échoué.	30 jours
Échec de l'émission automatique du certificat		KLSRV_CERTIFICATE_AUTO_ISSUE_ERROR	Cet événement se produit en cas d'erreur lors de la création d'un certificat client pour un appareil mobile (un appareil fonctionnant sous un protocole mobile).	90 jours

Événements d'information du Serveur d'administration

Le tableau ci-dessous montre les événements du Serveur d'administration de Kaspersky Security Center au niveau de gravité **Information**.

Événements d'information du Serveur d'administration

Nom affiché du type d'événement	ID de type d'événement	Type d'événement	Durée de stockage par défaut	Remarques
Clé de licence utilisée à plus de 90 %	4097	KLSRV_EV_LICENSE_CHECK_90	30 jours	
Un nouvel appareil a été détecté	4100	KLSRV_EVENT_HOSTS_NEW_DETECTED	30 jours	

Nom affiché du type d'événement	ID de type d'événement	Type d'événement	Durée de stockage par défaut	Remarques
L'appareil a été ajouté automatiquement au groupe	4101	KLSRV_EVENT_HOSTS_NEW_REDIRECTED	30 jours	
L'appareil a été déplacé automatiquement selon la règle	1074	KLSRV_HOST_MOVED_WITH_RULE_EX	30 jours	
L'appareil a été supprimé du groupe : longue absence d'activité sur le réseau	4104	KLSRV_INVISIBLE_HOSTS_REMOVED	30 jours	
Pour un des groupes des applications sous licence, le nombre d'installations autorisées est épuisé à plus de 95 %	4128	KLSRV_INVLICPROD_EXPIRED_SOON	30 jours	
Des fichiers à envoyer à Kaspersky pour analyse ont été détectés	4131	KLSRV_APS_FILE_APPEARED	30 jours	
L'ID d'instance FCM de l'appareil mobile a modifié	4137	KLSRV_GCM_DEVICE_REGID_CHANGED	30 jours	
Les mises à jour ont bien été copiées dans le dossier indiqué	4122	KLSRV_UPD_REPL_OK	30 jours	
La connexion au Serveur d'administration secondaire a été établie	4115	KLSRV_EV_SLAVE_SRV_CONNECTED	30 jours	
La connexion au Serveur d'administration principal a été établie	4117	KLSRV_EV_MASTER_SRV_CONNECTED	30 jours	
Les bases de données ont été mises à jour	4144	KLSRV_UPD_BASES_UPDATED	30 jours	
Audit : une connexion au Serveur d'administration a été établie	4147	KLAUD_EV_SERVERCONNECT	30 jours	
Audit : un objet a été modifié	4148	KLAUD_EV_OBJECTMODIFY	30 jours	Cet événement permet de suivre les modifications apportées aux objets suivants : • Groupe d'administration • Groupe de sécurité • Utilisateur • Paquet • Tâche • Stratégie • Serveur • Serveur virtuel
Audit : l'état de l'objet a été modifié	4150	KLAUD_EV_TASK_STATE_CHANGED	30 jours	Par exemple, cet événement se produit lorsqu'une tâche a échoué avec une erreur.
Audit : les paramètres de groupe ont été modifiés	4149	KLAUD_EV_ADMGROUP_CHANGED	30 jours	
Audit : la connexion au Serveur d'administration a été interrompue	4151	KLAUD_EV_SERVERDISCONNECT	30 jours	

Nom affiché du type d'événement	ID de type d'événement	Type d'événement	Durée de stockage par défaut	Remarques
Audit : les propriétés de l'objet ont été modifiées	4152	KLAUD_EV_OBJECTPROPMODIFIED	30 jours	Cet événement suit les modifications apportées aux propriétés suivantes : • Utilisateur • Licence • Serveur • Serveur virtuel
Audit : les autorisations de l'utilisateur ont été modifiées	4153	KLAUD_EV_OBJECTACLMODIFIED	30 jours	
Audit : les clés de chiffrement ont été importées ou exportées à partir du Serveur d'administration	5100	KLAUD_EV_DPEKEYSEXPORT	30 jours	
Audit (le test de connexion au serveur SIEM a réussi)	5110	KLAUD_EV_SIEM_TEST_SUCCESS	30 jours	Les événements de ce type se produisent lorsqu'un test de connexion au serveur SIEM a réussi.
Certificat de réserve créé		Certificat de réserve de serveur créé	30 jours	Cet événement se produit lorsqu'un certificat de Serveur d'administration a été créé.
Renouvellement du certificat		Certificat de serveur renouvelé	30 jours	Cet événement se produit lorsque le certificat du Serveur d'administration a été renouvelé.
Le certificat a été émis automatiquement		KLSRV_CERTIFICATE_AUTO_ISSUED	30 jours	Cet événement se produit lorsqu'un certificat pour un appareil mobile (un appareil fonctionnant sous un protocole mobile) a été créé.

Les événements **Certificat de réserve créé, Renouvellement du certificat** et **Le certificat a été émis automatiquement** sont publiés automatiquement par le Serveur d'administration et affichés dans la Console d'administration uniquement lorsque les opérations correspondant à ces événements sont exécutées pour les certificats de Serveur d'administration pour les appareils mobiles et les appareils UEFI.

Événements de l'Agent d'administration

Cette section contient des informations sur les événements liés à l'agent d'administration.

Événements liés aux erreurs de fonctionnement de l'Agent d'administration

Le tableau ci-dessous indique les types d'événements de l'Agent d'administration de Kaspersky Security Center, regroupés par niveau de sécurité **Erreur de fonctionnement**.

Pour chaque événement pouvant être généré par une application, vous pouvez spécifier les paramètres de notification et les paramètres de stockage sous l'onglet **Configuration des événements** dans la stratégie de l'application. Si vous souhaitez configurer les paramètres de notification pour tous les événements à la fois, configurez les paramètres de notification généraux dans les propriétés du Serveur d'administration.

Nom affiché du type d'événement	ID de type d'événement	Type d'événement	Description	Durée de stockage par défaut
Erreur d'installation de la mise à jour	7702	KLNAG_EV_PATCH_INSTALL_ERROR	Des événements de ce type se produisent si l'Installation automatique des mises à jour et des correctifs pour les modules de Kaspersky Security Center ne réussit pas. L'événement ne concerne pas les mises à jour des applications Kaspersky administrées. Lisez la description de l'événement. Cet événement peut être dû à un problème Windows sur le serveur d'administration. Si la description mentionne un problème de configuration Windows, résolvez le problème.	30 jours
Échec de l'installation de la mise à jour du logiciel tiers	7697	KLNAG_EV_3P_PATCH_INSTALL_ERROR	Des événements de ce type se produisent si les fonctionnalités de la gestion des vulnérabilités et des correctifs et d'Administration des appareils mobiles sont en cours d'utilisation, et si la mise à jour des logiciels tiers n'a pas réussi. Vérifiez si le lien vers le logiciel tiers est valide. Lisez la description de l'événement.	30 jours
Échec de l'installation des mises à jour Windows Update	7717	KLNAG_EV_WUA_INSTALL_ERROR	Ce type d'événements se produit si les mises à jour Windows échouent. Configurez les mises à jour Windows dans une stratégie d'Agent d'administration. Lisez la description de l'événement. Recherchez l'erreur dans la base de connaissance Microsoft. Contactez le Support Technique de Microsoft si vous ne parvenez pas à résoudre le problème vous-même.	30 jours
Gestion des utilisateurs : erreurs	7723	KLNAG_EV_USR_MNG_ERR	Événement d'avertissement général.	30 jours
Impossible de restaurer le fichier sudoers à la valeur de référence	7726	KLNAG_EV_SUDOER_RESTORED_ERR	L'événement contient la description de l'erreur de remplacement du fichier sudoers.	30 jours
Il est impossible d'installer les certificats racine	7728	KLNAG_EV_ROOT_CERT_INSTALL_ERR	L'événement contient la description de l'erreur d'installation des certificats.	30 jours
Impossible de supprimer les certificats racine	7730	KLNAG_EV_ROOT_CERT_REMOVE_ERR	L'événement contient la description de l'erreur de suppression des certificats.	30 jours

Événements d'avertissement de l'Agent d'administration

Le tableau suivant reprend les événements de l'Agent d'administration de Kaspersky Security Center, regroupés par niveau de gravité **Avertissement**.

Pour chaque événement pouvant être généré par une application, vous pouvez spécifier les paramètres de notification et les paramètres de stockage sous l'onglet **Configuration des événements** dans la stratégie de l'application. Si vous souhaitez configurer les paramètres de notification pour tous les événements à la fois, configurez les paramètres de notification généraux dans les propriétés du Serveur d'administration.

Événements d'avertissement de l'Agent d'administration

Nom affiché du type d'événement	ID de type d'événement	Type d'événement	Durée de stockage par défaut
Avertissement renvoyé lors de l'installation des mises à jour des modules de l'application	7701	KLNAG_EV_PATCH_INSTALL_WARNING	30 jours
L'installation de la mise à jour du logiciel tiers s'est terminée avec un avertissement	7696	KLNAG_EV_3P_PATCH_INSTALL_WARNING	30 jours
L'installation de la mise à jour du logiciel tiers a été reportée	7698	KLNAG_EV_3P_PATCH_INSTALL_SLIPPED	30 jours
Un problème de sécurité est survenu	549	GNRL_EV_APP_INCIDENT_OCCURED	30 jours
Le proxy KSN a démarré. Échec de la vérification de la disponibilité de KSN	7718	KSNPROXY_STARTED_CON_CHK_FAILED	30 jours
Gestion des utilisateurs : avertissements	7722	KLNAG_EV_USR_MNG_WRN	30 jours
Le fichier Sudoers ne correspond pas à la valeur de référence	7724	KLNAG_EV_SUDOER_DIFFERENT	30 jours

Événements informatifs de l'Agent d'administration

Le tableau suivant reprend les événements de l'Agent d'administration de Kaspersky Security Center, regroupés par niveau de gravité **Information**.

Pour chaque événement pouvant être généré par une application, vous pouvez spécifier les paramètres de notification et les paramètres de stockage sous l'onglet **Configuration des événements** dans la stratégie de l'application. Si vous souhaitez configurer les paramètres de notification pour tous les événements à la fois, configurez les paramètres de notification généraux dans les propriétés du Serveur d'administration.

Événements informatifs de l'Agent d'administration

Nom affiché du type d'événement	ID de type d'événement	Type d'événement	Durée de stockage par défaut
La mise à jour des modules de l'application a bien été appliquée	7699	KLNAG_EV_PATCH_INSTALLED_SUCCESSFULLY	30 jours
L'installation de la mise à jour du module logiciel est lancée	7700	KLNAG_EV_PATCH_INSTALL_STARTING	30 jours
L'application a été installée	7703	KLNAG_EV_INV_APP_INSTALLED	30 jours
L'application a été désinstallée	7704	KLNAG_EV_INV_APP_UNINSTALLED	30 jours
L'application contrôlée a été installée	7705	KLNAG_EV_INV_OBS_APP_INSTALLED	30 jours
L'application contrôlée a été désinstallée	7706	KLNAG_EV_INV_OBS_APP_UNINSTALLED	30 jours
L'application tierce a été installée	7707	KLNAG_EV_INV_CMPTR_APP_INSTALLED	30 jours
Un nouvel appareil a été ajouté	7708	KLNAG_EV_DEVICE_ARRIVAL	30 jours
L'appareil a été supprimé	7709	KLNAG_EV_DEVICE_REMOVE	30 jours
Un nouvel appareil a été détecté	7710	KLNAG_EV_NAC_DEVICE_DISCOVERED	30 jours
L'appareil a été autorisé	7711	KLNAG_EV_NAC_HOST_AUTHORIZED	30 jours
Partage du bureau Windows : le fichier est lu	7712	KLUSRLOG_EV_FILE_READ	30 jours
Partage du bureau Windows : le fichier a été modifié	7713	KLUSRLOG_EV_FILE_MODIFIED	30 jours
Partage du bureau Windows : l'application a démarré	7714	KLUSRLOG_EV_PROCESS_LAUNCHED	30 jours
Partage du bureau Windows : lancé	7715	KLUSRLOG_EV_WDS_BEGIN	30 jours
Partage du bureau Windows : arrêté	7716	KLUSRLOG_EV_WDS_END	30 jours

Nom affiché du type d'événement	ID de type d'événement	Type d'événement	Durée de stockage par défaut
L'installation de la mise à jour d'un logiciel tiers a réussi	7694	KLNAG_EV_3P_PATCH_INSTALLED_SUCCESSFULLY	30 jours
L'installation de la mise à jour du logiciel tiers est lancée	7695	KLNAG_EV_3P_PATCH_INSTALL_STARTING	30 jours
Le proxy KSN a démarré. La vérification de la disponibilité de KSN a réussi	7719	KSNPROXY_STARTED_CON_CHK_OK	30 jours
Le serveur proxy KSN a été arrêté	7720	KSNPROXY_STOPPED	30 jours

Événements du Serveur MDM iOS

Cette section contient des informations sur les événements liés au serveur MDM iOS.

Événements liés aux erreurs de fonctionnement du Serveur MDM iOS

Le tableau suivant reprend les événements du Serveur MDM iOS de Kaspersky Security Center, regroupés par niveau de gravité **Erreur de fonctionnement**.

Pour chaque événement pouvant être généré par une application, vous pouvez spécifier les paramètres de notification et les paramètres de stockage sous l'onglet **Configuration des événements** dans la stratégie de l'application. Si vous souhaitez configurer les paramètres de notification pour tous les événements à la fois, configurez les paramètres de notification généraux dans les propriétés du Serveur d'administration.

Événements liés aux erreurs de fonctionnement du Serveur MDM iOS

Nom affiché du type d'événement	Type d'événement	Durée de stockage par défaut
Il est impossible de demander la liste des profils	PROFILELIST_COMMAND_FAILED	30 jours
Il est impossible d'installer le profil	INSTALLPROFILE_COMMAND_FAILED	30 jours
Il est impossible de supprimer le profil	REMOVEPROFILE_COMMAND_FAILED	30 jours
Il est impossible de demander la liste des profils provisioning	PROVISIONINGPROFILELIST_COMMAND_FAILED	30 jours
Il est impossible d'installer le profil provisioning	INSTALLPROVISIONINGPROFILE_COMMAND_FAILED	30 jours
Il est impossible de supprimer le profil provisioning	REMOVEPROVISIONINGPROFILE_COMMAND_FAILED	30 jours
Il est impossible de demander la liste des certificats	CERTIFICATELIST_COMMAND_FAILED	30 jours
Il est impossible de demander la liste des applications installées	INSTALLEDAPPLICATIONLIST_COMMAND_FAILED	30 jours
Il est impossible de demander les informations générales sur l'appareil mobile	DEVICEINFORMATION_COMMAND_FAILED	30 jours
Il est impossible de demander les informations sur la sécurité	SECURITYINFO_COMMAND_FAILED	30 jours
Impossible de verrouiller l'appareil mobile	DEVICELOCK_COMMAND_FAILED	30 jours
Il est impossible de purger le mot de passe	CLEARPASSCODE_COMMAND_FAILED	30 jours
Échec de la suppression des données de l'appareil mobile	ERASEDEVICE_COMMAND_FAILED	30 jours
Il est impossible d'installer l'application	INSTALLAPPLICATION_COMMAND_FAILED	30 jours
Il est impossible d'installer le code rédemption pour l'application	APPLYREDEMPTIONCODE_COMMAND_FAILED	30 jours

Nom affiché du type d'événement	Type d'événement	Durée de stockage par défaut
Il est impossible de demander la liste des apps administrées	MANAGEDAPPLICATIONLIST_COMMAND_FAILED	30 jours
Il est impossible de supprimer l'app administrée	REMOVEAPPLICATION_COMMAND_FAILED	30 jours
Les paramètres d'itinérance sont rejetés	SETROAMINGSETTINGS_COMMAND_FAILED	30 jours
Une erreur s'est produite dans le fonctionnement de l'app	PRODUCT_FAILURE	30 jours
Le résultat d'exécution de la commande contient les données incorrectes	MALFORMED_COMMAND	30 jours
Il est impossible d'envoyer une notification (Push Notification)	SEND_PUSH_NOTIFICATION_FAILED	30 jours
Il est impossible d'envoyer une commande	SEND_COMMAND_FAILED	30 jours
L'appareil est introuvable	DEVICE_NOT_FOUND	30 jours

Événements d'avertissement du Serveur MDM iOS

Le tableau suivant affiche les événements du Serveur MDM iOS de Kaspersky Security Center dont le niveau de gravité est **Avertissement**.

Pour chaque événement pouvant être généré par une application, vous pouvez spécifier les paramètres de notification et les paramètres de stockage sous l'onglet **Configuration des événements** dans la stratégie de l'application. Si vous souhaitez configurer les paramètres de notification pour tous les événements à la fois, configurez les paramètres de notification généraux dans les propriétés du Serveur d'administration.

Événements d'avertissement du Serveur MDM iOS

Nom affiché du type d'événement	Type d'événement	Durée de stockage par défaut
Tentative de connexion d'un appareil mobile verrouillé	INACTICE_DEVICE_TRY_CONNECTED	30 jours
Le profil est supprimé	MDM_PROFILE_WAS_REMOVED	30 jours
Tentative de réutilisation du certificat client	CLIENT_CERT_ALREADY_IN_USE	30 jours
Un appareil inactif a été détecté	FOUND_INACTIVE_DEVICE	30 jours
Le code rédemption est requis	NEED_REDEMPTION_CODE	30 jours
Le profil a été inclus dans une stratégie supprimée de l'appareil	UMDM_PROFILE_WAS_REMOVED	30 jours

Événements d'information du Serveur MDM iOS

Le tableau suivant reprend les événements du Serveur MDM iOS de Kaspersky Security Center, regroupés par niveau de gravité **Information**.

Pour chaque événement pouvant être généré par une application, vous pouvez spécifier les paramètres de notification et les paramètres de stockage sous l'onglet **Configuration des événements** dans la stratégie de l'application. Si vous souhaitez configurer les paramètres de notification pour tous les événements à la fois, configurez les paramètres de notification généraux dans les propriétés du Serveur d'administration.

Événements d'information du Serveur MDM iOS

Nom affiché du type d'événement	Type d'événement	Durée de stockage par défaut
Un nouvel appareil mobile est connecté	NEW_DEVICE_CONNECTED	30 jours
La demande de la liste des profils est exécutée avec succès	PROFILELIST_COMMAND_SUCCESSFULL	30 jours

Nom affiché du type d'événement	Type d'événement	Durée de stockage par défaut
L'installation du profil est exécutée avec succès	INSTALLPROFILE_COMMAND_SUCCESSFULL	30 jours
La suppression du profil est exécutée avec succès	REMOVEPROFILE_COMMAND_SUCCESSFULL	30 jours
La demande de la liste des profils provisioning est exécutée avec succès	PROVISIONINGPROFILELIST_COMMAND_SUCCESSFULL	30 jours
L'installation du profil provisioning est exécutée avec succès	INSTALLPROVISIONINGPROFILE_COMMAND_SUCCESSFULL	30 jours
La suppression du profil provisioning est exécutée avec succès	REMOVEPROVISIONINGPROFILE_COMMAND_SUCCESSFULL	30 jours
La demande de la liste des certificats numériques est exécutée avec succès	CERTIFICATELIST_COMMAND_SUCCESSFULL	30 jours
La demande de la liste des applications installées est exécutée avec succès	INSTALLEDAPPLICATIONLIST_COMMAND_SUCCESSFULL	30 jours
La demande des informations générales sur l'appareil mobile est exécutée avec succès	DEVICEINFORMATION_COMMAND_SUCCESSFULL	30 jours
La demande des informations sur la sécurité est exécutée avec succès	SECURITYINFO_COMMAND_SUCCESSFULL	30 jours
L'appareil mobile est bloqué avec succès	DEVICELOCK_COMMAND_SUCCESSFULL	30 jours
La purge du mot de passe est exécutée avec succès	CLEARPASSCODE_COMMAND_SUCCESSFULL	30 jours
Les données ont été supprimées de l'appareil mobile	ERASEDEVICE_COMMAND_SUCCESSFULL	30 jours
L'installation de l'application est exécutée avec succès	INSTALLAPPLICATION_COMMAND_SUCCESSFULL	30 jours
L'installation du code rédemption pour l'application a réussi	APPLYREDEMPTIONCODE_COMMAND_SUCCESSFULL	30 jours
La demande de la liste des apps administrées est exécutée avec succès	MANAGEDAPPLICATIONLIST_COMMAND_SUCCESSFULL	30 jours
L'application administrée a été supprimée avec succès	REMOVEAPPLICATION_COMMAND_SUCCESSFULL	30 jours
Les paramètres d'itinérance ont été appliqués	SETROAMINGSETTINGS_COMMAND_SUCCESSFUL	30 jours

Blocage des événements fréquents

Cette section fournit des informations concernant la gestion du blocage des événements fréquents, la suppression du blocage des événements fréquents et l'exportation de la liste des événements fréquents vers un fichier.

À propos du blocage des événements fréquents

Une application administrée, par exemple Kaspersky Endpoint Security for Windows, installée sur un ou plusieurs appareils administrés peut envoyer de nombreux événements du même type au Serveur d'administration. La réception d'événements fréquents peut surcharger la base de données du Serveur d'administration et écraser d'autres événements. Le Serveur d'administration commence à bloquer les événements les plus fréquents lorsque le nombre de tous les événements reçus dépasse la limite indiquée pour la base de données.

Le Serveur d'administration bloque la réception automatique des événements fréquents. Vous ne pouvez pas bloquer vous-même les événements fréquents ni choisir les événements à bloquer.

Si vous voulez découvrir si un événement est bloqué, vous pouvez vérifier si cet événement est présent dans la section **Blocage d'événements fréquents** des propriétés du Serveur d'administration. Si l'événement est bloqué, vous pouvez effectuer l'une des opérations suivantes :

- Si vous voulez éviter d'écraser la base de données, vous pouvez continuer à bloquer la réception de ce type d'événements.
- Si vous voulez, par exemple, trouver la raison de l'envoi des événements fréquents au Serveur d'administration, vous pouvez débloquer les événements fréquents et continuer à recevoir les événements de ce type de toute façon.
- Si vous souhaitez continuer à recevoir les événements fréquents jusqu'à ce qu'ils soient de nouveau bloqués, vous pouvez supprimer le blocage des événements fréquents.

Gestion du blocage des événements fréquents

Le Serveur d'administration bloque automatiquement la réception d'événements fréquents, mais vous pouvez arrêter le blocage et continuer à recevoir des événements fréquents. Vous pouvez également bloquer la réception d'événements fréquents que vous avez débloqués auparavant.

Pour administrer le blocage des événements fréquents, procédez comme suit :

1. Dans l'arborescence de la console de Kaspersky Security Center, ouvrez le menu contextuel du dossier **Serveur d'administration** d'un clic droit, puis sélectionnez l'option **Propriétés**.
2. Dans la fenêtre des propriétés du Serveur d'administration, accédez au volet **Sections**, puis sélectionnez **Blocage d'événements fréquents**.
3. Dans la section **Blocage d'événements fréquents** :
   - Sélectionnez les options **Type d'événement** des événements dont vous souhaitez bloquer la réception.
   - Désélectionnez les options **Type d'événement** des événements que vous souhaitez continuer à recevoir.
4. Cliquez sur le bouton **Appliquer**.
5. Cliquez sur le bouton **OK**.

Le Serveur d'administration reçoit les événements fréquents pour lesquels vous avez désélectionné l'option **Type d'événement** et bloque la réception des événements fréquents pour lesquels vous avez sélectionné l'option **Type d'événement**.

Suppression du blocage des événements fréquents

Vous pouvez supprimer le blocage des événements fréquents et commencer à recevoir ces événements jusqu'à ce que le Serveur d'administration bloque de nouveau ce type d'événements fréquents.

Pour supprimer le blocage des événements fréquents, procédez comme suit :

1. Dans l'arborescence de la console de Kaspersky Security Center, ouvrez le menu contextuel du dossier **Serveur d'administration** d'un clic droit, puis sélectionnez l'option **Propriétés**.
2. Dans la fenêtre des propriétés du Serveur d'administration, accédez au volet **Sections**, puis sélectionnez **Blocage d'événements fréquents**.
3. Dans la section **Blocage d'événements fréquents**, cliquez sur la ligne de l'événement fréquent pour lequel vous souhaitez supprimer le blocage.
4. Cliquez sur le bouton **Supprimer**.

L'événement fréquent est supprimé de la liste des événements fréquents. Le Serveur d'administration recevra des événements de ce type.

Exportation d'une liste d'événements fréquents vers un fichier

Pour exporter une liste d'événements fréquents vers un fichier, procédez comme suit :

1. Dans l'arborescence de la console de Kaspersky Security Center, ouvrez le menu contextuel du dossier **Serveur d'administration** d'un clic droit, puis sélectionnez l'option **Propriétés**.
2. Dans la fenêtre des propriétés du Serveur d'administration, accédez au volet **Sections**, puis sélectionnez **Blocage d'événements fréquents**.
3. Cliquez sur le bouton **Exporter dans un fichier**.
4. Dans la fenêtre **Enregistrer sous** qui s'ouvre, indiquez le chemin d'accès au fichier dans lequel vous souhaitez enregistrer la liste.
5. Cliquez sur **Enregistrer**.

Tous les enregistrements de la liste des événements fréquents sont exportés vers un fichier.

Contrôle de modification de l'état des machines virtuelles

Le Serveur d'administration conserve les informations sur l'état des appareils administrés, par exemple, le registre du matériel et la liste des appareils administrés, les paramètres des applications administrées, des tâches et des stratégies. Si une machine virtuelle est un appareil administré, l'utilisateur peut à tout moment restaurer son état depuis l'image de la machine virtuelle (snapshot), faite auparavant. Finalement, les informations sur l'état de la machine virtuelle sur le Serveur d'administration peuvent dépasser.

Par exemple, à 12h00 l'administrateur a créé sur le Serveur d'administration une stratégie de protection qui a commencé à fonctionner à 12h01 sur la machine virtuelle VM_1. À 12h30 l'utilisateur de la machine virtuelle VM_1 a modifié son état, en exécutant le restauration depuis l'image faite à 11h00. La stratégie de protection ne fonctionne plus sur la machine virtuelle. Cependant, le Serveur d'administration contient les informations dépassées sur le fait que la stratégie de protection sur la machine virtuelle VM_1 continue son fonctionnement.

Kaspersky Security Center permet de surveiller la modification de l'état des machines virtuelles.

Après chaque synchronisation avec l'appareil, le Serveur d'administration crée un identificateur unique qui est conservé sur l'appareil et sur le Serveur d'administration. Avant de commencer la synchronisation suivante, le Serveur d'administration compare les valeurs des identificateurs de deux côtés. Si les valeurs des identificateurs ne coïncident pas, le Serveur d'administration considère la machine virtuelle comme une machine restaurée depuis l'image. Le Serveur d'administration remet à zéro les paramètres des tâches et des stratégies, valables pour cette machine virtuelle, et envoie à celle-ci les stratégies à jour, ainsi que la liste des tâches de groupe.

Suivi de l'état de la protection antivirus à l'aide d'informations du registre système

Pour surveiller l'état de la protection antivirus sur l'appareil client à l'aide des informations enregistrées par l'Agent d'administration en fonction du système d'exploitation de l'appareil, procédez comme suit :

- Sur les appareils exécutant Windows :

  1. Ouvrez le registre système de l'appareil client (par exemple, localement à l'aide de la commande regedit dans le menu **Démarrer** → **Exécuter**).

  2. Rendez-vous dans la section :

     - Pour les systèmes 32 bits :

       HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1103\1.0.0.0\Statistics\AVState

     - Pour les systèmes 64 bits :

       HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1103\1.0.0.0\Stati

     Ainsi, le registre système affichera les informations sur l'état de la protection antivirus de l'appareil client.

- Sur les appareils fonctionnant sous Linux :

  - Les informations sont contenues dans des fichiers texte séparés, un pour chaque type de données, situés dans /var/opt/kaspersky/klnagent/1103/1.0.0.0/Statistics/AVState/.

- Sur les appareils exécutant macOS :

  - Les informations sont contenues dans des fichiers texte séparés, un pour chaque type de données, situés dans /Library/Application Support/Kaspersky Lab/klnagent/Data/1103/1.0.0.0/Statistics/AVState/.

Les valeurs spécifiques des clés, décrites dans le tableau ci-dessous, correspondent à chaque état de la protection antivirus.

Clés du registre et leurs valeurs possibles

Clé (type de données)	Valeur	Description
`Protection_LastConnected (REG_SZ)`	JJ-MM-AAAA HH-MM-SS	Date et heure (au format UTC) de la dernière connexion au Serveur d'administration.
`Protection_AdmServer (REG_SZ)`	IP, nom DNS ou nom NetBIOS	Nom du Serveur d'administration qui administre l'appareil
`Protection_NagentVersion (REG_SZ)`	a.b.c.d	Numéro de version de l'Agent d'administration installé sur l'appareil
`Protection_NagentFullVersion (REG_SZ)`	a.b.c.d (patch1; patch2; ...; patchN)	Numéro complet de la version d'Agent d'administration (avec correctifs) installée sur l'appareil
`Protection_HostId (REG_SZ)`	Identifiant de l'appareil	Identificateur de l'appareil

Clé (type de données)	Valeur	Description
`Protection_DynamicVM (REG_DWORD)`	0 — non 1 — oui	L'Agent d'administration est installé en mode VDI dynamique
`Protection_AvInstalled (REG_DWORD)`	0 — non 1 — oui	L'application de sécurité est installée sur l'appareil
`Protection_AvRunning (REG_DWORD)`	0 — non 1 — oui	Protection en temps réel de l'appareil active
`Protection_HasRtp (REG_DWORD)`	0 — non 1 — oui	Module de protection en temps réel installé
`Protection_RtpState (REG_DWORD)`	État de la protection en temps réel :	
	0	Inconnu
	1	Désactivé
	2	Suspendu(e)
	3	Lancement en cours
	4	Activé
	5	Activé avec le niveau de protection élevé (protection maximale)
	6	Activé avec un faible niveau de protection (vitesse maximale)
	7	Activé avec les paramètres par défaut (recommandés)
	8	Activé avec des paramètres personnalisés
	9	Défaillance dans le fonctionnement
`Protection_LastFscan (REG_SZ)`	JJ-MM-AAAA HH-MM-SS	Date et heure (au format UTC) de la dernière analyse complète
`Protection_BasesDate (REG_SZ)`	JJ-MM-AAAA HH-MM-SS	Date et heure (au format UTC) d'édition des bases de l'application

Consultation et configuration des actions quand les appareils sont inactifs

Si les appareils client au sein d'un groupe sont inactifs, vous pouvez recevoir des notifications à ce sujet. Vous pouvez également supprimer automatiquement ces appareils.

Pour voir ou configurer les actions lorsque les appareils du groupe sont inactifs :

1. Cliquez-droit sur le nom du groupe d'administration requis dans l'arborescence de la console.
2. Dans le menu contextuel, sélectionnez l'option **Propriétés**.

   Cette action ouvre la fenêtre des propriétés du groupe d'administration.
3. Dans la fenêtre **Propriétés**, accédez à la section **Appareils**.

4. Le cas échéant, activez ou désactivez les options suivantes :

- **Informer l'administrateur si l'appareil n'est pas actif pendant plus de (jours)**

  Quand cette option est activée, l'administrateur reçoit des notifications sur les appareils inactifs. Vous pouvez définir la période à l'issue de laquelle l'événement **L'appareil est resté inactif sur le réseau depuis longtemps** est créé. Par défaut, la valeur de cet intervalle est de 7 jours.

  Cette option est activée par défaut.

- **Supprimer l'appareil du groupe après une inactivité de plus de (jours)**

  Quand cette option est activée, vous pouvez définir la période à l'issue de laquelle un appareil est supprimé automatiquement du groupe. Par défaut, la valeur de cet intervalle est de 60 jours.

  Cette option est activée par défaut.

- **Hériter du groupe parent**

  Les paramètres de cette section sont hérités du groupe parent auquel appartient l'appareil client. Quand cette option est activée, les paramètres du groupe **Activité des appareils sur le réseau** sont verrouillés et ne peuvent être modifiés.

  Cette option est disponible uniquement si le groupe d'administration possède un groupe parent.

  Cette option est activée par défaut.

- **Forcer l'héritage des groupes enfants**

  Les valeurs des paramètres sont diffusées dans les groupes enfants mais ces paramètres sont verrouillés dans les propriétés des groupes enfants.

  Cette option est Inactif par défaut.

5. Cliquez sur le bouton **OK**.

Vos modifications sont enregistrées et appliquées.

Désactivation des annonces de Kaspersky

Dans Kaspersky Security Center Web Console, la section Annonces de Kaspersky (**Surveillance et rapports → Annonces de Kaspersky**) vous tient informé en fournissant des informations relatives à votre version de Kaspersky Security Center et aux applications administrées installées sur les appareils administrés. Si vous ne souhaitez pas recevoir les annonces de Kaspersky, vous pouvez désactiver cette fonctionnalité.

Les annonces de Kaspersky incluent deux types d'informations : les annonces relatives à la sécurité et les annonces marketing. Vous pouvez désactiver les annonces de chaque type séparément.

Pour désactiver les annonces relatives à la sécurité, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le Serveur d'administration pour lequel vous souhaitez désactiver les annonces relatives à la sécurité.

2. Cliquez-droit, puis sélectionnez **Propriétés** dans le menu contextuel qui s'affiche.

3. Dans la fenêtre des propriétés du Serveur d'administration qui s'ouvre, dans la section **Annonces de Kaspersky**, désactivez l'option **&Autoriser l'affichage d'annonces de Kaspersky dans Kaspersky Security Center Web Console**.

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

Les annonces de Kaspersky sont désactivées.

Les annonces marketing sont désactivées par défaut. Vous ne recevez des annonces marketing que si vous avez activé Kaspersky Security Network (KSN). Vous pouvez désactiver ce type d'annonces en désactivant KSN.

Réglage des points de distribution et des passerelles de connexion

La structure des groupes d'administration dans Kaspersky Security Center exerce les fonctions suivantes :

- Désignation de la zone d'action des stratégies.

  Il existe une autre méthode d'application des paramètres nécessaires sur les appareils : le recours aux *profils de stratégie*. Dans ce cas, vous définissez la zone d'action des stratégies avec des tags, les emplacements des appareils dans les unités organisationnelles Active Directory ou l'appartenance aux groupes de sécurité Active Directory.

- Désignation de la zone d'action des tâches de groupe.

  Il y existe une méthode de désignation de la zone d'action des tâches de groupe qui ne repose pas sur la hiérarchie des groupes d'administration : l'utilisation de tâche pour des sélections d'appareils et des ensembles d'appareils.

- Désignation des privilèges d'accès aux appareils et aux Serveurs d'administration secondaires et virtuels

- Ceci assigne les points de distribution.

Lors de la mise en place de la structure de groupes d'administration, il faut prendre en considération la topologie du réseau de l'entreprise pour garantir la désignation optimale des points de distribution. La distribution optimale des points de distribution permet de diminuer le trafic réseau à l'intérieur du réseau de l'entreprise.

En fonction de la structure organisationnelle de l'entreprise et de la topologie des réseaux, les configurations typiques suivantes de structure des groupes d'administration existent :

- Un bureau

- plusieurs petits bureaux isolés

Les appareils fonctionnant comme points de distribution doivent être protégés, y compris physiquement contre tout accès non autorisé.

Configuration typique des points de distribution : un bureau simple

Dans la configuration typique " un bureau ", tous les appareils se trouvent sur le réseau de l'entreprise et se " voient ". Le réseau de l'entreprise peut comprendre plusieurs " parties " mises en évidence (des réseaux ou des segments de réseau) et reliées par des canaux étroits.

Les moyens suivants de construction de la structure de groupes d'administration existent :

- Construction de la structure des groupes d'administration en tenant compte de la topologie du réseau. La structure des groupes d'administration ne doit pas obligatoirement refléter exactement la topologie du réseau. Il suffit que quelques groupes d'administration correspondent à des parties du réseau mises en évidence. Les points de distribution peuvent être désignés automatiquement ou manuellement.

- Construction de la structure des groupes d'administration qui ne reflète pas la topologie du réseau. Dans ce cas, vous devez désactiver la désignation automatique des points de distribution et désigner dans chaque partie du réseau mise en évidence un ou plusieurs appareils en tant que points de distribution sur le groupe d'administration racine, par exemple, sur le groupe **Appareils administrés**. Tous les points de distribution se trouvent au même niveau et possèdent la même zone d'action, à savoir tous les appareils du réseau de l'entreprise. Chaque Agent d'administration se connecte dans ce cas au point de distribution qui possède l'itinéraire le plus court. L'utilitaire tracert permet de définir l'itinéraire d'accès au point de distribution.

Configuration typique des points de distribution : plusieurs petits bureaux isolés

Cette configuration typique correspond à plusieurs petits bureaux distants, potentiellement connectés au siège principal via Internet. Chacun de ces bureaux distants se trouve au-delà du NAT. Autrement dit, la connexion d'un bureau distant à un autre est impossible. Ils sont isolés.

La configuration doit absolument se refléter dans la structure des groupes d'administration : pour chacun des bureaux distants. il faut créer un groupe d'administration distinct (les groupes **Bureau 1**, **Bureau 2** sur l'illustration ci-après).

Bureaux distants affichés dans la structure des groupes d'administration

Sur chaque groupe d'administration correspondant à un bureau, il faut désigner un ou plusieurs points de distribution. Les points de distribution doivent être des appareils du bureau distant dotés d'espace suffisant sur le disque. Ainsi, les appareils qui se trouvent par exemple dans le groupe **Bureau 1** vont contacter les points de distribution assignés au groupe d'administration **Bureau 1**.

Si certains utilisateurs se déplacent d'un bureau à l'autre avec des ordinateurs portables, il faut sélectionner dans chaque bureau distant, en plus des points de distribution cités ci-dessus, deux ou plusieurs appareils et les assigner comme points de distribution pour le groupe d'administration de niveau supérieur (le groupe **Groupe racine pour les bureaux** dans l'illustration ci-dessus).

Exemple : Par exemple, voici un ordinateur portable qui se trouve dans le groupe d'administration **Bureau 1**, mais qui est déplacé physiquement dans le bureau qui correspond au groupe **Bureau 2**. Après le déplacement, l'Agent d'administration sur l'ordinateur portable tente de contacter les points de distribution assignés au groupe **Bureau 1**, mais ceux-ci ne sont pas accessibles. Alors l'Agent d'administration commence à contacter les points de distribution désignés pour le groupe **Groupe racine pour les bureaux**. Étant donné que les bureaux distants sont isolés les uns des autres, seules les requêtes d'accès aux points de distribution assignés au groupe d'administration **Groupe racine pour les bureaux** aboutissent lorsque l'Agent d'administration tente d'accéder aux points de distribution dans le groupe **Bureau 2**. Autrement dit, l'ordinateur portable demeure dans le groupe d'administration qui correspond à son bureau d'origine, mais il utilise malgré tout le point de distribution du bureau où il se trouve physiquement à l'heure actuelle.

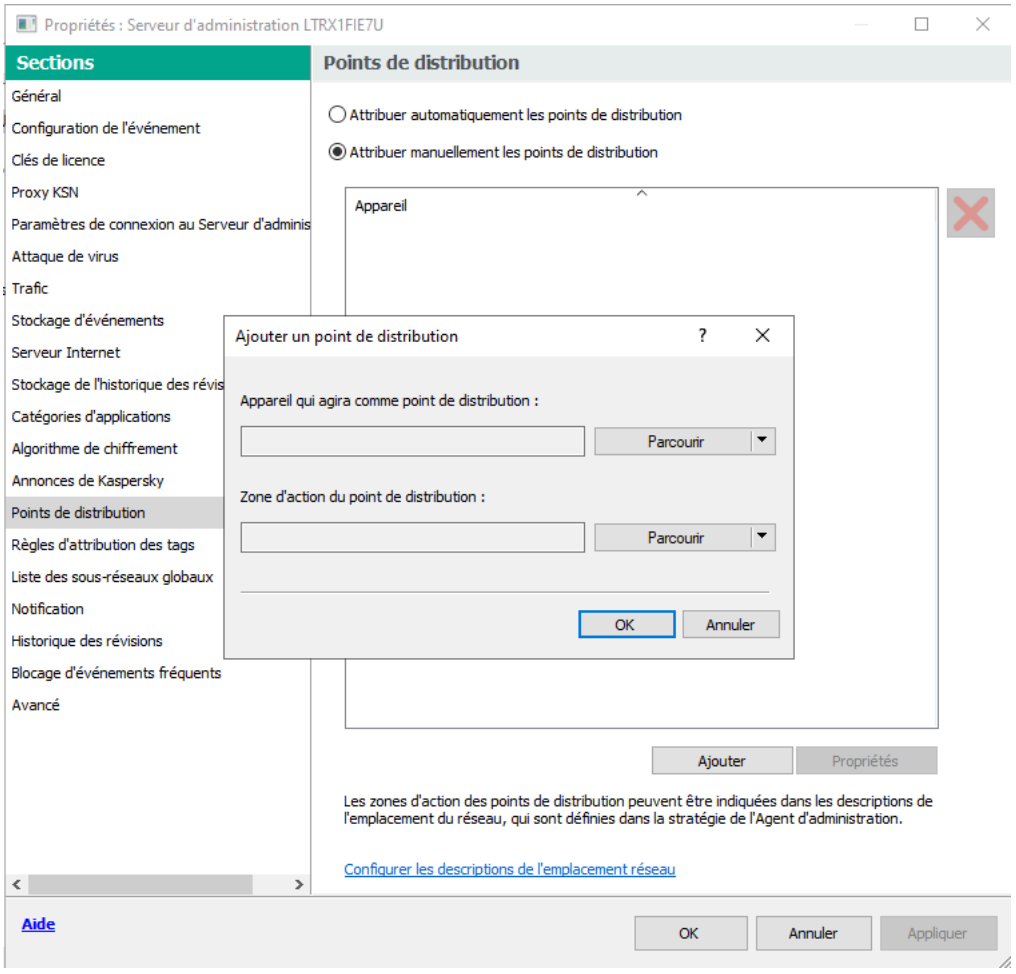
Désignation d'un appareil administré pour servir de point de distribution

Vous pouvez désigner manuellement un point de distribution pour un groupe d'administration et le configurer comme passerelle des connexions dans la Console d'administration.

Pour désigner un appareil en tant que point de distribution du groupe d'administration, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez l'entrée **Serveur d'administration**.
2. Dans le menu contextuel du Serveur d'administration, sélectionnez l'option **Propriétés**.
3. Ouvrir à nouveau la fenêtre des propriétés du Serveur d'administration, sélectionnez la section **Points de distribution**.
4. Dans la partie droite de la fenêtre, sélectionnez l'option **Assigner manuellement les points de distribution**.

5. Cliquez sur le bouton **Ajouter**.



Attribuer un point de distribution manuellement

Cette opération permet d'ouvrir la fenêtre **Ajouter un point de distribution**.

6. Dans la fenêtre **Ajouter un point de distribution**, exécutez les opérations suivantes :

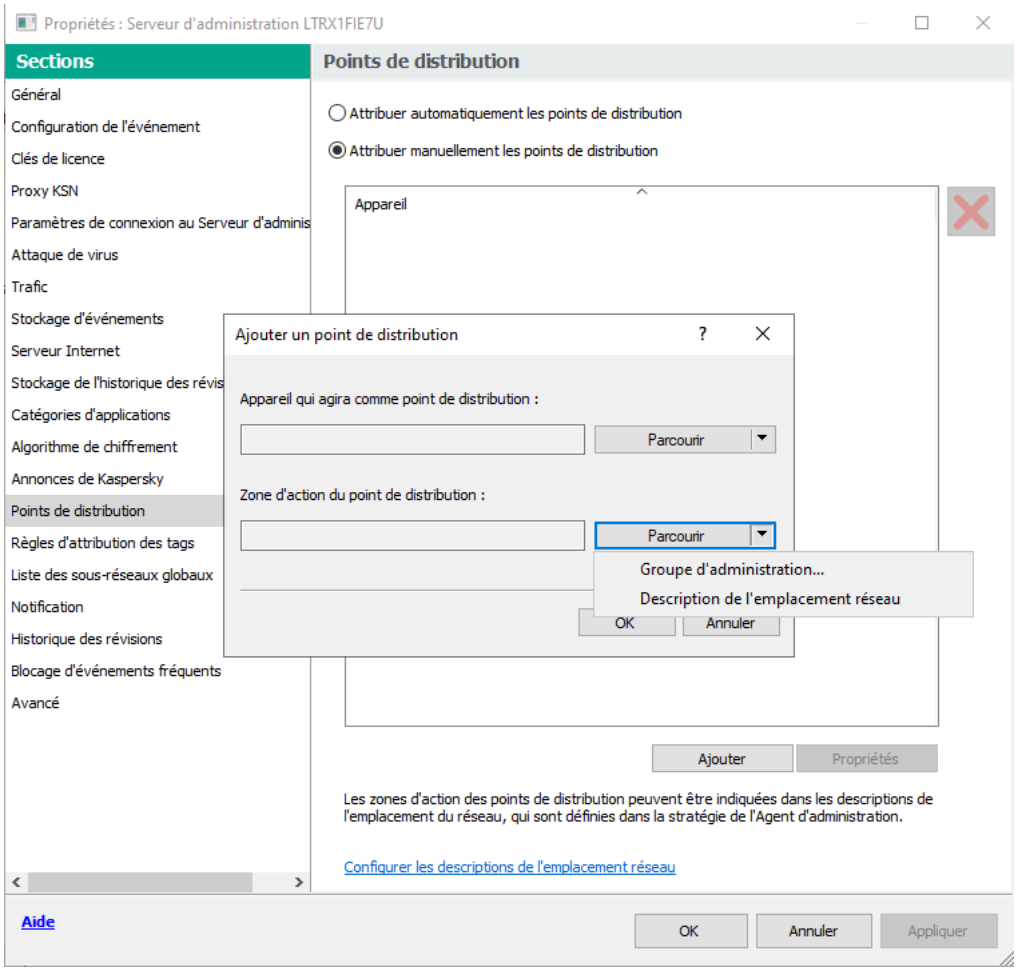
   a. Sous **Appareil qui agira comme point de distribution**, cliquez sur la flèche vers le bas (▾) sur le bouton **Sélectionner**, puis sélectionnez l'option **Ajouter l'appareil du &groupe**.

   b. Dans la fenêtre **Sélectionner les appareils** qui s'ouvre, sélectionnez l'appareil qui agira comme point de distribution.

   c. Sous **Zone d'action du point de distribution**, cliquez sur la flèche vers le bas (▾) sur le bouton **Sélectionner**.

   d. Indiquez un ensemble d'appareils sur lesquels le point de distribution diffusera les mises à jour. Vous pouvez indiquer le groupe d'administration ou la description de l'emplacement réseau.

e. Cliquez sur le bouton **OK** pour fermer la fenêtre **Ajouter un point de distribution**.



Sélection de la portée du point de distribution

Le point de distribution que vous avez ajouté sera affiché dans la liste des points de distribution, dans la section **Points de distribution**.

Le premier appareil doté d'un Agent d'administration qui se connectera au Serveur d'administration virtuel sera automatiquement désigné comme point de distribution et configuré comme passerelle des connexions.

Connexion d'un appareil Linux en tant que passerelle dans la zone démilitarisée

Pour connecter un appareil Linux en tant que passerelle dans la zone démilitarisée (DMZ) :

1. Téléchargez et installez l'Agent d'administration sur l'appareil Linux.

2. Exécutez l'Assistant de post-installation et suivez la procédure afin de configurer la configuration de l'environnement local. Dans l'invite de commande, exécutez la commande suivante :
   ```
   $ sudo /opt/kaspersky/klnagent64/lib/bin/setup/postinstall.pl
   ```

3. À l'étape demandant le mode d'Agent d'administration, choisissez l'option **Utiliser comme passerelle de connexion**.

4. Dans la Console d'administration basée sur MMC, dans le menu contextuel du Serveur d'administration, choisissez l'option **Propriétés**.

5. Dans la fenêtre des propriétés du Serveur d'administration qui s'ouvre, sélectionnez la section **Points de distribution**.

6. Dans la fenêtre **Points de distribution** qui s'ouvre, dans la partie droite de la fenêtre :

   a. Sélectionnez l'option **Assigner manuellement les points de distribution**.

   b. Cliquez sur le bouton **Ajouter**.

   Cette opération permet d'ouvrir la fenêtre **Ajouter un point de distribution**.

7. Dans la fenêtre **Ajouter un point de distribution**, exécutez les opérations suivantes :

   a. Sous **Appareil qui agira comme point de distribution**, cliquez sur la flèche orientée vers le bas (▾) sur le bouton **Sélectionner**, puis sélectionner l'option **Ajouter la passerelle de connexion, située en DMZ, en fonction de l'adresse**.

   b. Sous **Zone d'action du point de distribution**, cliquez sur la flèche vers le bas (▾) sur le bouton **Sélectionner**.

   c. Indiquez un ensemble d'appareils sur lesquels le point de distribution diffusera les mises à jour. Vous pouvez spécifier un groupe d'administration.

   d. Cliquez sur le bouton **OK** pour fermer la fenêtre **Ajouter un point de distribution**.

8. Le point de distribution que vous avez ajouté sera affiché dans la liste des points de distribution, dans la section **Points de distribution**.

9. Exécutez l'utilitaire klnagchk pour vérifier si une connexion à Kaspersky Security Center a été correctement configurée. Dans la ligne de commande, exécutez la commande suivante :
   ```
   $ sudo /opt/kaspersky/klnagent64/bin/klnagchk
   ```

10. Dans le menu principal, accédez à Kaspersky Security Center et découvrez l'appareil.

11. Dans la fenêtre qui s'ouvre, cliquez sur l'appareil <Device name>.

12. Dans la liste déroulante, sélectionnez le lien **Déplacer vers le groupe**.

13. Dans la fenêtre **Sélectionner un groupe** qui s'ouvre, cliquez sur le lien **Points de distribution**.

14. Cliquez sur le bouton **OK**.

15. Redémarrez le service Agent d'administration sur le client Linux en exécutant la commande suivante dans la ligne de commande :
   ```
   $ sudo /opt/kaspersky/klnagent64/bin/klnagchk -restart
   ```

La connexion d'un appareil Linux en tant que passerelle dans la DMZ est terminée.

Après cela, vous pouvez connecter un appareil Linux au Serveur d'administration via la passerelle de connexion configurée. N'exécutez ces procédures qu'après avoir terminé le scénario d'installation principal.

Connexion d'un appareil sous Linux au Serveur d'administration via une passerelle de connexion

Une passerelle de connexion permet de connecter des appareils clients de la zone démilitarisée (DMZ) au Serveur d'administration. Les appareils basés sur Windows et Linux peuvent agir comme une passerelle de connexion. Une fois connecté et configuré la passerelle de connexion, vous pouvez utiliser cette passerelle pour connecter un appareil Linux au Serveur d'administration. Suivez la procédure ci-dessous uniquement après avoir terminé le scénario d'installation principal.

Pour connecter un appareil sous Linux au Serveur d'administration par une passerelle de connexion, effectuez les actions suivantes sur cet appareil :

1. Téléchargez et installez l'Agent d'administration sur l'appareil Linux.

2. Exécutez le script de post-installation de l'Agent d'administration en exécutant la commande suivante dans la ligne de commande :
   ```
   $ sudo /opt/kaspersky/klnagent64/lib/bin/setup/postinstall.pl
   ```

3. À l'étape demandant le mode d'Agent d'administration, choisissez l'option **Se connecter au Serveur via la passerelle de connexion** et entrez l'adresse de la passerelle de connexion.

4. Vérifiez la connexion avec Kaspersky Security Center et la passerelle de connexion en utilisant la commande suivante dans la ligne de commande :
   ```
   $ sudo /opt/kaspersky/klnagent64/bin/klnagchk
   ```
   L'adresse de la passerelle de connexion s'affiche dans la sortie.

La connexion d'un appareil sous Linux au Serveur d'administration via une passerelle de connexion est terminée. Vous pouvez utiliser cet appareil pour mettre à jour la distribution, pour installer à distance des applications et pour récupérer des informations sur les appareils en réseau.

Ajout d'une passerelle de connexion dans la DMZ en tant que point de distribution

Une passerelle de connexion attend les connexions du Serveur d'administration au lieu d'établir des connexions avec le Serveur d'administration. Cela signifie que juste après l'installation d'une passerelle de connexion sur un appareil dans la DMZ, le Serveur d'administration n'énumère pas l'appareil parmi les appareils administrés. Par conséquent, vous avez besoin d'une procédure spéciale pour vous assurer que le Serveur d'administration amorce une connexion à la passerelle de connexion.

Pour ajouter un appareil avec une passerelle de connexion comme point de distribution :

1. Dans l'arborescence de la console, sélectionnez l'entrée **Serveur d'administration**.

2. Dans le menu contextuel du Serveur d'administration, sélectionnez l'option **Propriétés**.

3. Ouvrir à nouveau la fenêtre des propriétés du Serveur d'administration, sélectionnez la section **Points de distribution**.

4. Dans la partie droite de la fenêtre, sélectionnez l'option **Assigner manuellement les points de distribution**.

5. Cliquez sur le bouton **Ajouter**.

   Cette opération permet d'ouvrir la fenêtre **Ajouter un point de distribution**.

6. Dans la fenêtre **Ajouter un point de distribution**, exécutez les opérations suivantes :

   a. Sous **Appareil qui agira comme point de distribution**, cliquez sur la flèche orientée vers le bas (▾) sur le bouton **Sélectionner**, puis sélectionner l'option **Ajouter la passerelle &de connexion, située en DMZ, en fonction de l'adresse**.

   b. Dans la fenêtre **Saisie de l'adresse de la passerelle de connexion** qui ouvre, entrez l'adresse IP de la passerelle de connexion (ou entrez le nom si la passerelle de connexion est accessible par son nom).

   c. Sous **Zone d'action du point de distribution**, cliquez sur la flèche vers le bas (▾) sur le bouton **Sélectionner**.

   d. Indiquez un ensemble d'appareils sur lesquels le point de distribution diffusera les mises à jour. Vous pouvez indiquer le groupe d'administration ou la description de l'emplacement réseau.

      Nous vous recommandons de créer un groupe distinct pour les appareils administrés externes.

Une fois que vous avez effectué ces actions, la liste des points de distribution contient une nouvelle entrée intitulée **L'enregistrement temporaire pour la passerelle de connexion**.

Le Serveur d'administration tente presque immédiatement de se connecter à la passerelle de connexion à l'adresse que vous avez indiquée. Si l'opération réussit, le nom de l'entrée devient le nom de l'appareil de la passerelle de connexion. Ce processus prend jusqu'à cinq minutes.

Pendant que l'entrée temporaire pour la passerelle de connexion est convertie en une entrée nommée, la passerelle de connexion s'affiche également dans le groupe **Appareils non définis**.

Pour ajouter une passerelle de connexion à un réseau précédemment configuré, réinstallez l'Agent d'administration sur les appareils que vous souhaitez connecter à la passerelle de connexion récemment ajoutée.

Assignation automatique des points de distribution

Nous vous recommandons d'assigner les points de distribution automatiquement. Kaspersky Security Center choisira ainsi par lui-même les appareils à désigner comme points de distribution.

Pour assigner automatiquement des points de distribution :

1. Ouvrez la fenêtre principale de l'application.

2. Dans l'arborescence de la console, choisissez le nœud reprenant le nom du Serveur d'administration auquel vous souhaitez assigner automatiquement des points de distribution.

3. Dans le menu contextuel Serveur d'administration, cliquez sur **Propriétés**.

4. Dans la fenêtre des propriétés du Serveur d'administration, dans le volet **Sections**, sélectionnez **Points de distribution**.

5. Dans la partie droite de la fenêtre, sélectionnez l'option **Attribuer automatiquement les points de distribution**.

   Si l'assignation automatique d'appareils comme points de distribution est activée, vous ne pouvez pas configurer les points de distribution manuellement ni modifier la liste des points de distribution.

6. Cliquez sur le bouton **OK**.

Le Serveur d'administration assigne et configure automatiquement les points de distribution.

À propos de l'installation locale de l'Agent d'administration sur l'appareil choisi comme point de distribution

Pour que l'appareil choisi comme point de distribution puisse directement contacter le Serveur d'administration virtuel pour remplir le rôle de passerelle des connexions, il faut installer localement l'Agent d'administration sur cet appareil.

L'ordre de l'installation locale de l'Agent d'administration sur l'appareil choisi comme point de distribution correspond à l'ordre d'installation locale de l'Agent d'administration sur n'importe quel appareil du réseau.

L'appareil choisi comme point de distribution doit remplir les conditions suivantes :

- Lors de l'installation locale de l'Agent d'administration, il faut indiquer l'adresse du Serveur d'administration virtuel qui gère l'appareil dans le champ **Adresse du serveur** de la fenêtre **Serveur d'administration** de l'Assistant d'installation. Pour l'adresse de l'appareil, vous pouvez utiliser l'adresse IP ou le nom de l'appareil sur le réseau Windows.

  Le format suivant est utilisé pour indiquer l'adresse du Serveur d'administration virtuel : <Full address of the physical Administration Server to which the virtual Server is subordinate>/<Name of virtual Administration Server>.

- Pour qu'il puisse remplir le rôle de passerelle de connexions, il faut ouvrir tous les ports indispensables aux communications avec le Serveur d'administration.

Suite à l'installation sur l'appareil de l'Agent d'administration selon les paramètres indiqués, l'application Kaspersky Security Center exécute automatiquement les actions suivantes :

- Ajout de cet appareil au groupe **Appareils administrés** du Serveur d'administration virtuel.

- Désignation de cet appareil comme point de distribution du groupe **Appareils administrés** du Serveur d'administration virtuel.

Il suffit d'installer l'Agent d'administration localement, sur l'appareil désigné comme point de distribution pour le groupe **Appareils administrés** sur le réseau de l'entreprise. Vous pouvez installer à distance l'Agent d'administration sur les appareils qui remplissent la fonction de points de distribution dans les sous-groupes d'administration Pour ce faire, utilisez le point de distribution du groupe **Appareils administrés** en tant que passerelle de connexion.

À propos de l'utilisation d'un point de distribution comme passerelle de connexion

Si le Serveur d'administration se trouve en dehors de la zone démilitarisée (DMZ), les Agents d'administration qui sont dans cette zone perdent la possibilité de se connecter avec le Serveur.

Pour établir une connexion entre le Serveur d'administration et les Agents d'administration, il est possible d'utiliser comme passerelle de connexion un point de distribution. Le point de distribution offre au Serveur d'administration un port pour établir une connexion. Au lancement, le Serveur d'administration se connecte au point de distribution et n'interrompe pas la connexion avec ce dernier tout au long de son fonctionnement.

Une fois qu'il a reçu le signal du Serveur d'administration, le point de distribution envoie un signal UDP aux Agents d'administration pour la connexion au Serveur d'administration. Une fois que les Agents d'administration ont reçu le signal, ils se connectent au point de distribution qui transmet les informations entre les Agents d'administration et le Serveur d'administration. L'échange d'informations peut avoir lieu sur un réseau IPv4 ou IPv6.

Il est recommandé d'utiliser comme passerelle de connexion l'appareil sélectionné et d'attribuer à cette passerelle de connexion pas plus de 10 000 appareils clients (y compris les appareils mobiles).

Pour ajouter une passerelle de connexion à un réseau précédemment configuré, procédez comme suit :

1. Installer l'Agent d'administration en mode passerelle de connexion.
2. Réinstallez l'Agent d'administration sur les appareils que vous souhaitez connecter à la passerelle de connexion récemment ajoutée.

Ajout de plages IP à la liste des plages sondées par un point de distribution

Vous pouvez ajouter des plages IP à la liste des plages sondées d'un point de distribution.

Pour ajouter une plage IP à la liste des plages sondées :

1. Dans l'arborescence de la console, sélectionnez l'entrée **Serveur d'administration**.
2. Dans le menu contextuel de l'entrée, sélectionnez l'option **Propriétés**.
3. Dans la fenêtre des propriétés du Serveur d'administration qui s'ouvre, sélectionnez la section **Points de distribution**.
4. Dans la liste, sélectionnez le point de distribution requis, puis cliquez sur **Propriétés**.
5. Dans la fenêtre des propriétés du point de distribution qui s'ouvre, dans le volet de gauche **Sections**, sélectionnez **Recherche d'appareils** → **Plages IP**.
6. Cochez la case **Autoriser le sondage des plages**.

7. Cliquez sur le bouton **Ajouter**.

   Le bouton **Ajouter** est activé uniquement si vous cochez la case **Autoriser le sondage des plages**.

   La fenêtre **Plage IP** s'ouvre.

8. Dans la fenêtre **Plage IP**, saisissez le nom de la nouvelle plage IP (le nom par défaut est Nouvelle plage).

9. Cliquez sur le bouton **Ajouter**.

10. Exécutez une des actions suivantes :

    - Définissez la plage IP en utilisant des adresses IP de début et de fin.
    - Définissez la plage IP en utilisant l'adresse et le masque de sous-réseau.
    - Cliquez sur **Parcourir** et ajoutez un sous-réseau tiré de la liste globale des sous-réseaux.

11. Cliquez sur le bouton **OK**.

12. Cliquez sur **OK** pour ajouter la nouvelle plage avec le nom indiqué.

    La nouvelle plage apparaît dans la liste des plages sondées.

Utilisation d'un point de distribution en tant que serveur push

Dans Kaspersky Security Center, un point de distribution peut servir de serveur push pour les appareils administrés via le protocole mobile et pour les appareils administrés par l'Agent d'administration. Par exemple, un serveur push doit être activé si vous souhaitez pouvoir forcer la synchronisation des appareils KasperskyOS avec le Serveur d'administration. Un serveur push a la même portée d'appareils administrés que le point de distribution sur lequel le serveur push est activé. Si plusieurs points de distribution sont affectés au même groupe d'administration, vous pouvez activer le serveur push sur chacun des points de distribution. Dans ce cas, le Serveur d'administration équilibre la charge entre les points de distribution.

> Un serveur push prend en charge jusqu'à 50 000 connexions simultanées.

Vous souhaiterez peut-être utiliser des points de distribution comme serveurs push pour vous assurer qu'il existe une connexion permanente entre un appareil administré et le Serveur d'administration. Une connexion permanente est nécessaire pour certaines opérations, telles que l'exécution et l'arrêt des tâches locales, la réception de statistiques pour une application administrée ou la création d'un tunnel. Si vous utilisez un point de distribution comme serveur push, vous n'avez pas besoin d'utiliser l'option **Maintenir la connexion au Serveur d'administration** option sur les appareils administrés ou envoyer des paquets au port UDP de l'Agent d'administration.

Pour utiliser un point de distribution en tant que serveur push :

1. Dans l'arborescence de la console, sélectionnez l'entrée **Serveur d'administration**.

2. Dans le menu contextuel de l'entrée, sélectionnez l'option **Propriétés**.

3. Dans la fenêtre des propriétés du Serveur d'administration qui s'ouvre, sélectionnez la section **Points de distribution**.

4. Dans la liste, sélectionnez le point de distribution requis, puis cliquez sur **Propriétés**.

5. Dans la fenêtre des propriétés du point de distribution qui s'ouvre, dans la section **Général** du côté gauche du volet **Sections**, sélectionnez l'option **Utilisez ce point de distribution comme serveur push**.

6. Spécifiez le numéro de port du serveur push, c'est-à-dire le port sur le point de distribution que les appareils clients utiliseront pour la connexion.

   Le numéro du port est de 13295 par défaut.

7. Cliquez sur **OK** pour fermer la fenêtre de propriétés du point de distribution.

8. Ouvrez la fenêtre des propriétés de stratégie de l'Agent d'administration.

9. Dans la section **Connectivité**, accédez à la sous-section **Réseau**.

10. Dans la sous-section **Réseau**, sélectionnez l'option **Utiliser le point de distribution pour forcer la connexion au Serveur d'administration**.

11. Cliquez sur le bouton **OK** pour quitter la fenêtre.

Le point de distribution commence à agir comme un serveur push. Il peut désormais envoyer des notifications push aux appareils client.

Si vous administrez des appareils avec un KasperskyOS installé, ou si vous prévoyez de le faire, vous devez utiliser un point de distribution comme serveur push. Vous pouvez également utiliser un point de distribution en tant que serveur push si vous souhaitez envoyer des notifications push aux appareils clients.

Autres travaux de routine

Cette section contient des recommandations sur l'utilisation quotidienne de Kaspersky Security Center.

Administration des Serveurs d'administration

Cette section contient les informations sur l'utilisation des Serveurs d'administration et sur la configuration des paramètres du Serveur d'administration.

Création d'une hiérarchie des Serveurs d'administration : ajout d'un Serveur d'administration secondaire

Vous pouvez ajouter un Serveur d'administration en tant que Serveur d'administration secondaire et définir en même temps une relation hiérarchique de type "serveur principal/serveur secondaire". L'ajout est possible, que le Serveur d'administration que vous souhaitez rendre secondaire, pour la connexion à la Console d'administration, soit accessible ou non.

En cas de regroupement de Serveurs dans une hiérarchie, le port 13291 des deux Serveurs doit être accessible. Le port 13291 est nécessaire à la réception des connexions de la Console d'administration au Serveur d'administration.

Connexion du Serveur d'administration en guise de serveur secondaire du Serveur d'administration principal

Vous pouvez ajouter un Serveur d'administration en guise de Serveur secondaire avec connexion au Serveur d'administration principal via le port 13000. Vous aurez besoin d'un appareil avec la Console d'administration installée et permettant d'accéder aux ports TCP 13291 sur les deux Serveurs d'administration : futur Serveur d'administration principal et futur Serveur d'administration secondaire.

Pour ajouter un Serveur d'administration disponible pour la connexion via la Console d'administration, à titre de Serveur secondaire, procédez comme suit :

1. Assurez-vous que le port 13000 du Serveur d'administration principal supposé peut recevoir les connexions des Serveurs d'administration secondaires.

2. Connectez-vous au Serveur d'administration principal via la Console d'administration.

3. Choisissez le groupe d'administration auquel vous envisagez d'ajouter le Serveur d'administration secondaire.

4. Dans l'espace de travail du nœud **Serveurs d'administration** du groupe sélectionné, cliquez sur le lien **Ajouter un Serveur d'administration secondaire**.

   L'Assistant d'ajout de Serveur d'administration secondaire démarre.

5. À la première étape de l'assistant (saisie de l'adresse du Serveur d'administration ajouté au groupe), saisissez le nom de réseau du futur Serveur d'administration secondaire.

6. Suivez les instructions de l'assistant.

La hiérarchie "principal/secondaire" est établie. Le Serveur d'administration principal recevra la connexion du Serveur d'administration secondaire.

Si vous n'avez pas d'appareil avec la Console d'administration installée donnant accès aux ports TCP 13291 des deux Serveurs d'administration (par exemple, si le futur Serveur d'administration secondaire se trouve dans un bureau distant et l'administrateur système du bureau distant ne rend pas le port 13291 accessible sur Internet pour des raisons de sécurité), vous pouvez tout de même ajouter un Serveur d'administration secondaire.

Pour ajouter un Serveur d'administration indisponible pour la connexion via la Console d'administration, à titre de Serveur d'administration secondaire, procédez comme suit :

1. Confirmez que le port 13000 du futur Serveur d'administration principal est disponible pour la connexion depuis les Serveurs d'administration secondaires.

2. Enregistrez le fichier du certificat du futur Serveur d'administration principal sur un appareil externe (par exemple, une clé USB) ou envoyez-le à l'administrateur système du bureau distant où se trouve le Serveur d'administration.

   Le fichier du certificat du Serveur d'administration se trouve sur le Serveur d'administration à l'adresse %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert\klserver.cer.

3. Enregistrez le fichier du certificat du futur Serveur d'administration secondaire sur un appareil externe (par exemple, une clé USB). Si le futur Serveur d'administration secondaire se trouve dans un bureau distant, demandez à l'administrateur système du bureau distant de vous renvoyer le certificat.

   Le fichier du certificat du Serveur d'administration se trouve sur le Serveur d'administration à l'adresse %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert\klserver.cer.

4. Connectez-vous au Serveur d'administration principal via la Console d'administration.

5. Choisissez le groupe d'administration auquel vous envisagez d'ajouter le Serveur d'administration secondaire.

6. Dans l'espace de travail du nœud **Serveurs d'administration**, cliquez sur le lien **Ajouter un Serveur d'administration secondaire**.

   L'Assistant d'ajout de Serveur d'administration secondaire démarre.

7. À la première étape de l'Assistant (saisie de l'adresse), laissez le champ **Adresse du Serveur d'administration secondaire (facultative)** vide.

8. Dans la fenêtre **Fichier du certificat du Serveur d'administration secondaire**, cliquez sur le bouton **Parcourir** et sélectionnez le fichier de certificat du Serveur d'administration secondaire que vous avez enregistré.

9. Après l'exécution de l'Assistant, connectez-vous à l'aide d'une autre instance de Console d'administration au futur Serveur d'administration secondaire. Si ce Serveur d'administration se trouve dans un bureau distant, demandez à l'administrateur système du bureau distant de se connecter au futur Serveur d'administration secondaire et d'exécuter les étapes ultérieures sur ce dernier.

10. Dans le menu contextuel de l'entrée **Serveur d'administration**, choisissez l'option **Propriétés**.

11. Dans les propriétés du Serveur d'administration, passez à la section **Avancé**, puis à la sous-section **Hiérarchie des Serveurs d'administration**.

12. Cochez la case **Ce Serveur d'administration est secondaire dans la h&iérarchie**.

    Les champs de saisie peuvent alors être remplis et modifiés.

13. Dans le champ **Adresse du Serveur d'administration principal**, saisissez le nom de réseau du futur Serveur d'administration principal.

14. Choisissez le fichier enregistré précédemment contenant le certificat du futur Serveur d'administration principal en appuyant sur le bouton **Parcourir**.

15. Cliquez sur le bouton **OK**.

La hiérarchie "principal/secondaire" est établie. Vous pouvez vous connecter au Serveur d'administration secondaire via la Console d'administration. Le Serveur d'administration principal recevra la connexion du Serveur d'administration secondaire.

Connexion du Serveur d'administration principal à un Serveur d'administration secondaire

Vous pouvez ajouter un nouveau Serveur d'administration à titre de Serveur secondaire de telle sorte que le Serveur d'administration principal se connecte au Serveur d'administration secondaire via le port 13000. Cela s'impose, par exemple, si vous placez le Serveur d'administration secondaire dans une zone démilitarisée.

Vous aurez besoin d'un appareil avec la Console d'administration installée et permettant d'accéder aux ports TCP 13291 sur les deux Serveurs d'administration : futur Serveur d'administration principal et futur Serveur d'administration secondaire.

Pour ajouter un nouveau Serveur d'administration à titre de Serveur secondaire, puis connecter le Serveur d'administration principal à celui-ci via le port 13000, procédez comme suit :

1. Assurez-vous que le port 13000 du Serveur d'administration secondaire supposé peut recevoir les connexions du Serveur d'administration principal.

2. Connectez-vous au Serveur d'administration principal via la Console d'administration.

3. Choisissez le groupe d'administration auquel vous envisagez d'ajouter le Serveur d'administration secondaire.

4. Dans l'espace de travail du nœud **Serveurs d'administration** du groupe d'administration concerné, cliquez sur le lien **Ajouter un Serveur d'administration secondaire**.

   L'Assistant d'ajout de Serveur d'administration secondaire démarre.

5. À la première étape de l'assistant (saisie de l'adresse du Serveur d'administration à ajouter au groupe), saisissez le nom de réseau du futur Serveur d'administration secondaire et cochez la case **Connecter le Serveur d'administration principal au Serveur d'administration secondaire dans la DMZ**.

6. Si vous êtes connecté au futur Serveur d'administration secondaire via un serveur proxy, cochez la case **Utiliser un serveur proxy** à la première étape de l'Assistant et saisissez les paramètres de connexion.

7. Suivez les instructions de l'assistant.

La hiérarchie des Serveurs d'administration est établie. Le Serveur d'administration secondaire acceptera la connexion du Serveur d'administration principal.

Connexion au Serveur d'administration et permutation entre les Serveurs d'administration

Lors du lancement, l'application Kaspersky Security Center tente de se connecter au Serveur d'administration. S'il existe plusieurs Serveurs d'administration sur votre réseau, l'application se connectera au Serveur utilisé lors d'une session précédente de Kaspersky Security Center.

> Lors du premier démarrage de l'application après l'installation, une tentative de connexion au Serveur d'administration, indiqué lors de l'installation de Kaspersky Security Center, s'exécute.

Après la connexion au Serveur d'administration, la structure des dossiers de ce Serveur s'affiche dans l'arborescence de la console.

Si plusieurs Serveurs d'administration ont été ajoutés dans l'arborescence de la console, vous pouvez se déplacer entre eux.

La Console d'administration est nécessaire au fonctionnement avec chaque Serveur d'administration. Avant la première connexion à un nouveau Serveur d'administration, assurez-vous que le port 13291 par lequel les connexions de la Console d'administration sont acceptées, et tous les autres ports restants pour la connexion du Serveur d'administration avec d'autres modules de Kaspersky Security Center sont ouverts.

Pour se connecter à un autre Serveur d'administration, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez l'entrée portant le nom du Serveur d'administration requis.

2. Dans le menu contextuel du nœud, sélectionnez l'option **&Se connecter au Serveur d'administration**.

3. Dans la fenêtre **Paramètres de connexion** qui s'ouvre, dans le champ **Adresse du Serveur d'administration**, indiquez le nom du Serveur d'administration auquel vous voulez vous connecter. En tant que le nom du Serveur d'administration, vous pouvez indiquer l'adresse IP ou le nom de l'appareil dans le réseau Windows. En cliquant sur le bouton **Avancé** dans la partie inférieure de la fenêtre, vous pouvez configurer les paramètres de connexion au Serveur d'administration (cf. ill. ci-après).

   Pour vous connecter au Serveur d'administration via un port autre que le port par défaut, saisissez une valeur dans le champ **Adresse du Serveur d'administration** en utilisant le format <Administration Server name> : <Port>.

   Pour vous connecter à un Serveur d'administration virtuel, saisissez une valeur dans le champ **Adresse du Serveur d'administration** au format <adresse du Serveur d'administration>/<nom du serveur virtuel>.

   > Les utilisateurs qui ne jouissent pas des privilèges de **Lecture** ne pourront pas accéder au Serveur d'administration.

Processus de connexion au Serveur d'administration

4. Cliquez sur le bouton **OK** pour terminer la permutation entre les Serveurs.

   Après la connexion au Serveur d'administration, la structure des dossiers de l'entrée correspondante est actualisée dans l'arborescence de la console.

Privilèges d'accès au Serveur d'administration et à ses objets

Lors de l'installation de Kaspersky Security Center, les groupes d'utilisateurs **KLAdmins** et **KLOperators** sont automatiquement formés Ces groupes possèdent des privilèges de connexion au Serveur d'administration et de fonctionnement avec ses objets.

Selon le compte utilisateur sous lequel l'installation de Kaspersky Security Center se passe, les groupes **KLAdmins** et **KLOperators** sont créés de la manière suivante :

- Si l'installation se passe sous le compte utilisateur, appartenant au domaine, alors les groupes sont créés dans le domaine, incluant le Serveur d'administration, et sur le Serveur d'administration.
- Si l'installation se passe sous le compte utilisateur du système, les groupes sont créés uniquement sur le Serveur d'administration.

La consultation des groupes **KLAdmins** et **KLOperators** et l'insertion des modifications nécessaires dans les privilèges d'utilisateurs des groupes **KLAdmins** et **KLOperators** peut être réalisée à l'aide des outils standards d'administration du système d'exploitation.

Tous les privilèges sont accordés au groupe **KLAdmins** et les privilèges de lecture au groupe **KLOperators**. L'ensemble des droits présentés dans le groupe **KLAdmins** n'est pas disponible à la modification.

Les utilisateurs du groupe **KLAdmins** portent le nom : les *administrateurs de Kaspersky Security Center*, les utilisateurs du groupe **KLOperators** – les *opérateurs de Kaspersky Security Center*.

Outre les utilisateurs du groupe **KLAdmins**, les privilèges d'administrateur de Kaspersky Security Center sont accordés aux administrateurs locaux des appareils sur lesquels le Serveur d'administration est installé.

Il est possible d'exclure les administrateurs locaux de la liste des utilisateurs qui possèdent les privilèges d'administrateur de Kaspersky Security Center.

Toutes les opérations lancées par les administrateurs de Kaspersky Security Center sont exécutées avec les privilèges du compte utilisateur du Serveur d'administration.

Pour chaque Serveur d'administration dans le réseau, un propre groupe **KLAdmins** peut être formé. Ce groupe possédera des privilèges uniquement dans le cadre du travail avec ce Serveur.

Si les appareils appartiennent au même domaine et font partie des groupes d'administration de Serveurs différents, l'administrateur est l'administrateur de Kaspersky Security Center dans le cadre de tous ces groupes d'administration. Le groupe **KLAdmins** est unique pour ces groupes d'administration et est créé lors de l'installation du premier Serveur d'administration. Les opérations lancées par l'administrateur Kaspersky Security Center sont exécutées avec les privilèges du compte utilisateur du Serveur d'administration pour lequel elles ont été lancées.

Après l'installation de l'application, l'administrateur Kaspersky Security Center peut procédez comme suit :

- Modifier les privilèges accordés aux groupes **KLOperators**.
- Définir les privilèges d'accès aux fonctions de l'application Kaspersky Security Center aux autres groupes de sécurité et aux utilisateurs particuliers enregistrés sur le poste de travail de l'administrateur.
- Définir les privilèges d'accès des utilisateurs au travail dans chaque groupe d'administration.

L'administrateur de Kaspersky Security Center peut établir les privilèges d'accès à chaque groupe d'administration ou aux autres objets du Serveur d'administration dans la section **Sécurité** de la fenêtre des propriétés de l'objet sélectionné.

Vous pouvez surveiller les actions de l'utilisateur à l'aide des enregistrements sur les événements dans le fonctionnement du Serveur d'administration. Les enregistrements relatifs aux événements sont affichés dans l'entrée **Serveur d'administration**, sur l'onglet **Événements**. Ces événements possèdent le niveau d'importance **Événements d'information**, et les types d'événement commencent par le mot « **Audit** ».

Conditions de connexion au Serveur d'administration via Internet

Si le Serveur d'administration est un serveur à distance, c'est-à-dire il se trouve en dehors du réseau d'entreprise, les appareils clients se connectent à lui via Internet.

Pour la connexion des appareils au Serveur d'administration via Internet, il est nécessaire d'exécuter les conditions suivantes :

- Le Serveur d'administration à distance doit posséder l'adresse IP externe et, sur cette adresse, le port entrant 13000 doit être ouvert (pour la connexion depuis les agents d'administration). Il est aussi recommandé d'ouvrir le port UDP 13000 (pour la réception des notifications de la désactivation des appareils).

- Des Agents d'administration doivent être installés sur les appareils.

- Lors de l'installation de l'Agent d'administration sur les appareils, l'adresse IP externe du Serveur d'administration à distance doit être indiquée. Si pour l'installation, un paquet d'installation est utilisé, indiquez l'adresse IP externe manuellement dans les propriétés du paquet d'installation, dans la section **Paramètres**.

- Pour administrer les applications et les tâches d'un appareil à l'aide du Serveur d'administration à distance, dans la fenêtre des propriétés correspondant à cet appareil, dans la section **Général**, cochez la case **Maintenir la connexion au Serveur &d'administration**. Après avoir coché la case, il faut attendre la synchronisation de l'appareil distant avec le Serveur d'administration. La connexion permanente avec le Serveur d'administration peut prendre en charge pas plus de 300 appareils clients en même temps.

Pour accélérer l'exécution des tâches reçues depuis le Serveur d'administration à distance, vous pouvez ouvrir sur les appareils le port 15000. Dans ce cas pour lancer une tâche, le Serveur d'administration envoie un paquet spécial à l'Agent d'administration par le port 15000 sans attendre la synchronisation avec l'appareil.

Connexion sécurisée au Serveur d'administration

L'échange des informations entre les appareils clients et le Serveur d'administration, ainsi que la connexion de la Console d'administration au Serveur d'administration peuvent être exécutées en utilisant le protocole Security Transport du (SGBD Layer). Le protocole SSL permet d'identifier les parties, qui coopèrent lors de la connexion, de chiffrer les données transmises et de garantir leur intégrité tout au long de la transmission. L'authentification des parties coopérants et le chiffrement des données par clés ouvertes sont à la base du protocole SSL.

Authentification du Serveur d'administration lors de la connexion de l'appareil

Lors de la première connexion de l'appareil client au Serveur d'administration, l'Agent d'administration sur l'appareil reçoit une copie du certificat de Serveur d'administration et le sauvegarde localement.

> Lors de l'installation locale de l'Agent d'administration sur l'appareil, le certificat de Serveur d'administration peut être sélectionné à la main.

Selon la copie reçue du certificat, l'analyse des privilèges et des pouvoirs du Serveur d'administration sera réalisée au cours des connexions ultérieures.

Par la suite, lors de chaque connexion de l'appareil au Serveur d'administration, l'Agent d'administration demandera le certificat de Serveur d'administration et le comparera avec sa copie locale. S'ils ne concordent pas, l'accès du Serveur d'administration à l'appareil sera interdit.

Authentification du Serveur d'administration lors de la connexion de la Console d'administration

Lors de la première connexion au Serveur d'administration, la Console d'administration demande le certificat de Serveur d'administration et sauvegarde sa copie localement sur le poste de travail de l'administrateur. Selon la copie reçue du certificat, au cours des connexions suivantes de la Console d'administration au Serveur d'administration, l'identification du Serveur d'administration sera exécutée.

Si le certificat de Serveur d'administration ne concorde pas avec la copie du certificat sauvegardée sur le poste de travail de l'administrateur, la Console d'administration affiche une demande afin de pouvoir confirmer la connexion au Serveur d'administration portant le nom attribué et d'obtenir un nouveau certificat. Après la connexion, la Console d'administration sauvegardera la copie du nouveau certificat de Serveur d'administration. Elle sera utilisée ultérieurement pour identifier le Serveur.

Configuration de la liste d'autorisation d'adresses IP pour se connecter au Serveur d'administration

Par défaut, les utilisateurs peuvent se connecter à Kaspersky Security Center depuis n'importe quel appareil sur lequel Kaspersky Security Center Web Console (ci-après dénommée Web Console) ou la Console d'administration basée sur MMC est installée. Cependant, vous pouvez configurer le Serveur d'administration afin que les utilisateurs puissent s'y connecter uniquement à partir d'appareils avec des adresses IP autorisées. Dans ce cas, même si un intrus vole un compte de Kaspersky Security Center, il ne pourra pas se connecter à Kaspersky Security Center car l'adresse IP de l'appareil de l'intrus ne se trouve pas dans la liste d'autorisation.

L'adresse IP est vérifiée lorsqu'un utilisateur se connecte à Kaspersky Security Center ou exécute une application qui interagit avec le Serveur d'administration via Kaspersky Security Center OpenAPI. À ce moment, l'appareil d'un utilisateur tente d'établir une connexion avec le Serveur d'administration. Si une adresse IP de l'appareil ne figure pas dans la liste d'autorisation, l'erreur d'authentification se produit et l'événement KLAUD_EV_SERVERCONNECT signale qu'une connexion avec le Serveur d'administration n'a pas été établie.

Conditions requises pour une liste d'autorisation d'adresses IP

Les adresses IP sont vérifiées uniquement lorsque les applications suivantes tentent de se connecter au Serveur d'administration :

- Web Console Server

  Si vous vous connectez à Web Console sur un appareil et que le serveur de Web Console est installé sur un autre appareil, vous pouvez configurer un pare-feu sur l'appareil où le serveur de Web Console est installé à l'aide des moyens standard du système d'exploitation. Ensuite, si quelqu'un essaie de se connecter à Web Console, un pare-feu empêche les intrus d'intervenir.

- Console d'administration
- Applications interagissant avec le Serveur d'administration via les objets d'automatisation klakaut
- Applications interagissant avec le Serveur d'administration via OpenAPI, comme Kaspersky Anti Targeted Attack Platform ou Kaspersky Security for Virtualization

Par conséquent, indiquez les adresses des appareils sur lesquels les applications répertoriées ci-dessus sont installées.

Vous pouvez définir des adresses IPv4 et IPv6. Vous ne pouvez pas spécifier de plages d'adresses IP.

Comment établir une liste d'autorisation d'adresses IP

Si vous n'avez pas encore défini de liste d'autorisation, suivez les instructions ci-dessous.

Pour établir une liste d'autorisation d'adresses IP pour se connecter à Kaspersky Security Center :

1. Sur l'appareil du Serveur d'administration, exécutez l'invite de commande sous un compte avec des droits d'administrateur.

2. Remplacez votre répertoire actuel par le dossier d'installation de Kaspersky Security Center (généralement, <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center).

3. Saisissez la commande suivante en utilisant les droits d'administrateur :
   `klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "<IP addresses>" -t s`

   Indiquez les adresses IP qui répondent aux exigences énumérées ci-dessus. Plusieurs adresses IP doivent être séparées par un point-virgule.

   Exemple d'autorisation de connexion d'un seul appareil au Serveur d'administration :

   `klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "192.0.2.0" -t s`

   Exemple d'autorisation de connexion de plusieurs appareils au Serveur d'administration :

   `klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "192.0.2.0; 198.51.100.0; 203.0.113.0" -t s`

4. Relancez le service du Serveur d'administration.

Vous pouvez savoir si vous avez correctement configuré la liste d'autorisation d'adresses IP dans les journaux d'événement Kaspersky sur le Serveur d'administration.

Comment modifier une liste d'autorisation d'adresses IP

Vous pouvez modifier une liste d'autorisation comme vous l'avez fait lors de sa création. Pour cela, exécutez la même commande et indiquez une nouvelle liste d'autorisation :

```
klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "<IP addresses>" -t s
```

Si vous souhaitez supprimer certaines adresses IP de la liste d'autorisation, réécrivez-la. Par exemple, votre liste d'autorisation inclut les adresses IP suivantes : 192.0.2.0 ; 198.51.100.0 ; 203.0.113.0. Vous souhaitez supprimer l'adresse IP 198.51.100.0. Pour ce faire, saisissez la commande suivante à l'invite de commande, en :

```
klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "192.0.2.0; 203.0.113.0" -t s
```

N'oubliez pas de redémarrer le service du Serveur d'administration.

Comment réinitialiser une liste d'autorisation configurée d'adresses IP

Pour réinitialiser une liste d'autorisation d'adresses IP déjà configurée, procédez comme suit :

1. Entrez la commande suivante à l'invite de commande, en utilisant les droits d'administrateur :
   `klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "" -t s`

2. Relancez le service du Serveur d'administration.

Après cela, les adresses IP ne sont plus vérifiées.

Utilisation de l'utilitaire klsclag pour fermer le port 13291

Le port 13291 du Serveur d'administration est utilisé pour recevoir les connexions des Consoles d'administration. Ce port est ouvert par défaut. Si vous ne souhaitez pas utiliser la Console d'administration MMC ou l'utilitaire klakaut, vous pouvez fermer ce port à l'aide de l'utilitaire klsclag. Cet utilitaire modifie la valeur du paramètre KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN.

Pour fermer le port 13291 :

1. Exécutez l'invite de commande Windows en utilisant les droits d'administrateur, puis remplacez votre répertoire actuel par celui contenant l'utilitaire klscflag. L'utilitaire klsclag se trouve dans le dossier dans lequel le Serveur d'administration est installé. Chemin d'installation par défaut est <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

2. Exécutez la commande suivante dans la ligne de commande :
   ```
   klscflag -ssvset -pv klserver -s 87 -n KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN -sv false -
   svt BOOL_T -ss "|ss_type = \"SS_SETTINGS\";"
   ```

3. Relancez le service du Serveur d'administration de Kaspersky Security Center.

   Le port 13291 est fermé.

Pour vérifier si le port 13291 a été fermé avec succès :

Exécutez la commande suivante dans la ligne de commande :

```
klscflag -ssvget -pv klserver -s 87 -n KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN -svt BOOL_T -
ss "|ss_type = \"SS_SETTINGS\";"
```

Cette commande renvoie le résultat suivant :

```
+--- (PARAMS_T)
+---KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN = (BOOL_T)false
```

La valeur `false` signifie que le port est fermé. Sinon, la `true` valeur s'affiche.

Se déconnecter du Serveur d'administration

Pour se déconnecter du Serveur d'administration, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le nœud correspondant au Serveur d'administration duquel il faut se déconnecter.

2. Sélectionnez l'option **S&e déconnecter du Serveur d'administration** dans le menu contextuel de l'entrée.

Ajout d'un Serveur d'administration à l'arborescence de la console

Pour ajouter un Serveur d'administration à l'arborescence de la console, procédez comme suit :

1. Dans la fenêtre principale de Kaspersky Security Center, sélectionnez l'entrée **Kaspersky Security Center** dans l'arborescence de la console.

2. Dans le menu contextuel, sélectionnez l'option **Nouveau** → **Serveur d'administration**.

Une entrée appelée **Serveur d'administration - <Device name> (Non connecté)** apparaîtra dans l'arborescence de console. Utilisez cette entrée pour la connecter à n'importe quel Serveur d'administration installé sur votre réseau.

Suppression d'un Serveur d'administration de l'arborescence de console

Pour supprimer un Serveur d'administration de l'arborescence de la console, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez l'entrée correspondant au Serveur d'administration à supprimer.

2. Sélectionnez l'option **Supprimer** dans le menu contextuel de l'entrée.

Ajout d'un Serveur d'administration virtuel à l'arborescence de la console

Pour ajouter un Serveur d'administration virtuel à l'arborescence de la console, procédez comme suit :

1. Dans l'arborescence de la console, choisissez le nœud reprenant le nom du Serveur d'administration dont vous avez besoin et pour lequel il faut créer Serveur d'administration virtuel.

2. Dans l'entrée du Serveur d'administration, choisissez le dossier **Serveurs d'administration**.

3. Dans l'espace de travail du dossier **Serveurs d'administration**, cliquez sur le lien **Ajouter un Serveur d'administration virtuel**.

   L'assistant de création du Serveur d'administration virtuel démarre.

4. Dans la fenêtre **Nom du Serveur d'administration virtuel**, indiquez le nom du Serveur d'administration virtuel à créer.

   Le nom du Serveur d'administration virtuel ne peut pas contenir plus de 255 caractères, ni de caractères spéciaux ("*<>?\:|).

5. Dans la fenêtre **Saisie de l'adresse de connexion des appareils au Serveur d'administration virtuel**, spécifiez l'adresse de connexion de l'appareil

   L'adresse de connexion du Serveur d'administration virtuel est une adresse de réseau via laquelle les appareils seront connectés. L'adresse de connexion comprend deux parties : l'adresse de réseau du Serveur d'administration physique et le nom du Serveur d'administration virtuel séparés par un slash. Le nom du Serveur d'administration virtuel sera automatiquement renseigné. L'adresse indiquée sera utilisée sur ce Serveur d'administration virtuel comme adresse par défaut dans les paquets d'installation de l'Agent d'administration.

6. Dans la fenêtre **Création du compte d'administrateur du Serveur d'administration virtuel**, désignez un utilisateur de la liste en tant qu'administrateur du Serveur virtuel ou ajoutez un nouveau compte administrateur en cliquant sur le bouton **Créer**.

   Vous pouvez indiquer plusieurs comptes utilisateur.

Dans l'arborescence de la console, un nœud appelé **Serveur d'administration <Name of virtual Administration Server>** est créé.

Changement du compte utilisateur du service du Serveur d'administration. Utilitaire klsrvswch

S'il vous faut modifier le compte utilisateur du service du Serveur d'administration, défini lors de l'installation de l'application Kaspersky Security Center, vous pouvez utiliser l'utilitaire de changement du compte du service du Serveur d'administration klsrvswch.

Lors de l'installation de Kaspersky Security Center, l'utilitaire est automatiquement copié dans le dossier d'installation de l'application.

Le nombre de lancements de l'utilitaire est illimité.

Vous devez lancer l'utilitaire klsrvswch sur l'appareil du Serveur d'administration sous le compte avec privilèges d'administrateur qui a été utilisé pour installer le Serveur d'administration.

L'utilitaire klsrvswch permet de modifier le type de compte utilisateur. Par exemple, si vous utilisez un compte utilisateur local, vous pouvez le remplacer par un compte de domaine ou un compte de service administré (et vice versa). L'utilitaire klsrvswch ne vous permet pas de modifier le type de compte en compte de service administré de groupe (gMSA).

Windows Vista et les versions ultérieures de Windows n'acceptent pas l'utilisation d'un compte LocalSystem pour le Serveur d'administration. Dans ces versions de Windows, l'option **Compte LocalSystem** n'est pas active.

Pour modifier le compte utilisateur du service du Serveur d'administration, procédez comme suit :

1. Lancez l'utilitaire klsrvswch depuis le dossier d'installation du Kaspersky Security Center. Chemin d'installation par défaut : <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

   Finalement, l'Assistant de changement du compte utilisateur du service du Serveur d'administration se lance. Suivez les instructions de l'assistant.

2. Dans la fenêtre **Compte utilisateur du service du Serveur d'administration**, sélectionnez **Compte LocalSystem**.

Suite au fonctionnement de l'Assistant, le compte utilisateur du Serveur d'administration change. Le service du Serveur d'administration se lance sous le *Compte LocalSystem* et utilise ses identifiants.

Pour que Kaspersky Security Center fonctionne correctement, il faut que le compte utilisateur possède les droits d'accès d'administrateur des ressources pour le placement de la base des informations du Serveur d'administration au démarrage du service du Serveur d'administration.

Pour remplacer un compte utilisateur du service du Serveur d'administration par un compte utilisateur ou un compte de service administré :

1. Lancez l'utilitaire klsrvswch depuis le dossier d'installation du Kaspersky Security Center. Chemin d'installation par défaut : <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

   Finalement, l'Assistant de changement du compte utilisateur du service du Serveur d'administration se lance. Suivez les instructions de l'assistant.

2. Dans la fenêtre **Compte utilisateur du service du Serveur d'administration**, sélectionnez **Compte utilisateur**.

3. Cliquez sur le bouton **Rechercher**.

   La fenêtre **Sélectionnez l'utilisateur** s'ouvre.

4. Dans la fenêtre **Sélectionnez l'utilisateur**, cliquez sur le bouton **Type d'objet**.

5. Dans la liste des types d'objet, sélectionnez **Utilisateurs** (si vous voulez un compte utilisateur) ou **Comptes utilisateur du service** (si vous voulez un compte utilisateur du service administré), puis cliquez **OK**.

6. Dans le champ du nom de l'objet, saisissez le nom du compte ou une partie de celui-ci, puis cliquez sur **Vérifier les noms**.

7. Dans la liste des correspondances, sélectionnez le nom nécessaire, puis cliquez sur **OK**.

8. Si vous avez sélectionné **Compte utilisateur du service** dans la fenêtre **Mot de passe du compte utilisateur**, laissez les champs **Mot de passe** et **Confirmation du mot de passe** vides. Si vous avez sélectionné **Utilisateurs**, saisissez un nouveau mot de passe pour l'utilisateur, puis confirmez-le.

Le service du Serveur d'administration compte utilisateur sera être modifié le compte utilisateur que vous avez sélectionné.

Lors de l'utilisation de Microsoft SQL Server en mode d'authentification des comptes utilisateurs par les outils Windows, il faut assurer l'accès à la base des données. Le compte utilisateur doit posséder la base de données de Kaspersky Security Center. Par défaut, il faut utiliser le schéma dbo.

Modification des informations d'identification du SGBD

Vous devrez peut-être modifier les informations d'identification du SGBD, par exemple, afin d'effectuer une rotation des informations d'identification à des fins de sécurité.

Pour modifier les identifiants SGBD dans un environnement Windows à l'aide de klsrvswch.exe :

1. Lancez l'utilitaire klsrvswch depuis le dossier d'installation du Kaspersky Security Center. Chemin d'installation par défaut : <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

   Vous devez lancer l'utilitaire klsrvswch sur l'appareil du Serveur d'administration sous le compte avec privilèges d'administrateur qui a été utilisé pour installer le Serveur d'administration.

2. Cliquez sur le bouton **Suivant** de l'assistant jusqu'à atteindre l'étape **Modifier les identifiants d'accès au SGBD**.

3. À l'étape **Modifier les identifiants d'accès au SGBD** de l'Assistant, procédez comme suit :

   L'étape **Modifier les identifiants d'accès au SGBD** de l'assistant est ignorée si l'authentification Windows est utilisée.

   - Sélectionnez l'option **Appliquer les nouveaux identifiants**.
   - Spécifiez un nouveau nom de compte dans le champ **Compte**.
   - Spécifiez un nouveau mot de passe pour un compte dans le champ **Mot de passe**.
   - Spécifiez le nouveau mot de passe dans le champ **Confirmer le mot de passe**.

   Vous devez spécifier les identifiants d'un compte qui existe dans le SGBD.

4. Cliquez sur le bouton **Suivant**.

Une fois l'assistant terminé, les identifiants SGBD sont modifiés.

L'utilitaire klsrvswch peut uniquement être utilisé pour modifier le mot de passe du compte pour l'authentification SQL. Il n'est pas possible de change de méthode d'autorisation. Pour changer de méthode d'autorisation, réinstallez le Serveur d'administration et spécifiez les paramètres souhaités.

Modification du dossier partagé du Serveur d'administration

Le dossier partagé du Serveur d'administration est indiqué lors de l'installation du Serveur d'administration. Vous pouvez modifier l'emplacement du dossier partagé dans les propriétés du Serveur d'administration.

Pour modifier le dossier partagé, procédez comme suit :

1. Créez un dossier de partage réseau et configurez les permissions pour le partage et pour la structure des dossiers afin d'octroyer le contrôle total au sous-groupe **Tout le monde**.
2. Dans l'arborescence de la console de Kaspersky Security Center, ouvrez le menu contextuel du dossier **Serveur d'administration**, puis sélectionnez **Propriétés**.
3. Dans la fenêtre des propriétés du Serveur d'administration, dans le volet **Sections**, sélectionnez **Avancé**, puis **Dossier partagé du Serveur d'administration**.
4. Dans la section **Dossier partagé du Serveur d'administration**, cliquez sur le bouton **Modifier**.
5. Sélectionnez le dossier que vous souhaitez utiliser comme dossier partagé.
6. Cliquez sur **OK** pour fermer la fenêtre des propriétés du Serveur d'administration.
7. Attribuez des droits de lecture au sous-groupe **Tout le monde** pour le dossier que vous avez sélectionné comme étant partagé.

Résolution des problèmes avec les entrées du Serveur d'administration

L'arborescence de la console dans le volet gauche de la Console d'administration contient les entrées des serveurs d'administration. Vous pouvez ajouter autant de serveurs d'administration que vous le souhaitez à l'arborescence.

La liste des entrées du Serveur d'administration dans l'arborescence de la console est stockée dans un cliché instantané d'un fichier .msc par la console de gestion Microsoft. Le cliché instantané de ce fichier se trouve dans le dossier %USERPROFILE%\AppData\Roaming\Microsoft\MMC\ de l'appareil où la Console d'administration est installée. Pour chaque entrée du Serveur d'administration, le fichier contient les informations suivantes :

- Adresse du Serveur d'administration
- Numéro de port
- Utilisation de TLS

  Ce paramètre dépend du numéro du port utilisé pour connecter la Console d'administration avec le Serveur d'administration.
- Nom d'utilisateur
- Certificat du Serveur d'administration

Elimination des défaillances

Lorsque la Console d'administration se connecte au Serveur d'administration, le certificat stocké localement est comparé au certificat du Serveur d'administration. Si les certificats ne correspondent pas, la Console d'administration génère une erreur. Par exemple, les certificats peuvent ne plus correspondre si vous remplacez le certificat du Serveur d'administration. Dans ce cas, recréez l'entrée du Serveur d'administration dans la console.

Pour recréer une entrée du Serveur d'administration, procédez comme suit :

1. Fermez la fenêtre de la Console d'administration de Kaspersky Security Center.
2. Supprimez le fichier de Kaspersky Security Center 15.1 dans %USERPROFILE%\AppData\Roaming\Microsoft\MMC\.
3. Exécution de la Console d'administration de Kaspersky Security Center.

   Vous serez invité à vous connecter au Serveur d'administration et à accepter son certificat existant.
4. Exécutez une des actions suivantes :

   - Acceptez le certificat existant en cliquant sur le bouton **Oui**.
   - Pour spécifier votre certificat, cliquez sur le bouton **Non**, puis accédez au fichier de certificat à utiliser pour authentifier le Serveur d'administration.

Le problème relatif au certificat est résolu. Vous pouvez utiliser la Console d'administration pour vous connecter au Serveur d'administration.

Affichage et modification des paramètres du Serveur d'administration

Vous pouvez configurer les paramètres du Serveur d'administration dans la fenêtre des propriétés du Serveur d'administration.

Pour ouvrir la fenêtre Propriétés : Serveur d'administration,

Dans le menu contextuel de l'entrée du Serveur d'administration dans l'arborescence de la console, sélectionnez l'option **Propriétés**.

Configuration des paramètres généraux du Serveur d'administration

Vous pouvez configurer les paramètres généraux du Serveur d'administration dans les sections **Général**, **Paramètres de connexion au Serveur d'administration**, **Stockage d'événements** et **Sécurité** de la fenêtre des propriétés du Serveur d'administration.

La section **Sécurité** ne s'affiche pas dans la fenêtre des propriétés du Serveur d'administration si son affichage est désactivé dans l'interface de la Console d'administration.

*Pour activer l'affichage de la section **Sécurité** dans la Console d'administration, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le Serveur d'administration que vous voulez.
2. Dans le menu **Consulter** de la fenêtre principale de l'application, sélectionnez **&Configuration de l'interface**.
3. Dans la fenêtre **Configuration de l'interface** qui s'ouvre, cochez la case **Afficher les sections avec les paramètres de sécurité** et cliquez sur **OK**.
4. Dans la fenêtre contenant le message de l'application, cliquez sur **OK**.

La section **Sécurité** s'affiche dans la fenêtre des propriétés du Serveur d'administration.

Paramètres d'interface de la Console d'administration

Vous pouvez ajuster les paramètres d'interface de la Console d'administration pour afficher ou masquer les contrôles de l'interface utilisateur liés aux fonctionnalités suivantes :

- Gestion des vulnérabilités et des correctifs
- Chiffrement et protection des données
- Paramètres Endpoint control
- Administration des appareils mobiles
- Serveurs d'administration secondaires
- Sections Paramètres de sécurité

Pour configurer les paramètres d'interface de la Console d'administration :

1. Dans l'arborescence de la console, sélectionnez le Serveur d'administration que vous voulez.
2. Dans le menu **Consulter** de la fenêtre principale de l'application, sélectionnez **&Configuration de l'interface**.
3. Dans la fenêtre **Configuration de l'interface** qui s'ouvre, cochez les cases en regard des fonctionnalités que vous souhaitez afficher et cliquez sur **OK**.
4. Dans la fenêtre contenant le message de l'application, cliquez sur **OK**.

Les fonctionnalités sélectionnées seront affichées dans l'interface de la Console d'administration.

Traitement et stockage des événements sur le Serveur d'administration

Les informations sur les événements qui surviennent durant le fonctionnement de l'application et des appareils administrés sont stockées dans la base de données du Serveur d'administration. Chaque événement est lié à un type défini et à un niveau d'importance (*Événement critique*, *Erreur de fonctionnement*, *Avertissement*, *Information*). En fonction des conditions dans lesquelles l'événement s'est produit, l'application peut attribuer aux événements d'un type unique des niveaux d'importance différents.

Vous pouvez consulter les types et les niveaux d'importance dans la section **Paramètres des événements** de la fenêtre de propriétés du Serveur d'administration. Dans la section **Paramètres des événements**, vous pouvez aussi configurer les paramètres de traitement de chaque événement du Serveur d'administration :

- Consignation des événements sur le Serveur d'administration et dans les journaux des événements du système d'exploitation sur l'appareil et sur le Serveur d'administration.
- Mode de notification de l'administrateur sur l'événement (par exemple, SMS, message électronique).

Dans la section **Stockage d'événements** de la fenêtre de propriétés du Serveur d'administration, vous pouvez configurer les paramètres de stockage des événements dans la base de données du Serveur d'administration en limitant le nombre d'enregistrements sur les événements et la durée de stockage de ces derniers. Quand vous définissez le nombre maximal d'événements, l'application calcule un espace de stockage approximatif requis pour la quantité indiquée. Ce calcul approximatif permet d'évaluer si vous avez assez d'espace libre sur le disque pour éviter un débordement de base de données. Par défaut, la capacité de la base de données du Serveur d'administration est de 400 000 événements. La capacité maximale recommandée de la base de données est de 45 millions d'événements.

L'application vérifie la base de données toutes les 10 minutes. Si le nombre d'événements atteint la valeur maximale indiquée plus 10 000, l'application supprime les événements les plus anciens de manière à ne conserver que le nombre maximal d'événements indiqué.

Quand le Serveur d'administration supprime les anciens événements, il ne peut pas enregistrer les nouveaux événements dans la base de données. Durant cette période, les informations relatives aux événements qui ont été rejetés sont écrites dans le journal des événements Kaspersky. Les nouveaux événements sont placés dans une file d'attente et enregistrés dans la base de données dès que la suppression est terminée.

Vous pouvez modifier les paramètres de n'importe quelle tâche pour enregistrer les événements liés à la progression de la tâche ou enregistrer uniquement les résultats de l'exécution de la tâche. Ainsi, vous diminuez le nombre d'événements dans la base de données, vous augmentez la vitesse de fonctionnement des scénarios liés à l'analyse du tableau des événements dans la base de données, et vous réduisez le risque que les événements critiques soient ignorés.

Consultation du journal des connexions au Serveur d'administration

L'historique des connexions et des tentatives de connexion au Serveur d'administration lors de son fonctionnement peut être enregistré dans un fichier journal. Les informations de ce fichier permettent de suivre non seulement les connexions à l'intérieur de votre infrastructure réseau, mais également les tentatives non autorisées d'accès au Serveur d'administration.

Pour enregistrer les événements de connexion au Serveur d'administration, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le Serveur d'administration pour lequel vous souhaitez enregistrer les événements dans le journal.
2. Dans le menu contextuel Serveur d'administration, sélectionnez l'option **Propriétés**.
3. Dans la fenêtre des propriétés qui s'ouvre, dans la section **Paramètres de connexion au Serveur d'administration**, sélectionnez la sous-section **Ports de connexion**.
4. Activer l'option **&Consigner les événements de connexion du Serveur d'administration**.
5. Cliquez sur **OK** pour fermer la fenêtre des propriétés du Serveur d'administration.

Tous les autres événements de connexions entrantes vers le Serveur d'administration, résultats d'authentification et erreurs SSL seront enregistrés dans le fichier %ProgramData%\KasperskyLab\adminkit\logs\sc.syslog.

Contrôle de l'émergence d'épidémies de virus

Kaspersky Security Center vous permet de réagir opportunément à l'apparition des menaces des épidémies de virus. L'évaluation de l'épidémie de virus se réalise par le contrôle de l'activité de virus sur les appareils.

Vous pouvez configurer les règles d'évaluation de menaces virales et les actions à entreprendre dans le cas de leur apparition. Pour ce faire, la section **Attaque de virus** de la fenêtre des propriétés du Serveur d'administration.

Vous pouvez spécifier la procédure de notification de l'événement *Attaque de virus* dans la section **Configuration de l'événement** de la fenêtre des propriétés Serveur d'administration, dans la fenêtre des propriétés de l'événement *Attaque de virus*.

L'événement *Attaque de virus* se forme quand l'événement *Objet malveillant détecté* survient dans le fonctionnement des applications de sécurité. Par conséquent, pour pouvoir identifier une épidémie de virus, les informations sur les événements *Objet malveillant détecté* doivent être enregistrées sur le Serveur d'administration.

Les paramètres d'enregistrement des informations sur l' événement *Objet malveillant détecté* sont définis dans les stratégies des applications de sécurité.

> Sous le titre *Objet malveillant détecté*, les informations en provenance des appareils du Serveur d'administration principal sont prises en compte. Les informations depuis les Serveurs d'administration secondaires ne sont pas prises en compte. Pour chaque Serveur d'administration secondaire, les paramètres de l'événement *Attaque de virus* doivent être configurés individuellement.

Restriction du trafic

Pour diminuer le trafic dans le réseau, il est possible de limiter la vitesse de transfert des données sur le Serveur d'administration depuis les plages IP ou les intervalles IP en particulier.

Vous pouvez créer et configurer les règles de restriction du trafic dans la section **Trafic** de la fenêtre des propriétés du Serveur d'administration.

Pour créer une règle de la restriction du trafic, procédez comme suit :

1. Dans l'arborescence de la console, choisissez le nœud reprenant le nom du Serveur d'administration pour lequel il faut créer une règle de restriction du trafic.
2. Dans le menu contextuel Serveur d'administration, sélectionnez l'option **Propriétés**.
3. Dans la fenêtre des propriétés du Serveur d'administration, sélectionnez la section **Trafic**.

4. Cliquez sur le bouton **Ajouter**.

5. Définissez les paramètres suivants dans la section **Nouvelle règle** :

   Dans la section **Plage d'adresses IP pour lesquelles il faut limiter le trafic**, vous pouvez sélectionner le mode de définition du sous-réseau ou de la plage pour lequel la vitesse sera réduite et indiquer la valeur des paramètres correspondant à la méthode sélectionnée. Sélectionnez l'une des méthodes ci-dessous :

   - **Définir la plage en utilisant l'adresse et le &masque de réseau**

     Le trafic se limite selon les paramètres du sous-réseau. Renseignez l'adresse du sous-réseau et le masque de sous-réseau pour définir l'intervalle des limites du trafic.

     Vous pouvez également cliquer sur **Parcourir** pour ajouter des sous-réseaux tirés de la liste globale des sous-réseaux.

   - **Définir la plage en utilisant des adresses de début et de fin**

     Le trafic se limite d'après l'intervalle d'adresses IP. Indiquez l'intervalle d'adresses IP dans les champs de saisie **Début** et **Fin**.

     Par défaut, cette option est sélectionnée.

   La section **Restriction du trafic** permet de régler les limites de la vitesse de transfert des données :

   - **Période**

     La plage horaire pendant laquelle la restriction du trafic sera en place. Les limites de la plage horaire peuvent être indiquées dans les champs de saisie.

   - **Limite (Ko/s)**

     Valeur critique de la vitesse totale de transmission des données entrant et sortant du Serveur d'administration. La restriction s'applique durant l'intervalle défini dans le champ **Période**.

   - **Limiter le trafic pour le temps restant (Ko/s)**

     Le trafic est limité non seulement pendant l'intervalle indiqué dans le champ **Période**, mais aussi à d'autres moments.

     Celle-ci est décochée par défaut. La valeur du champ peut ne pas correspondre à la valeur du champ **Restriction (Ko/s)**.

Les règles de restriction du trafic touchent principalement le transfert de fichiers. Ces règles ne s'appliquent pas au trafic généré par la synchronisation entre le Serveur d'administration et l'Agent d'administration ou entre les Serveurs d'administration principaux et secondaires.

Configuration des paramètres du Serveur Web

Le Serveur Web est utilisé pour publier les paquets d'installation autonomes, les profils MDM iOS, ainsi que les fichiers du dossier partagé.

Vous pouvez configurer les paramètres de connexion du Serveur Web au Serveur d'administration et définir le certificat de Serveur Web dans la section **Serveur Internet** de la fenêtre des propriétés du Serveur d'administration.

Travail avec les utilisateurs internes

Les comptes utilisateur des *utilisateurs internes* sont utilisés pour travailler avec les Serveurs d'administration virtuels. Dans le cadre de fonctionnalité de l'application Kaspersky Security Center, les utilisateurs internes possèdent les privilèges des utilisateurs réels.

Les comptes des utilisateurs internes sont créés et utilisés uniquement à l'intérieur de Kaspersky Security Center. Les informations sur les utilisateurs internes ne sont pas transmises au système d'exploitation. Kaspersky Security Center effectue l'authentification des utilisateurs internes.

Vous pouvez configurer les paramètres des comptes utilisateurs internes dans le dossier **Comptes utilisateurs** de l'arborescence de la console.

Copie de sauvegarde et restauration des paramètres du Serveur d'administration

La tâche de sauvegarde et l'utilitaire klbackup permettent de réaliser une sauvegarde des paramètres du Serveur d'administration et des bases de données qu'il utilise. La copie de sauvegarde reprend tous les paramètres principaux et les objets du Serveur d'administration : les certificats du Serveur d'administration, les clés principales de chiffrement des disques des appareils administrés, les clés pour les licences, la structure des groupes d'administration avec tout le contenu, les tâches, les stratégies, etc. La copie de sauvegarde permet de restaurer le fonctionnement du Serveur d'administration très rapidement : d'une dizaine de minutes à deux heures.

En l'absence d'une copie de sauvegarde, un échec peut provoquer la perte irréversible des certificats et de tous les paramètres du Serveur d'administration. Il faudrait alors configurer à nouveau Kaspersky Security Center et réaliser à nouveau le déploiement initial de l'Agent d'administration sur le réseau de l'organisation. De plus, les clés principales du chiffrement des disques des appareils administrés seraient également perdues, ce qui pose un risque de perte irréversible des données chiffrées sur les appareils dotés de Kaspersky Endpoint Security. Par conséquent, ne négligez pas les sauvegardes régulières du Serveur d'administration à l'aide de la tâche de sauvegarde standard.

L'Assistant de configuration initiale de l'application crée la tâche de sauvegarde des paramètres du Serveur d'administration avec le lancement quotidien à 4h00 du matin. Les copies de sauvegarde sont enregistrées par défaut dans le dossier %ALLUSERSPROFILE%\Application Data\KasperskySC.

Si vous utilisez une instance de Microsoft SQL Server installée sur un autre appareil en guise de SGBD, il faut modifier la tâche de sauvegarde : indiquer en tant que dossier d'enregistrement des copies de sauvegarde le chemin UNC, accessible en écriture, au service du Serveur d'administration et au service SQL Server. Cette exigence spéciale est le résultat des particularités de la sauvegarde dans le SGBD Microsoft SQL Server.

Si vous utilisez à titre de SGBD une instance locale de Microsoft SQL Server, il est recommandé d'enregistrer aussi les copies de sauvegarde sur un lecteur distinct afin de les protéger contre un endommagement simultané avec le Serveur d'administration.

Puisque la copie de sauvegarde contient d'importantes données, la tâche de sauvegarde et l'utilitaire klbackup prévoient la protection des copies de sauvegarde par mot de passe. Par défaut, aucun mot de passe n'est défini lors de la création de la tâche de sauvegarde. Vous devez spécifier un mot de passe dans les propriétés de la tâche de sauvegarde. Le non-respect de cette exigence signifie que les clés des certificats du Serveur d'administration, les clés pour les licences et la clé principale du chiffrement des disques des appareils administrés ne sont pas chiffrées.

Outre les sauvegardes régulières, il faut aussi créer une copie de sauvegarde avant toute modification importante, notamment avant la mise à jour du Serveur d'administration jusqu'à version la plus récente et avant l'installation des correctifs du Serveur d'administration.

Si vous utilisez Microsoft SQL Server en tant que SGBD, vous pouvez réduire la taille des copies de sauvegarde. Pour ce faire, activez l'option **Compresser la sauvegarde** dans les paramètres de SQL Server.

La restauration au départ d'une copie de sauvegarde s'opère via l'utilitaire klbackup sur l'instance opérationnelle du Serveur d'administration opérationnel qui vient d'être installé et dont la version est identique à la version du Serveur pour lequel la copie de sauvegarde avait été créée (ou plus récente).

L'instance du Serveur d'administration sur lequel la restauration a lieu doit utiliser un SGBD du même type (par exemple, le même SQL Server ou MariaDB) de la même version ou d'une version plus récente. La version du Serveur d'administration peut être la même (avec un correctif semblable ou plus récent) ou plus récente.

Cette section décrit les scénarios typiques de restauration des paramètres et des objets du Serveur d'administration.

Utilisation de la capture du système de fichiers pour réduire la durée de la copie de sauvegarde

Par rapport aux versions antérieures, l'inactivité du Serveur d'administration dans Kaspersky Security Center 15.1 pendant la copie de sauvegarde des données est inférieure. De plus, les paramètres de la tâche intègrent la fonction **Utiliser la capture du système de fichiers lors de l'exécution de la copie de sauvegarde des données**. Cette fonction permet de réduire davantage le temps mort provoqué par l'utilitaire klbackup lors de l'exécution des sauvegardes du cliché instantané du disque (cela prend quelques secondes) et de la création simultanée de la copie de la base de données (cela ne dure que quelques minutes). Après avoir créé le cliché instantané du disque et réalisé la copie de la base de données, klbackup permet à nouveau la connexion au Serveur d'administration.

Vous pouvez utiliser la fonction de création d'une capture du système de fichiers uniquement quand deux conditions sont remplies :

- Le dossier partagé du Serveur d'administration et le dossier %ALLUSERSPROFILE %\KasperskyLab se trouvent sur un disque logique et localement par rapport au Serveur d'administration.
- Le dossier %ALLUSERSPROFILE %\KasperskyLab ne contient pas de liens symboliques créés manuellement.

N'utilisez pas la fonction si une de ces deux conditions n'est pas remplie. Suite à une tentative de création d'une capture du système de fichiers, l'application affiche un message d'erreur.

Pour pouvoir utiliser la fonction, il faut avoir un compte utilisateur doté des privilèges de création de captures du disque logique sur lequel se trouve le dossier %ALLUSERSPROFILE%. Le compte utilisateur du service du Serveur d'administration n'a pas de tels privilèges.

Pour utiliser la fonction de création d'une capture du système de fichiers en vue de réduire la durée de la copie de sauvegarde, procédez comme suit :

1. Dans la section **Tâches**, choisissez la tâche de sauvegarde.
2. Dans le menu contextuel, sélectionnez l'option **Propriétés**.
3. Dans la fenêtre des propriétés de la tâche qui s'ouvre, sélectionnez la section **Paramètres**.
4. Cochez la case **Utiliser la capture du système de fichiers lors de l'exécution de la copie de sauvegarde des données**.
5. Dans les champs **Nom d'utilisateur** et **Mot de passe**, saisissez le nom et le mot de passe du compte utilisateur doté du privilège de création de captures du disque logique sur lequel se trouve le dossier %ALLUSERSPROFILE%.
6. Cliquez sur le bouton **Appliquer**.

Lors des prochains lancements de la tâche de copie de sauvegarde, l'utilitaire klbackup créera les captures du système de fichiers et les temps d'arrêt du Serveur d'administration pendant l'exécution de la tâche diminueront.

Panne de l'appareil doté du Serveur d'administration

Si l'appareil doté du Serveur d'administration tombe en panne après la défaillance, il est recommandé d'exécuter les actions suivantes :

- Attribuer la même adresse au nouveau Serveur d'administration : le nom NetBIOS, nom de domaine complet, IP statique, en fonction de ce qui avait été défini lors du déploiement des Agents d'administration.
- Installer le Serveur d'administration avec un SGBD du même type, de la même version ou d'une version plus récente. Il est possible d'installer la même version du Serveur avec le même correctif ou un correctif plus récent, ou une version plus récente. Après l'installation, il n'est pas nécessaire d'exécuter la configuration initiale à l'aide de l'Assistant.
- Dans le menu **Démarrer**, lancez l'utilitaire klbackup et réalisez la restauration.

Endommagement des paramètres du Serveur d'administration ou de la base de données

Si le Serveur d'administration est devenu inopérationnel suite à l'endommagement des paramètres ou de la base de données (par exemple, à cause d'une panne d'alimentation), il est conseillé de suivre le scénario de restauration suivant :

1. Lancer l'analyse du système de fichiers sur l'appareil concerné.
2. Désinstaller la version inopérationnelle du Serveur d'administration.

3. Installer à nouveau le Serveur d'administration avec la SGBD du même type et de version identique ou plus récente. Il est possible d'installer la même version du Serveur avec le même correctif ou un correctif plus récent, ou une version plus récente. Après l'installation, il n'est pas nécessaire d'exécuter la configuration initiale à l'aide de l'Assistant.

4. Depuis le menu **Démarrer**, lancez l'utilitaire de la copie de sauvegarde klbackup et réalisez la restauration.

Il est inadmissible de restaurer le Serveur d'administration à l'aide d'une méthode autre que l'utilitaire standard klbackup.

Tous les cas de restauration du Serveur d'administration à l'aide d'un logiciel tiers entraînent toujours une perte de synchronisation des données sur les nœuds de l'application distribuée Kaspersky Security Center et par conséquent, un mauvais fonctionnement de l'application.

Copie de sauvegarde et restauration des données du Serveur d'administration

La copie de sauvegarde des données permet de déplacer le Serveur d'administration d'un appareil à un autre sans perte d'informations. Grâce à la sauvegarde, vous pouvez restaurer les données lorsque vous déplacez la base de données du Serveur d'administration vers un autre appareil, ou lors de la mise à niveau vers une version plus récente de Kaspersky Security Center. Vous pouvez également utiliser la sauvegarde des données pour déplacer les données du Serveur d'administration de Kaspersky Security Center Windows sous la gestion de Kaspersky Security Center Linux (le déplacement des données de Kaspersky Security Center Windows n'est pas pris en charge).

Notez que les plug-ins d'administration installés ne sont pas sauvegardés. Après avoir restauré les données du Serveur d'administration à partir d'une copie de sauvegarde, vous devez télécharger et réinstaller les plug-ins pour les applications administrées.

Avant de sauvegarder les données du Serveur d'administration, vérifiez si un Serveur d'administration virtuel est ajouté au groupe d'administration. Si un Serveur d'administration virtuel est ajouté, assurez-vous qu'un administrateur est affecté à ce Serveur d'administration virtuel avant la sauvegarde. Vous ne pouvez pas accorder à l'administrateur des droits d'accès au Serveur d'administration virtuel après la sauvegarde. Notez que si les informations d'identification du compte administrateur sont perdues, vous ne pourrez pas attribuer un nouvel administrateur au serveur d'administrateur virtuel.

Pour sauvegarder ou restaurer un cluster de basculement de Kaspersky Security Center, vous devez interrompre le cluster dans son ensemble à des fins de maintenance, puis le redémarrer une fois la sauvegarde ou la restauration terminée.

Vous pouvez créer une copie de sauvegarde des données du Serveur d'administration à l'aide d'une des options suivantes :

- Créer et lancer la tâche de copie de sauvegarde des données via la Console d'administration.
- Lancez l'utilitaire klbackup sur l'appareil où le Serveur d'administration est installé. Cet utilitaire figure dans le kit de distribution de Kaspersky Security Center. Après l'installation du Serveur d'administration, l'utilitaire se trouve dans la racine du dossier de destination indiqué lors de l'installation de l'application.

La copie de sauvegarde des données du Serveur d'administration enregistre les données suivantes :

- Base de données du Serveur d'administration (stratégies, tâches, paramètres des applications, événements enregistrés sur le Serveur d'administration).
- Les données de configuration de la structure du groupe d'administration et des appareils clients.
- Le stockage des distributifs des applications pour l'installation à distance.
- Le certificat du Serveur d'administration.
- Contenu du dossier *Mises à jour*.

  Par défaut, le chemin du dossier est C:\ProgramData\KasperskyLab\adminkit\1093\.working\share\Updates\

La restauration des données du Serveur d'administration est possible uniquement à l'aide de l'utilitaire klbackup. Vous devez effectuer la restauration sur une instance opérationnelle du Serveur d'administration qui vient d'être installée et dont la version est identique à la version du Serveur pour lequel la copie de sauvegarde avait été créée (ou plus récente).

Tâche de sauvegarde des données du Serveur d'administration

Création d'une tâche de sauvegarde des données du Serveur d'administration

La tâche de sauvegarde est une tâche du Serveur d'administration. Elle est créé à l'aide de l'Assistant de démarrage rapide. Si la tâche de copie de sauvegarde, créée par l'Assistant de configuration initiale de l'application, a été supprimée, vous pouvez la créer manuellement.

Pour créer une tâche de sauvegarde des données du Serveur d'administration, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le dossier **Tâches**.
2. Lancez le processus de création de la tâche par un des moyens suivants :
   - En sélectionnant **Nouveau → Tâche** dans le menu contextuel du dossier **Tâches** dans l'arborescence de la console.
   - En cliquant sur le bouton **Créer une tâche** dans l'espace de travail.

   Ceci permet de lancer l'Assistant de création d'une tâche. Suivez les instructions de l'assistant. Dans la fenêtre de l'Assistant **Sélection du type de tâche**, sélectionnez le type de tâche **Sauvegarde des données du Serveur d'administration**.

La tâche **Sauvegarde des données du Serveur d'administration** peut être créée dans un seul exemplaire. Si la tâche de sauvegarde des données du Serveur d'administration a déjà été créée pour le Serveur d'administration, alors elle ne s'affiche pas dans la fenêtre de sélection du type de tâche de l'Assistant de création de la tâche de copie de sauvegarde du Serveur d'administration.

Configuration de la sauvegarde des données du Serveur d'administration

Après avoir créé la tâche de sauvegarde, vous pouvez configurer les paramètres de la tâche.

Pour configurer la tâche Sauvegarde des données du Serveur d'administration, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le dossier **Tâches**.
2. Dans le menu contextuel de la tâche **Sauvegarde des données du Serveur d'administration**, sélectionnez l'option **Propriétés**.

La fenêtre des propriétés de la tâche *Sauvegarde des données du Serveur d'administration* s'ouvre. Les propriétés suivantes sont disponibles :

- **Général**

  La section **Général** permet d'indiquer le nom de la tâche ainsi que de consulter la date de création de la tâche, la date de la dernière commande, les états de lancement de la tâche et les résultats de la tâche.

- **Notification**

  Le groupe **Notification** permet de configurer les paramètres de stockage des événements liés aux résultats de l'exécution des tâches et de configurer les notifications sur les résultats de l'exécution des tâches.

- **Programmation**

  La section **Programmation** permet de définir une programmation de lancement de la tâche.

- **Destination**

  Le groupe **Destination** permet d'indiquer le chemin d'accès au dossier de stockage des copies de sauvegarde des données du Serveur d'administration.

- **Paramètres**

  La section **Paramètres** permet de définir le mot de passe de la protection des copies de sauvegarde et, si nécessaire, le nombre de copies de sauvegarde.

  Vous pouvez également créer un cliché instantané du disque logique où se trouve le dossier %ALLUSERSPROFILE% et copier la base de données du Serveur d'administration. Pour ce faire, vous devez activer l'option **Utiliser la capture du système de fichiers pour la sauvegarde des données**, puis indiquer le nom et le mot de passe du compte autorisé à créer des captures.

- **Sécurité**

  La section **Sécurité** permet d'octroyer aux utilisateurs et aux groupes des autorisations pour effectuer des opérations sur le Serveur d'administration. Si l'option **Hériter des paramètres du &Serveur d'administration** est activée, les paramètres de sécurité de la tâche sont hérités du Serveur d'administration.

  Quand cette option est désactivée, vous pouvez configurez les paramètres de sécurité pour la tâche. Vous pouvez affecter un rôle à un utilisateur ou à un groupe d'utilisateurs ou attribuer des permissions à un utilisateur ou à un groupe d'utilisateurs, tel qu'appliqué à la tâche.

  Par défaut, l'option **Hériter des paramètres du &Serveur d'administration** est activée.

- **Historique des révisions**

  La section **Historique des révisions** permet de suivre les modifications apportées à la tâche. Chaque enregistrement de modification dans une tâche entraîne la création d'une révision.

Utilitaire de copie de sauvegarde et de restauration des données (klbackup)

Vous pouvez exécuter la copie des données du Serveur d'administration pour sauvegarder et restaurer successivement à l'aide de l'utilitaire klbackup qui fait partie du distributif Kaspersky Security Center.

L'utilitaire klbackup peut fonctionner en deux modes :

- Interactif
- Silencieux

Sauvegarde et restauration des données en mode interactif

La restauration des données du Serveur d'administration à partir d'une copie de sauvegarde créée à l'aide de l'utilitaire klbackup en mode interactif peut s'accompagner d'une erreur. Si vous avez installé le correctif 15.1.0.20748-pf2 pour le Serveur d'administration, puis créé une copie de sauvegarde à l'aide de l'utilitaire klbackup avec l'option **Migrer la base de données** désactivée, une exception se produit lors de la restauration de cette copie (pour tous les SGBD, sauf MySQL et MariaDB). Si le correctif 15.1.0.20748-pf2 pour le Serveur d'administration est installé et que vous souhaitez créer une copie de sauvegarde sans migrer vers un autre SGBD, utilisez une tâche de sauvegarde des données ou exécutez l'utilitaire klbackup via la ligne de commande.

Pour créer une copie de sauvegarde des données du Serveur d'administration en mode interactif, procédez comme suit :

1. Exécutez l'utilitaire klbackup situé dans le dossier d'installation de Kaspersky Security Center.

   L'Assistant de sauvegarde et de restauration des données démarre.

2. Dans la première fenêtre de l'Assistant, sélectionnez **Réaliser la sauvegarde des données du Serveur d'administration**.

   Si vous sélectionnez l'option **Exécuter la sauvegarde et la restauration uniquement pour le certificat du Serveur d'administration**, seule une copie de sauvegarde du certificat et de la clé privée du Serveur d'administration sera enregistrée. La sauvegarde du certificat et de la clé privée du Serveur d'administration peut être utile lorsque vous effectuez la migration du Serveur d'administration de Kaspersky Security Center Windows vers le Serveur d'administration de Kaspersky Security Center Linux. De plus, vous pouvez migrer des appareils gérés entre Serveurs d'administration de Kaspersky Security Center Linux et entre Serveurs d'administration de Kaspersky Security Center Windows. Pour plus d'informations, consultez la section Utilisation de l'utilitaire klbackup pour basculer des appareils gérés sous l'administration d'un autre Serveur d'administration.

   Cliquez sur **Suivant**.

3. Dans la fenêtre suivante de l'Assistant, spécifiez les options suivantes :

- **Dossier de destination de la sauvegarde**
- **Migrer la base de données**

  Activez cette option si vous stockez actuellement les données du Serveur d'administration dans une base de données Microsoft SQL Server et que vous devez les migrer vers l'une des bases de données suivantes : MySQL ou MariaDB, PostgreSQL ou Postgres Pro, Azure SQL. Cette option est désactivée par défaut.

  - **Migrer au format MySQL/MariaDB**

    Activez cette option si vous utilisez actuellement SQL Server comme DBMS pour le Serveur d'administration et que vous souhaitez migrer les données de SQL Server vers MySQL ou MariaDB DBMS. Kaspersky Security Center créera une sauvegarde compatible avec MySQL et MariaDB. Après cela, vous pouvez restaurer les données de la sauvegarde dans MySQL ou MariaDB.

  - **Migrer vers Postgres**

    Activez cette option si vous utilisez actuellement SQL Server comme SGBD pour le Serveur d'administration et que vous souhaitez migrer les données de SQL Server vers le SGBD PostgreSQL ou Postgres Pro. Kaspersky Security Center créera une sauvegarde compatible avec PostgreSQL et Postgres Pro. Après cela, vous pouvez restaurer les données de la sauvegarde dans PostgreSQL ou Postgres Pro.

    Cette option est accessible si vous faites une demande auprès du Support technique de Kaspersky et installez le correctif 15.1.0.20748-pf2 pour le Serveur d'administration ou passez à la version 15.1.0.22239 de Kaspersky Security Center Windows.

  - **Migrer au format Azure**

    Activez cette option si vous utilisez actuellement SQL Server comme DBMS pour le Serveur d'administration et que vous souhaitez migrer les données de SQL Server vers Azure SQL DBMS. Kaspersky Security Center créera une sauvegarde compatible avec Azure SQL. Après cela, vous pouvez restaurer les données de la sauvegarde dans Azure SQL.

- **Inclure la date et l'heure actuelles dans le nom du dossier de destination de sauvegarde**
- **Mot de passe pour la sauvegarde**

4. Cliquez sur **Suivant** pour exécuter la copie de sauvegarde.

5. Si vous utilisez une base de données dans un Cloud comme Amazon Web Services (AWS) ou Microsoft Azure, remplissez les champs suivants dans la fenêtre **Se connecter au stockage cloud** :

   - Pour AWS :

     - **Nom du compartiment S3**

       Le nom du compartiment S3 que vous avez créé pour la Sauvegarde.

     - **ID de clé d'accès**

       Vous avez reçu l'ID de clé (séquence de caractères alphanumériques) lorsque vous avez créé le compte utilisateur IAM pour travailler avec l'instance de stockage du seau S3.

       Le champ est disponible si vous avez sélectionné la base de données RDS sur un seau S3.

     - **Clé secrète**

       La clé secrète que vous avez reçue avec l'ID de clé d'accès quand vous avez créé le compte utilisateur IAM.

       Les caractères de la clé secrète s'affichent sous la forme d'astérisques. Après que vous avez commencé à saisir la clé secrète, le bouton **Afficher** apparaît. Cliquez sur ce bouton pendant le temps qu'il vous faut pour consulter les caractères saisis.

       Ce champ est accessible si vous avez opté pour l'autorisation à l'aide d'une clé d'accès AWS IAM et non pas d'un rôle IAM.

   - Pour Microsoft Azure :

     - **Nom du compte du stockage Azure**

       Vous avez créé le nom du Compte du stockage Azure pour utiliser Kaspersky Security Center.

     - **Identifiant de l'abonnement Azure**

       Vous avez créé l'abonnement sur le portail Azure.

     - **Mot de passe Azure**

       Vous avez obtenu le mot de passe de l'ID de l'application quand vous avez créé celui-ci.

       Les caractères de la mot de passe s'affichent sous la forme d'astérisques. Après que vous avez commencé à saisir le mot de passe, le bouton **Afficher** apparaît. Maintenez ce bouton enfoncé pour voir les caractères saisis.

     - **ID de l'application Azure**

Vous avez créé cet identifiant de l'application sur le portail Azure.

Vous pouvez fournir un identifiant de l'application Azure pour le sondage et d'autres fins. Si vous souhaitez sonder un autre segment Azure, il faut d'abord supprimer la connexion Azure existante.

- **Nom du serveur SQL Azure**

  Le nom et le groupe de ressources sont disponibles dans les propriétés du Serveur Azure SQL

- **Groupe de ressources du serveur SQL Azure**

  Le nom et le groupe de ressources sont disponibles dans les propriétés du Serveur Azure SQL

- **Clé d'accès au stockage Azure**

  Disponible dans les propriétés de votre compte de stockage, dans la sections Clés d'accès. Vous pouvez utiliser n'importe quelle clé (clé1 ou clé2).

Pour restaurer les données du Serveur d'administration en mode interactif, procédez comme suit :

1. Exécutez l'utilitaire klbackup situé dans le dossier d'installation de Kaspersky Security Center. Lancez l'utilitaire sous le même compte que vous avez utilisé pour installer le Serveur d'administration. Nous vous recommandons d'exécuter l'utilitaire sur un Serveur d'administration nouvellement installé.

   L'Assistant de sauvegarde et de restauration des données démarre.

2. Dans la première fenêtre de l'assistant, sélectionnez l'option **Restaurer les données du Serveur d'administration**, puis cliquez sur **Suivant**.

   Si vous sélectionnez l'option **Exécuter la sauvegarde et la restauration uniquement pour le certificat du Serveur d'administration**, seuls le certificat et la clé privée du Serveur d'administration seront récupérés.

   Lorsque vous lancez l'utilitaire klbackup sur l'entrée inactive du cluster de basculement, vous serez invité à sélectionner l'une des options suivantes : définir le certificat du Serveur d'administration ou récupérer automatiquement les données du Serveur d'administration.

3. Dans la fenêtre **Paramètres de restauration** de l'Assistant :

   - Indiquez le dossier qui contient une copie de sauvegarde du Serveur d'administration.

     Si vous travaillez dans un cloud comme AWS ou Azure, définissez l'adresse du stockage. Vous devez aussi vous assurer que le fichier est intitulé backup.zip.

   - Indiquez le mot de passe saisi lors de la sauvegarde des données.

     Lors de la restauration des données, le même mot de passe que celui utilisé pour la sauvegarde doit être indiqué. Si le chemin d'accès au dossier partagé a changé après la sauvegarde, vous devez vérifier le fonctionnement des tâches qui utilisent les données restaurées (restauration, installation à distance) une fois que les données auront été restaurées. Le cas échéant, les paramètres de ces tâches doivent être modifiés. Lors de la restauration des données au départ du fichier de sauvegarde, personne ne peut utiliser le dossier partagé du Serveur d'administration. Le compte utilisateur sous lequel l'utilitaire klbackup est lancé doit avoir un accès complet au dossier partagé.

4. Cliquez sur le bouton **Suivant** pour restaurer les données.

Sauvegarde et restauration des données en mode silencieux

Pour créer une copie de sauvegarde des données ou pour restaurer les données du Serveur d'administration en mode silencieux,

Dans la ligne de commande de l'appareil où le Serveur d'administration est installé, lancez l'utilitaire klbackup avec l'ensemble de clés nécessaire.

Les indicateurs de l'Agent d'administration ne sont pas restaurés lorsque vous utilisez l'utilitaire klbackup. Vous devez configurer les indicateurs de l'Agent d'administration manuellement.

L'instance du Serveur d'administration sur lequel la restauration a lieu doit utiliser un SGBD du même type. La version du Serveur d'administration peut être la même (avec un correctif semblable ou plus récent) ou plus récente.

Syntaxe de l'utilitaire :

```
klbackup -path <backup path> [-linux_path < chemin de sauvegarde du serveur SQL >][-
node_cert < chemin du certificat >] [-logfile < fichier journal >] [-use_ts]|[-restore] [-
password < mot de passe >] [-cert_only] [-online] [-migrate postgres]
```

Si le mot de passe n'est pas saisi dans la ligne de commande de l'utilitaire klbackup, l'utilitaire demandera son entrée interactivement.

Description des paramètres :

- `-path <chemin de la sauvegarde>` : enregistre les informations dans le dossier de sauvegarde indiqué ou utilise les données du dossier de sauvegarde pour la restauration (paramètre obligatoire).

  Le compte du serveur de base de données et l'utilitaire klbackup doivent disposer des autorisations nécessaires pour modifier les données dans le dossier de sauvegarde.

- `-linux_path <chemin de sauvegarde du serveur SQL>` : chemin d'accès local au dossier avec les données de sauvegarde pour le serveur SQL sous Linux.

  Le compte du serveur de base de données et l'utilitaire klbackup doivent disposer des autorisations nécessaires pour modifier les données dans le dossier de sauvegarde du serveur SQL.

- `-node_cert <chemin du certificat>` : fichier de certificat de serveur servant à configurer le nœud de cluster de basculement inactif après la récupération. S'il n'est pas défini, il est automatiquement récupéré sur le Serveur.

  Quand vous exécutez l'utilitaire klbackup sur le nœud inactif du cluster de basculement, utilisez cette clé pour indiquer le chemin d'accès au certificat du Serveur.

- `-logfile <fichier journal>` : enregistre un rapport sur la sauvegarde et la restauration des données du serveur d'administration.

- `-use_ts` : lors de l'enregistrement des données, copiez les informations dans le dossier de sauvegarde, dans le sous-dossier avec un nom au format `klbackup AAAA-MM-JJ # HH-MM-SS`, qui inclut la date actuelle et l'heure de l'opération en UTC. Si aucune clé n'est indiquée, les données seront enregistrées à la racine du dossier de sauvegarde.

  Si vous essayez de sauvegarder des données dans le dossier dans lequel il existe déjà une copie de sauvegarde, un message d'erreur apparaît. Aucune mise à jour des données ne se produit.

  L'utilisation de la clé `-use_ts` permet de gérer les archives de données du Serveur d'administration. Par exemple, si le dossier `C:\KLBackups` a été spécifié en utilisant la clé `-path`, alors les données sur l'état du Serveur d'administration datant du 19 juin 2022, à 11 heures 30 minutes et 18 secondes, seront enregistrées dans le dossier `klbackup 2022/6/19 # 11-30-18`.

- `-restore` : restaurer les données du Serveur d'administration. La restauration des données s'opère en fonction des informations contenues dans le dossier de sauvegarde. Si aucune clé n'est disponible, la copie de sauvegarde des données s'opère dans le dossier de sauvegarde.

- `-password <mot de passe>` : mot de passe de protection des données sensibles.

  Un mot de passe oublié ne peut pas être récupéré. Il n'existe aucune exigence de mot de passe. La longueur du mot de passe est illimitée et l'absence de mot de passe est également possible.

  Lors de la restauration des données, le même mot de passe que celui utilisé pour la sauvegarde doit être indiqué. Si le chemin d'accès au dossier partagé a changé après la sauvegarde, vous devez vérifier le fonctionnement des tâches qui utilisent les données restaurées (restauration, installation à distance) une fois que les données auront été restaurées. Le cas échéant, les paramètres de ces tâches doivent être modifiés. Lors de la restauration des données au départ du fichier de sauvegarde, personne ne peut utiliser le dossier partagé du Serveur d'administration. Le compte utilisateur sous lequel l'utilitaire klbackup est lancé doit avoir un accès complet au dossier partagé. Nous vous recommandons d'exécuter l'utilitaire sur un Serveur d'administration nouvellement installé.

- `-cert_only` : enregistrez ou récupérez uniquement le certificat et la clé privée du Serveur d'administration.

  Cet indicateur peut être utile dans le cadre de la migration du Serveur d'administration de Kaspersky Security Center Windows vers le Serveur d'administration de Kaspersky Security Center Linux. De plus, vous pouvez migrer des appareils gérés entre Serveurs d'administration de Kaspersky Security Center Linux et entre Serveurs d'administration de Kaspersky Security Center Windows.

- `-online` : sauvegardez les données du Serveur d'administration en créant un instantané de volume afin de réduire la durée hors ligne du Serveur d'administration. Lorsque vous utilisez l'utilitaire pour récupérer des données, cette option est ignorée. N'utilisez pas cet indicateur lors de la création d'une sauvegarde en vue de la migration vers un autre SGBD.

- `-` archive 0 : conserver les données du serveur sous forme de fichiers bruts. Par défaut (`-archive 1`), les données du serveur sont stockées dans un fichier archive.

- `-migrate mysql` : créer une sauvegarde des données du Serveur d'administration stockées dans la base de données du serveur SQL compatible avec MySQL (y compris MariaDB). Vous pouvez restaurer les données de la sauvegarde dans MySQL.

- `-migrate postgres` : créer une sauvegarde des données du Serveur d'administration stockées dans la base de données du serveur SQL compatible avec PostgreSQL et Postgres Pro. Vous pouvez restaurer les données à partir de la sauvegarde dans PostgreSQL ou Postgres Pro. Utilisez cet indicateur lorsque vous effectuez la migration vers Kaspersky Security Center Linux à l'aide de la sauvegarde des données du Serveur d'administration.

  Cette option est accessible si vous faites une demande auprès du Support technique de Kaspersky et installez le correctif 15.1.0.20748-pf2 pour le Serveur d'administration ou passez à la version 15.1.0.22239 de Kaspersky Security Center Windows.

Utilisation de l'utilitaire klbackup pour basculer des appareils gérés sous l'administration d'un autre Serveur d'administration

L'utilitaire klbackup permet de basculer les appareils gérés sous l'administration d'un autre Serveur d'administration. Vous pouvez modifier le Serveur d'administration de Kaspersky Security Center Windows en Serveur d'administration de Kaspersky Security Center Linux à l'aide de l'utilitaire klbackup au moment de la migration. De plus, vous pouvez migrer des appareils gérés entre Serveurs d'administration de Kaspersky Security Center Linux et entre Serveurs d'administration de Kaspersky Security Center Windows.

Pour faire passer les appareils gérés sous l'administration d'un autre Serveur d'administration à l'aide de l'utilitaire klbackup :

1. Sur l'ancien appareil, créez une copie de sauvegarde du certificat du Serveur d'administration et de la clé privée.

   Il est possible de créer une copie de sauvegarde de l'une des manières suivantes :

   - À l'aide de l'interface de l'utilitaire klbackup (uniquement pour le Serveur d'administration de Kaspersky Security Center Windows)

     Lancez l'utilitaire klbackup situé dans le dossier d'installation de Kaspersky Security Center, puis créez une sauvegarde à l'aide de l'option **Exécuter la sauvegarde et la restauration uniquement pour le certificat du Serveur d'administration**.

   - En utilisant l'invite de commande (pour les Serveurs d'administration de Kaspersky Security Center Windows et de Kaspersky Security Center Linux à partir de la version 15.1)

     Exécutez l'utilitaire klbackup avec la clé `-cert_only` via la ligne de commande pour créer une copie de sauvegarde du certificat du Serveur d'administration et de la clé privée :

     ```
     klbackup -path <chemin vers la copie de sauvegarde du certificat du Serveur d'administration> -cert_only
     ```

2. Sur l'ancien appareil, déconnectez le Serveur d'administration du réseau.

3. Attribuez la même adresse à l'appareil doté d'un autre Serveur d'administration.

   Le nouveau Serveur d'administration peut recevoir le nom NetBIOS, le FQDN et l'adresse IP statique. Cela dépend de l'adresse du Serveur d'administration qui a été définie dans le paquet d'installation de l'Agent d'administration lors du déploiement des Agents d'administration. Vous pouvez également utiliser l'adresse de connexion qui détermine le Serveur d'administration auquel l'Agent d'administration se connecte (vous pouvez obtenir cette adresse sur les appareils administrés à l'aide de l'utilitaire klnagchk).

4. Sur l'appareil doté d'un autre Serveur d'administration, restaurez le certificat du Serveur d'administration et la clé privée à partir de la copie de sauvegarde.

   Il est possible de restaurer une copie de sauvegarde de l'une des manières suivantes :

   - À l'aide de l'interface de l'utilitaire klbackup (uniquement pour le Serveur d'administration de Kaspersky Security Center Windows)

     Lancez l'utilitaire klbackup, puis restaurez la sauvegarde à l'aide de l'option **Exécuter la sauvegarde et la restauration uniquement pour le certificat du Serveur d'administration**.

   - En utilisant l'invite de commande (pour les Serveurs d'administration de Kaspersky Security Center Windows et de Kaspersky Security Center Linux à partir de la version 15.1)

     Exécutez l'utilitaire klbackup avec la clé `-cert_only` via la ligne de commande pour restaurer une copie de sauvegarde du certificat du Serveur d'administration et de la clé privée :

     ```
     klbackup -path <chemin vers la copie de sauvegarde du certificat du Serveur d'administration> -restore -cert_only
     ```

Les appareils gérés sont placés sous l'administration d'un autre Serveur d'administration. Vous pouvez accéder à ce Serveur d'administration et vous assurer que les appareils administrés sont visibles sur le réseau et que l'Agent d'administration est installé et exécuté sur eux (la valeur *Oui* dans les colonnes **Visible**, **L'Agent d'administration est installé** et **L'Agent d'administration est en cours d'exécution**).

Sauvegarde et restauration des données du Serveur d'administration avec MySQL ou MariaDB

Vous pouvez utiliser une sauvegarde des données pour migrer les données du Serveur d'administration de Kaspersky Security Center Windows sous l'administration de Kaspersky Security Center Linux. La migration à l'aide de la sauvegarde des données du Serveur d'administration est prise en charge uniquement dans le cas d'une migration vers Kaspersky Security Center Linux 15.2 ou version ultérieure à partir de toute version prise en charge de Kaspersky Security Center Windows.

Si vous utilisez MySQL ou MariaDB comme SGBD pour Kaspersky Security Center Windows et pour Kaspersky Security Center Linux, le paramètre `lower_case_table_names` doit correspondre pour le SGBD actuel et le nouveau. Sinon, les données du Serveur d'administration ne seront pas migrées correctement.

Avant de sauvegarder les données du Serveur d'administration sur Kaspersky Security Center Windows, il faut vérifier la valeur du paramètre `lower_case_table_names`. Si vous ne définissez pas ce paramètre lors de l'installation antérieure du SGBD, la valeur par défaut du paramètre est utilisée. La valeur par défaut du paramètre `lower_case_table_names` pour Windows est `1`.

Lors de l'installation de MySQL ou de MariaDB pour Kaspersky Security Center Linux, définissez le paramètre `lower_case_table_names` sur la même valeur que celle indiquée pour ce paramètre sous Windows, en utilisant les instructions fournies sur le site Internet de MySQL. Si vous ne spécifiez pas ce paramètre, la valeur par défaut du paramètre est utilisée. Pour les systèmes d'exploitation Linux, la valeur par défaut du paramètre `lower_case_table_names` est différente de la valeur par défaut pour Windows.

Si vous souhaitez installer MySQL 8.0, la définition du paramètre `lower_case_table_names` conformément à cette instruction peut ne pas fonctionner. Dans ce cas, vous devez d'abord installer MySQL 5.7, spécifier le paramètre `lower_case_table_names` à l'aide de l'instruction, puis mettre à jour MySQL 5.7 vers MySQL 8.0. Si le paramètre `lower_case_table_names` ne correspond pas pour le SGBD actuel et le nouveau, les données du Serveur d'administration ne sont pas restaurées correctement.

Optimiation de la sauvegarde et de la restauration des données du Serveur d'administration

Pour optimiser la sauvegarde et la restauration des données du Serveur d'administration afin de réduire les temps d'arrêt du Serveur d'administration, effectuez l'une des opérations suivantes :

- Activez l'option **Utiliser la capture du système de fichiers lors de l'exécution de la copie de sauvegarde des données**.

  Consultez l'article suivant pour plus de détails : Utilisation d'une capture du système de fichiers pour réduire la durée de la sauvegarde .

- Configurez les indicateurs suivants :

  Exécutez l'invite de commande Windows en utilisant les droits d'administrateur, puis remplacez votre répertoire actuel par celui contenant l'utilitaire klscflag. L'utilitaire klsclag se trouve dans le dossier dans lequel le Serveur d'administration est installé. Chemin d'installation par défaut est <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

  - `KLSRV_BKP_FILES` : divise le fichier de base de données en plusieurs fichiers plus petits, de 2 à 32. Cette opération peut accélérer la sauvegarde et la restauration si les performances du SGBD sont limitées par le processeur.

    Exemple :

    ```
    klscflag -fset -pv klserver -n KLSRV_BKP_FILES -t d -v 2
    ```

  - `KLSRV_BKP_BACKUP_EXTRA_PARS` : spécifie les paramètres `COMPRESSION` et `MAXTRANSFERSIZE`. Cette opération peut accélérer la sauvegarde si les performances du SGBD sont limitées par l'entrée/sortie de fichiers.

    Exemple :

    ```
    klscflag -fset -pv klserver -n KLSRV_BKP_BACKUP_EXTRA_PARS -t s -v "COMPRESSION,
    MAXTRANSFERSIZE = 4194304"
    ```

  - `KLSRV_BKP_RESTORE_EXTRA_PARS` : spécifie le paramètre `MAXTRANSFERSIZE`. Cette opération peut accélérer la restauration si les performances du SGBD sont limitées par l'entrée/sortie de fichiers.

    Exemple :

    ```
    klscflag -fset -pv klserver -n KLSRV_BKP_RESTORE_EXTRA_PARS -t s -v "MAXTRANSFERSIZE
    = 4194304"
    ```

  - `KLSRV_BKP_ONLINE_DB_BACKUP` : supprime les temps d'arrêt du Serveur d'administration pendant la sauvegarde. Disponible uniquement pour les SGBD suivants :

    - PostgreSQL, Postgres Pro.
    - SQL Server avec le modèle de récupération complet. Pour plus d'informations, consultez la documentation SQL Server. Lorsque vous activez l'indicateur `KLSRV_BKP_ONLINE_DB_BACKUP`, le SGBD de SQL Server passe automatiquement au modèle de récupération complet.

    Exemple :

    ```
    klscflag.exe -fset -pv klserver -n KLSRV_BKP_ONLINE_DB_BACKUP -t d -v 1
    ```

Déplacement du Serveur d'administration sur un autre appareil

Si vous devez utiliser le Serveur d'administration sur un nouvel appareil, vous pouvez le déplacer de l'une des manières suivantes :

- Déplacez le Serveur d'administration et le serveur de base de données vers un nouvel appareil (le serveur de base de données peut être installé sur le nouvel appareil avec le Serveur d'administration ou sur un autre appareil).
- Conservez le serveur de base de données sur l'appareil précédent et déplacez uniquement le Serveur d'administration sur un nouvel appareil.

Pour déplacer le Serveur d'administration vers un nouvel appareil, procédez comme suit :

1. Sur l'appareil précédent, créez une sauvegarde des données du Serveur d'administration.

   Pour ce faire, vous pouvez exécuter la tâche de sauvegarde des données via la Console d'administration ou exécuter l'utilitaire klbackup.

   > Si vous utilisez actuellement SQL Server comme SGBD pour le Serveur d'administration, vous pouvez migrer les données de SQL Server vers le SGBD MySQL ou MariaDB. Pour ce faire, exécutez l' utilitaire klbackup en mode interactif pour créer une sauvegarde des données. Activez l'option **Migrer au format MySQL/MariaDB** dans la fenêtre **Paramètres de sauvegarde** de l'Assistant de sauvegarde et de restauration des données. Kaspersky Security Center créera une sauvegarde compatible avec MySQL et MariaDB. Après cela, vous pouvez restaurer les données de la sauvegarde dans MySQL ou MariaDB.

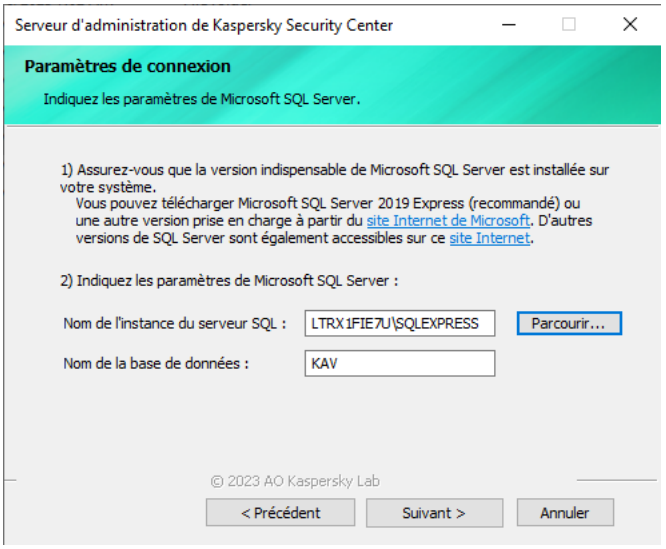
   > Vous pouvez également activer l'option **Migrer au format Azure** si vous souhaitez migrer les données depuis le SGBD SQL Server vers le SGBD SQL Azure.

2. Sur l'ancien appareil, déconnectez le Serveur d'administration du réseau.
3. Sélectionnez un nouvel appareil sur lequel installer le Serveur d'administration. Assurez-vous que le matériel et les logiciels de l'appareil sélectionné répondent à la configuration requise pour le Serveur d'administration, la Console d'administration et l'Agent d'administration. Vérifiez également que les ports utilisés sur le Serveur d'administration sont disponibles.
4. Attribuez la même adresse au nouvel appareil.

   Le nouveau Serveur d'administration peut recevoir le nom NetBIOS, le FQDN et l'adresse IP statique. Cela dépend de l'adresse du Serveur d'administration qui a été définie dans le paquet d'installation de l'Agent d'administration lors du déploiement des Agents d'administration. Vous pouvez également utiliser l'adresse de connexion qui détermine le Serveur d'administration auquel l'Agent d'administration se connecte (vous pouvez obtenir cette adresse sur les appareils administrés à l'aide de l'utilitaire klnagchk).
5. Sur le nouvel appareil, installez le système d'administration de base de données (SGBD) que le Serveur d'administration utilisera.

   La base de données peut être installée sur le nouvel appareil avec le Serveur d'administration ou sur un autre appareil. Assurez-vous que cet appareil répond aux exigences matérielles et logicielles. Lorsque vous sélectionnez un SGBD, tenez compte du nombre d'appareils couverts par le Serveur d'administration.
6. Lancez l'installation du Serveur d'administration sur le nouvel appareil.

7. Lors de l'installation du Serveur d'administration, configurez les paramètres de connexion au serveur de base de données.



Exemple de la fenêtre Paramètres de connexion pour Microsoft SQL Server

Selon l'emplacement du serveur de base de données, exécutez l'une des actions suivantes :

- Conserver le serveur de base de données sur l'appareil précédent

  1. Cliquez sur le bouton **Parcourir** en regard du champ **Nom de l'instance du serveur SQL**, puis sélectionnez le nom de l'appareil précédent dans la liste qui s'affiche.

     Notez que l'appareil précédent doit être disponible pour la connexion avec le nouveau Serveur d'administration.

  2. Saisissez le nom de la base de données précédente dans le champ **Nom de la base de données** de données.

- Déplacer le serveur de base de données vers un autre appareil

  1. Cliquez sur le bouton **Parcourir** en regard du champ **Nom de l'instance du serveur SQL**, puis sélectionnez le nom de l'appareil dans la liste qui s'affiche.

  2. Saisissez le nouveau nom de la base de données dans le champ **Nom de la base de données** de la base de données.

     Notez que le nom de la nouvelle base de données doit correspondre au nom de la base de données de l'appareil précédent. Les noms des bases de données doivent être identiques pour que vous puissiez utiliser la sauvegarde du Serveur d'administration. Le nom par défaut de la base de données est *KAV*.

8. Une fois l'installation terminée, restaurez les données du Serveur d'administration sur le nouvel appareil à l'aide de l'utilitaire klbackup.

Si vous utilisez SQL Server comme SGBD sur l'ancien et le nouvel appareil, notez que la version de SQL Server installée sur le nouvel appareil doit être identique ou ultérieure à la version de SQL Server installée sur l'appareil précédent. Sinon, vous ne pouvez pas récupérer les données du Serveur d'administration sur le nouvel appareil.

9. Ouvrez la Console d'administration et connectez-vous au Serveur d'administration.
10. Vérifiez que tous les appareils administrés sont connectés au Serveur d'administration.
11. Désinstallez le Serveur d'administration et le serveur de base de données de l'appareil précédent.

Vous pouvez également utiliser Kaspersky Security Center Web Console pour déplacer le Serveur d'administration et un serveur de base de données vers un autre appareil.

Évitement des conflits entre plusieurs Serveurs d'administration

Si le réseau compte plus d'un Serveur d'administration, ils peuvent voir les mêmes appareils clients. Cela peut entraîner, par exemple, l'installation par le Serveur d'administration d'une application déjà installée par un autre Serveur d'administration, et d'autres conflits. Pour empêcher l'installation d'une application sur un appareil administré par un autre Serveur d'administration, vous devez activer l'option **Installer uniquement sur les appareils administrés via &ce Serveur d'administration** dans les propriétés de la tâche *Installation à distance d'une application*.

Si vous activez l'option **Installer uniquement sur les appareils administrés via &ce Serveur d'administration**, puis que vous exécutez la tâche *Installation à distance d'une application*, une vérification est effectuée afin de déterminer si les appareils sont administrés par un autre Serveur d'administration. Pour les appareils administrés par un autre Serveur d'administration, la valeur de l'attribut **Administré par un autre Serveur d'administration** est définie sur `true`. La tâche *Installation à distance d'une application* ne sera pas appliquée à ces appareils.

Les valeurs de l'attribut **Administré par un autre Serveur d'administration** s'affichent dans la colonne **Administré par un autre Serveur d'administration** dans la liste des appareils administrés et la liste des appareils non définis.

Vous pouvez également utiliser la propriété **Administré par un autre Serveur d'administration** en tant que critère aux fins suivantes :

- Recherche d'appareils
- Sélections d'appareils
- Règles de déplacement des appareils
- Règles d'attribution automatique de tags

Pour réinitialiser l'attribut Administré par un autre Serveur d'administration :

1. Dans le menu principal de Kaspersky Security Center Web Console, accédez à **Découverte et déploiement → Appareils non définis**.
2. Sélectionnez l'appareil requis, puis cliquez sur le bouton **Supprimer l'attribut Administré par un autre Serveur d'administration**.

L'attribut **Administré par un autre Serveur d'administration** est réinitialisé.

Administration des groupes d'administration

Cette section contient les informations sur le travail avec les groupes d'administration.

Avec les groupes d'administration, vous pouvez effectuer les actions suivantes :

- Ajouter au groupe d'administration le nombre quelconque des groupes imbriqués de tous les niveaux hiérarchique.
- Ajouter au groupe d'administration des appareils.
- Modifier la hiérarchie des groupes d'administration en déplaçant des appareils individuels ou des groupes entiers dans d'autres groupes.
- Supprimer d'un groupe d'administration les sous-groupes et les appareils.
- Ajouter aux groupes d'administration des Serveurs d'administration virtuels et secondaires.
- Déplacer les appareils des groupes d'administration d'un Serveur d'administration vers les groupes d'administration d'un autre Serveur.
- Définir les applications de Kaspersky qui seront installées automatiquement sur les appareils ajoutés au groupe.

Vous pouvez exécuter ces actions uniquement si vous possédez la permission de **Modifier** dans la zone **Gestion des groupes d'administration** que vous souhaitez gérer (ou pour le Serveur d'administration de ces groupes).

Création des groupes d'administration

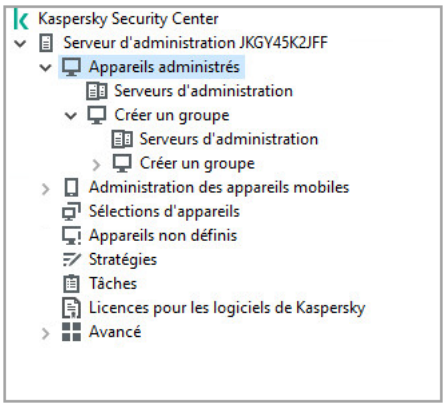
La hiérarchie des groupes d'administration se forme dans la fenêtre principale de l'application Kaspersky Security Center dans le dossier **Appareils administrés**. Les groupes d'administration s'affichent sous forme de dossiers dans l'arborescence de la console (cf. ill. ci-après).

Juste après l'installation de Kaspersky Security Center, le dossier **Appareils administrés** contient uniquement un dossier vide **Serveurs d'administration**.

La présence ou l'absence du dossier **Serveurs d'administration** dans l'arborescence de la console est définie par les paramètres de l'interface utilisateur. Pour afficher ce dossier, il faut accéder au menu **Consulter** → **Configuration de l'interface** et dans la fenêtre **Configuration de l'interface** qui s'ouvre cocher la case **Afficher les Serveurs d'administration secondaires**.

Lors de la création d'une hiérarchie de groupes d'administration, il est possible d'ajouter des appareils et des machines virtuelles au dossier **Appareils administrés**, ainsi que des groupes imbriqués. Le dossier **Serveurs d'administration** permet d'ajouter des Serveurs d'administration secondaires et virtuels.

Comme le dossier **Appareils administrés**, chaque groupe créé initialement contient uniquement un dossier **Serveurs d'administration** vide destiné à fonctionner avec les Serveurs d'administration secondaire et virtuel de ce groupe. Les informations sur les stratégies et les tâches de ce groupe, ainsi que les informations sur les appareils inclus dans ce groupe, sont affichées dans les onglets avec les noms correspondants dans l'espace de travail de ce groupe.



Consultation des hiérarchies des groupes d'administration

Pour créer un groupe d'administration, procédez comme suit :

1. Dans l'arborescence de la console, développez le dossier **Appareils administrés**.
2. Si vous voulez créer un sous-groupe dans un groupe d'administration existant, dans le dossier **Appareils administrés**, sélectionnez un sous-dossier correspondant au groupe qui doit inclure le nouveau groupe d'administration.

   Si vous créez un nouveau groupe d'administration de niveau supérieur de la hiérarchie, vous pouvez ignorer cette étape.
3. Lancez le processus de création du groupe d'administration par l'un des moyens suivants :

   - En utilisant la commande du menu contextuel **Nouveau → Groupe**.
   - En cliquant sur le bouton **Créer un groupe** situé dans l'espace de travail de la fenêtre principale de l'application, sous l'onglet **Appareils**.
4. Dans la fenêtre **Nom de groupe** qui s'ouvre, saisissez le nom du groupe et cliquez sur le bouton **OK**.

L'arborescence de la console affichera un nouveau dossier de groupe d'administration avec le nom saisi.

L'application permet de créer une structure de groupes d'administration sur la base de la structure d'Active Directory ou de la structure du réseau de domaine. Vous pouvez aussi créer une structure de groupes du fichier texte.

Pour créer une structure de groupes d'administration, procédez comme suit :

1. Dans l'arborescence de la console sélectionnez le dossier **Appareils administrés**.
2. Dans le menu contextuel du dossier **Appareils administrés**, sélectionnez **Toutes les tâches → Nouvelle structure de groupe**.

Finalement, l'Assistant de création de la structure des groupes d'administration se lance. Suivez les instructions de l'assistant.

Déplacement des groupes d'administration

Vous pouvez déplacer les groupes d'administration à l'intérieur de la hiérarchie des groupes.

Le groupe d'administration est déplacé avec tous les sous-groupes, les Serveurs d'administration secondaires, les appareils, les stratégies et les tâches de groupe. Tous les paramètres correspondant à sa nouvelle position dans la hiérarchie des groupes d'administration lui seront appliqués.

Le nom de groupe doit être unique entre groupes du même niveau de hiérarchie. Si dans le dossier dans lequel vous déplacez le groupe d'administration, un groupe avec un tel nom existe déjà, le nom du groupe doit être modifié avec le déplacement. Si vous n'avez pas modifié préalablement le nom du groupe déplacé, le suffixe **<next sequence number>** sera automatiquement ajouté à son nom lors du déplacement, par exemple : **(1)**, **(2)**.

Vous ne pouvez pas renommer le groupe **Appareils administrés**, car il s'agit d'un élément incorporé à la Console d'administration.

Pour déplacer le groupe dans un autre dossier de l'arborescence de la console, procédez comme suit :

1. Sélectionnez le groupe déplacé dans l'arborescence de la console.
2. Exécutez une des actions suivantes :
   - Déplacez le groupe à l'aide du menu contextuel :
     1. Sélectionnez l'option **Couper** dans le menu contextuel du groupe.
     2. Sélectionnez l'option **Coller** dans le menu contextuel du groupe d'administration dans lequel vous voulez déplacer le groupe sélectionné.
   - Déplacez le groupe à l'aide du menu principal de l'application :
     a. Dans le menu principal, sélectionnez **Action** → **Couper**.
     b. Sélectionnez dans l'arborescence de la console le groupe d'administration dans lequel vous voulez déplacer le groupe sélectionné.
     c. Sélectionnez l'option du menu principal **Action** → **Coller**.
   - Déplacez le groupe dans un autre groupe dans l'arborescence de la console à l'aide de la souris.

Suppression des groupes d'administration

Vous pouvez supprimer le groupe d'administration s'il ne contient pas des Serveurs d'administration secondaires, des groupes imbriqués et des appareils clients, et si aucune tâche ou stratégie n'a été créée pour lui.

Avant la suppression du groupe d'administration, il faut supprimer de ce groupe les Serveurs d'administration secondaires, les groupes imbriqués et les appareils clients.

Pour supprimer un groupe, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le groupe d'administration.
2. Exécutez une des actions suivantes :
   - Sélectionnez l'option **Supprimer** dans le menu contextuel du groupe.
   - Sélectionnez l'option **Action** → **Supprimer** dans le menu principal de l'application.
   - Cliquez sur la touche **DEL**.

Création automatique de structure des groupes d'administration

Kaspersky Security Center permet de former automatiquement une structure des groupes d'administration à l'aide de l'Assistant de création de la structure des groupes.

L'Assistant crée la structure des groupes d'administration sur la base des données suivantes :

- Structure des domaines et des groupes du réseau Windows
- Structure des groupes Active Directory
- Contenu du fichier texte créé par l'administrateur à la main

Lors de la composition du fichier texte, il faut respecter les règles suivantes :

- Le nom de chaque nouveau groupe doit commencer par une nouvelle ligne séparateur – traduction de la ligne. Les lignes vides sont ignorées.

  Exemple :

  Office 1

  Office 2

  Office 3

  Trois groupes hiérarchiques du premier niveau seront formés dans le groupe de destination.

- Il faut indiquer le nom du groupe placé par une barre oblique (/).

  Exemple :

  Office 1/Subdivision 1/Section 1/Groupe 1

  Quatre sous-groupes placés l'un dans l'autre seront formés dans le groupe de destination.

- Pour former quelques groupes placés du même niveau hiérarchique, il faut indiquer "le chemin complet vers le groupe".

  Exemple :

  Office 1/Subdivision 1/Section 1

  Office 1/Subdivision 2/Section 1

  Office 1/Subdivision 3/Section 1

  Office 1/Subdivision 4/Section 1

  Dans le groupe de destination un groupe du premier niveau hiérarchique "Office 1" sera formé. Il sera composé de quatre groupes placés du même niveau hiérarchique "Subdivision 1", "Subdivision 2", "Subdivision 3", "Subdivision 4". Chaque groupe est composé d'un groupe "Section 1".

La création d'une structure de groupes d'administration à l'aide de l'Assistant n'atteint pas l'intégrité du réseau : de nouveaux groupes sont ajoutés et ne remplacent pas les groupes existants. L'appareil client ne peut pas être inclus une seconde fois dans le groupe d'administration car, lors du déplacement vers le groupe d'administration, l'appareil est retiré du groupe **Appareils non définis**.

Si lors de la création d'une structure des groupes d'administration, un appareil n'a pas été inclus dans le groupe **Appareils non définis** (il était éteint ou déconnecté du réseau), il ne sera pas automatiquement déplacé dans le groupe d'administration. Vous pouvez ajouter les appareils dans les groupes d'administration à la main après la fin du fonctionnement de l'Assistant.

Pour lancer la création automatique d'une structure des groupes d'administration, procédez comme suit :

1. Sélectionnez le dossier **Appareils administrés** dans l'arborescence de la console.
2. Dans le menu contextuel du dossier **Appareils administrés**, sélectionnez **Toutes les tâches → Nouvelle structure de groupe**.

   Finalement, l'Assistant de création de la structure des groupes d'administration se lance. Suivez les instructions de l'assistant.

Installation automatique des applications sur les appareils du groupe d'administration

Vous pouvez définir les paquets d'installation à utiliser pour l'installation automatique à distance des applications Kaspersky sur les appareils clients d'un groupe d'administration.

Afin de configurer l'installation automatique des applications sur les appareils dans le groupe d'administration, procédez comme suit :

1. Sélectionnez le groupe d'administration nécessaire dans l'arborescence de la console.
2. Ouvrez la fenêtre des propriétés de ce groupe d'administration.
3. Dans le volet **Sections**, sélectionnez **Installation automatique** et dans l'espace de travail, sélectionnez les paquets d'installation des applications à installer sur les appareils.
4. Cliquez sur le bouton **OK**.

   Les tâches de groupe sont créées. Ces tâches sont lancées sur les appareils clients juste après avoir été ajoutées au groupe d'administration.

Si plusieurs paquets d'installation d'une seule application sont désignés pour une installation automatique, la tâche d'installation sera uniquement créée pour la version la plus récente de l'application.

Administration des appareils clients

Cette section contient les informations sur le travail avec les appareils clients.

Connexion des appareils clients au Serveur d'administration

La connexion de l'appareil client eu Serveur d'administration se réalise par l'Agent d'administration installé sur l'appareil client.

Lors de la connexion de l'appareil client au Serveur d'administration, les opérations suivantes sont exécutées :

- Synchronisation automatique des données :
  - La synchronisation de la liste des applications installées sur l'appareil client.
  - La synchronisation des stratégies, des paramètres des applications, des tâches et des paramètres des tâches.
- La réception par le Serveur d'administration des informations actuelles sur l'état des applications, sur l'exécution des tâches et sur les statistiques de fonctionnement des applications.
- La transmission sur le Serveur d'administration des informations sur les événements qui doivent être traités.

La synchronisation automatique des données s'effectue périodiquement, en fonction des paramètres de l'Agent d'administration (par exemple, une fois toutes les 15 minutes). Vous pouvez définir manuellement l'intervalle entre les connexions.

Les informations sur un événement sont envoyées sur le Serveur d'administration tout de suite après que l'événement a eu lieu.

Si le Serveur d'administration est un serveur à distance, c'est-à-dire il se trouve en dehors du réseau d'entreprise, les appareils clients se connectent à lui via Internet.

Pour la connexion des appareils au Serveur d'administration via Internet, il est nécessaire d'exécuter les conditions suivantes :

- Le Serveur d'administration à distance doit posséder l'adresse IP externe et, sur cette adresse, le port entrant 13000 doit être ouvert (pour la connexion depuis les agents d'administration). Il est aussi recommandé d'ouvrir le port UDP 13000 (pour la réception des notifications de la désactivation des appareils).
- Des Agents d'administration doivent être installés sur les appareils.
- Lors de l'installation de l'Agent d'administration sur les appareils, l'adresse IP externe du Serveur d'administration à distance doit être indiquée. Si pour l'installation, un paquet d'installation est utilisé, indiquez l'adresse IP externe manuellement dans les propriétés du paquet d'installation, dans la section **Paramètres**.
- Pour administrer les applications et les tâches d'un appareil à l'aide du Serveur d'administration à distance, dans la fenêtre des propriétés correspondant à cet appareil, dans la section **Général**, cochez la case **Maintenir la connexion au Serveur &d'administration**. Après avoir coché la case, il faut attendre la synchronisation de l'appareil distant avec le Serveur d'administration. La connexion permanente avec le Serveur d'administration peut prendre en charge pas plus de 300 appareils clients en même temps.

Pour accélérer l'exécution des tâches reçues depuis le Serveur d'administration à distance, vous pouvez ouvrir sur les appareils le port 15000. Dans ce cas pour lancer une tâche, le Serveur d'administration envoie un paquet spécial à l'Agent d'administration par le port 15000 sans attendre la synchronisation avec l'appareil.

Kaspersky Security Center permet de configurer la connexion de l'appareil client au Serveur d'administration de telle manière pour que la connexion ne se termine pas à la fin d'exécution des opérations. Une connexion permanente est nécessaire dans le cas, où le contrôle d'état des applications est requis, et que le Serveur d'administration ne peut pas initier la connexion avec l'appareil client (par exemple, la connexion est protégée par un pare-feu, il est interdit d'ouvrir des ports sur l'appareil client, l'adresse IP de l'appareil client est inconnue). Une connexion permanente de l'appareil client au Serveur d'administration peut être établie dans la fenêtre des propriétés, dans la section **Général**.

Il est recommandé d'établir une connexion permanente avec les appareils les plus importants. Le nombre total de connexions simultanées prises en charge par le Serveur d'administration est limité à 300.

Lors de la synchronisation manuelle, le mode auxiliaire de connexion est utilisé. Le Serveur d'administration initie la connexion dans ce mode. Avant la connexion sur l'appareil client, l'ouverture du port UDP est requise. Le Serveur d'administration envoie une demande de connexion sur le port UDP de l'appareil client. En réponse, l'analyse du certificat de Serveur d'administration est exécutée. Si le certificat de Serveur d'administration coïncide avec la copie du certificat sur l'appareil client, la connexion est exécutée.

Le lancement manuel du processus de synchronisation est aussi utilisé pour recevoir les informations actuelles sur l'état des applications, sur l'exécution des tâches et sur les statistiques de fonctionnement des applications.

Connexion manuelle de l'appareil client au Serveur d'administration. Utilitaire klmover

S'il vous faut connecter l'appareil client au Serveur d'administration à la main, vous pouvez utiliser l'utilitaire klmover sur l'appareil client.

Lors de l'installation de l'Agent d'administration sur l'appareil client, l'utilitaire est automatiquement copié dans le dossier d'installation de l'Agent d'administration.

Pour connecter l'appareil client au Serveur d'administration à la main à l'aide de l'utilitaire klmover,

Lancez l'utilitaire klmover sur l'appareil depuis la ligne de commande.

Lors du lancement depuis la ligne de commande, l'utilitaire klmover exécute les actions suivantes selon les clés utilisées :

- Ceci connecte l'Agent d'administration au Serveur d'administration, en utilisant les paramètres indiqués.
- Ceci enregistre les résultats de l'opération dans le fichier journal des événements, ou les afficher à l'écran.

Vous ne pouvez pas utiliser l'utilitaire klmover pour les appareils clients connectés au Serveur d'administration via des passerelles de connexion. Pour de tels appareils, vous devez soit reconfigurer l'Agent d'administration, soit réinstaller l'Agent d'administration et indiquer la passerelle de connexion.

Syntaxe de l'utilitaire :

```
klmover [-logfile <nom du fichier>] [-address <adresse du serveur>] [-pn <numéro de port>] [-ps <numéro de port SSL>] [-nossl] [-cert <chemin vers le fichier de certificat>] [-silent] [-dupfix] [-virtserv] [-cloningmode]
```

Les droits d'administrateur sont requis pour exécuter l'utilitaire.

Description des paramètres :

- `-logfile <nom du fichier>` : enregistre les résultats de l'exécution dans le fichier journal.

  Par défaut, les informations sont conservées dans le flux de sortie standard (stdout). Si la clé n'est pas utilisée, les résultats et les messages d'erreur sont affichés à l'écran.

- `-address <adresse du serveur>` : adresse du Serveur d'administration pour la connexion.

  L'adresse peut être une adresse IP, un nom NetBIOS ou DNS de l'appareil.

- `-pn <numéro de port>` : numéro de port à utiliser pour une connexion non chiffrée au Serveur d'administration.

  Le numéro de port par défaut est 14000.

- `-ps <numéro de port SSL>` : numéro de port SSL à utiliser pour une connexion chiffrée au Serveur d'administration sous protocole SSL.

  Le numéro de port par défaut est 13000.

- `-nossl` : utilise une connexion non chiffrée au Serveur d'administration.

  Si aucune clé n'est utilisée, la connexion de l'Agent d'administration au Serveur d'administration est établie à l'aide du protocole sécurisé SSL.

- `-cert <chemin vers le fichier de certificat>` : utilise le fichier de certificat spécifié pour l'authentification, afin d'accéder au Serveur d'administration.

  Si aucune clé n'est utilisée, l'Agent d'administration recevra le certificat lors de la première connexion au Serveur d'administration.

- `-silent` : exécute l'utilitaire en mode silencieux.

  Cette clé est utile, par exemple, pour exécuter l'outil à partir du scénario de connexion de l'utilisateur.

- `-dupfix` : clé utilisée en cas d'installation de l'Agent d'administration par une méthode différente de la normale (avec le paquet de distribution), par exemple, par restauration depuis une image disque.

- `-virtserv` : nom du Serveur d'administration virtuel

- `-cloningmode` : mode de clonage du disque de l'Agent d'administration

  Utilisez l'un des paramètres suivants pour configurer le mode de clonage du disque :

  - `-cloningmode` : demande l'état du mode de clonage du disque.
  - `-cloningmode 1` : active le mode de clonage du disque.
  - `-cloningmode 0` : désactive le mode de clonage du disque.

- `-nauninstpwd <mot de passe>` : la clé est utilisée pour définir le mot de passe de désinstallation de l'Agent d'administration.

  La clé n'est pas obligatoire.

Par exemple, pour connecter l'Agent d'administration au Serveur d'administration, exécutez la commande suivante :

```
klmover -address kscserver.mycompany.com -logfile klmover.log
```

Connexion en tunnel de l'appareil client avec le Serveur d'administration

Kaspersky Security Center permet d'établir des connexions TPC en tunnel depuis la Console d'administration via le Serveur d'administration et puis via l'Agent d'administration vers le port défini sur l'appareil administré. Le tunnel est utilisé pour connecter une app cliente qui se trouve sur un appareil doté de la Console d'administration au port TCP sur l'appareil administré si la connexion directe de l'appareil avec la Console d'administration et l'appareil n'est pas possible.

Plus particulièrement, le tunnel est utilisé pour établir une connexion à un poste de travail distant : aussi bien pour la connexion à une session en cours que pour la création d'une nouvelle session à distance.

Le tunnel peut également être utilisé à l'aide du mécanisme des outils externes. Ainsi, l'administrateur peut lancer de la sorte l'utilitaire putty, un client VNC et d'autres outils.

La connexion en tunnel de l'appareil client à distance avec le Serveur d'administration est nécessaire si le port de connexion au Serveur d'administration est inaccessible sur l'appareil. Le port sur l'appareil peut être inaccessible dans les cas suivants :

- L'appareil à distance est connecté au réseau local avec le mécanisme NAT utilisé.
- L'appareil à distance fait partie du réseau local du Serveur d'administration, mais son port est fermé par un pare-feu.

Pour exécuter une connexion en tunnel de l'appareil client avec le Serveur d'administration, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le dossier du groupe dont l'appareil client fait partie.
2. Sous l'onglet **Appareils**, sélectionnez l'appareil.
3. Dans le menu contextuel de l'appareil, sélectionnez l'option **Toutes les tâches → Connexion en tunnel**.
4. Dans la fenêtre **Connexion en tunnel** qui s'ouvre, créez un tunnel.

Connexion à distance au bureau de l'appareil client

L'administrateur peut obtenir l'accès au bureau de l'appareil client à l'aide de l'Agent d'administration installé sur l'appareil.

La connexion à distance à l'appareil client à l'aide de l'Agent d'administration est même possible dans le cas si les ports TCP et UDP de l'appareil client ne sont pas accessibles. Après la connexion à l'appareil, l'administrateur obtient l'accès complet aux informations sur cet appareil et peut administrer les applications installées sur celui-ci.

Cette section décrit comment établir une connexion à un appareil client Windows et à un appareil client macOS via l'Agent d'administration.

Connexion aux appareils clients Windows

La connexion à distance à l'appareil client Windows peut être exécutée de deux manières suivantes :

- A l'aide du module standard de Microsoft Windows "Connexion Bureau à distance".

  La connexion au bureau à distance est exécutée à l'aide de l'utilitaire titulaire de Windows mstsc.exe conformément aux paramètres de fonctionnement de cet utilitaire.

- A l'aide de la technologie Partage du bureau Windows.

Connexion à l'appareil client Windows à l'aide de la connexion Bureau à distance

La connexion à la session en cours sur le poste de travail distant de l'utilisateur s'établit sans notification. Une fois l'administrateur connecté à la session, l'utilisateur de l'appareil sera déconnecté sans notification.

Pour se connecter au bureau de l'appareil client à l'aide du module "Connexion Bureau à distance", procédez comme suit :

1. Dans l'arborescence de la Console d'administration, sélectionnez l'appareil auquel l'accès doit être obtenu.

2. Dans le menu contextuel de l'appareil, sélectionnez l'option, sélectionnez **Toutes les tâches → Se connecter à l'appareil → Nouvelle session RDP**.

   Finalement, l'utilitaire titulaire de Windows mstsc.exe sera lancé pour la connexion au bureau à distance.

3. Suivez les indications dans les fenêtres ouvertes de l'utilitaire.

Lorsque la connexion à l'appareil client est établie, le bureau de l'appareil client est accessible dans la fenêtre Connexion Bureau à distance de Microsoft Windows.

Connexion à l'appareil client Windows à l'aide du Partage du bureau Windows

Lors de la connexion à la séance existante du bureau à distance, l'utilisateur de cette séance sur l'appareil recevra une demande de connexion en provenance de l'administrateur. Les informations sur le processus de l'utilisation à distance de l'appareil et sur les résultats de cette utilisation ne sont pas conservées dans les rapports de Kaspersky Security Center.

L'administrateur peut se connecter à la séance existante sur l'appareil client sans la déconnexion de l'utilisateur travaillant dans cette séance. Dans ce cas, l'administrateur et l'utilisateur de la session sur l'appareil ont un accès collectif au bureau.

L'administrateur peut configurer l'audit des actions sur l'appareil client distant. Lors de l'audit, l'application enregistre les informations relatives aux fichiers que l'administrateur a ouverts et/ou modifiés sur l'appareil client.

Pour se connecter au bureau d'un appareil client à l'aide du Partage du bureau Windows, les conditions suivantes doivent être remplies :

- Microsoft Windows Vista ou une version plus récente est installée sur le poste de travail de l'administrateur. Le type du système d'exploitation de l'appareil hébergeant le Serveur d'administration ne représente pas une restriction pour la connexion à l'aide de Partage du bureau Windows.

  Pour vérifier si la fonctionnalité de partage de bureau Windows est incluse dans votre édition Windows, assurez-vous qu'il existe une clé CLSID\{32BE5ED2-5C86-480F-A914-0FF8885A1B3F} dans le registre Windows.

- Microsoft Windows Vista ou une version plus récente est installée sur l'appareil client.

- Kaspersky Security Center utilise la licence sur la Gestion des vulnérabilités et des correctifs.

Pour se connecter au bureau de l'appareil client à l'aide de la technologie Partage du bureau Windows, procédez comme suit :

1. Dans l'arborescence de la Console d'administration, sélectionnez l'appareil auquel l'accès doit être obtenu.

2. Dans le menu contextuel de l'appareil, sélectionnez l'option **Toutes les tâches → Se connecter à l'appareil → Partage du bureau Windows**.

3. Dans la fenêtre ouverte **Sélection de la session du bureau**, sélectionnez une session sur l'appareil client auquel vous devez vous connecter.

   Dans le cas d'une connexion réussie à l'appareil client, le bureau de cet appareil est accessible dans la fenêtre **Kaspersky Remote Desktop Session Viewer**.

4. Pour commencer à interagir avec l'appareil, dans le menu principal de la fenêtre **Kaspersky Remote Desktop Session Viewer**, sélectionnez **Actions → Mode interactif**.

L'utilitaire **Kaspersky Remote Desktop Session Viewer** requiert une licence commerciale.

Connexion aux appareils clients macOS

L'administrateur peut utiliser le système Virtual Network Computing (VNC) pour se connecter aux appareils macOS.

La connexion à un poste de travail distant est établie via un client VNC installé sur l'appareil doté du Serveur d'administration. Le client VNC fait passer le contrôle du clavier et de la souris de l'appareil client à l'administrateur.

Lorsque l'administrateur se connecte au bureau distant, l'utilisateur ne reçoit pas de notifications ni de demandes de connexion de la part de l'administrateur. L'administrateur se connecte à une session existante sur l'appareil client, sans déconnecter l'utilisateur de cette session.

Pour se connecter au bureau d'un appareil client macOS via le client VNC, les conditions suivantes doivent être remplies :

- Le client VNC est installé sur l'appareil du Serveur d'administration.
- La connexion à distance et l'administration à distance sont autorisées sur l'appareil client.
- L'utilisateur a autorisé l'accès de l'administrateur à l'appareil client dans les paramètres de **partage** du système d'exploitation macOS.

Pour se connecter au bureau d'un périphérique client via le système Virtual Network Computing :

1. Dans l'arborescence de la Console d'administration, sélectionnez l'appareil auquel l'accès doit être obtenu.
2. Dans le menu contextuel de l'appareil, sélectionnez l'option **Toutes les tâches → Connexion en tunnel**.
3. Dans la fenêtre **Connexion en tunnel** qui s'ouvre, procédez comme suit :
   a. Dans la section **1. Port de réseau**, indiquez le numéro de port réseau de l'appareil auquel vous devez vous connecter.
      Le numéro du port est de 5900 par défaut.
   b. Dans la section **2. Tunnel**, cliquez sur le bouton **Créer un tunnel**.
   c. Dans la section **3. Attributs réseau**, cliquez sur le bouton **Copier**.
4. Ouvrez le client VNC et collez les attributs réseau copiés dans le champ de texte. Appuyez sur **Entrée**.
5. Dans la fenêtre qui s'ouvre, affichez les détails du certificat. Si vous acceptez d'utiliser le certificat, cliquez sur le bouton **Oui**.
6. Dans la fenêtre **Authentification**, indiquez les informations d'identification de l'appareil client, puis cliquez sur **OK**.

Connexion aux appareils à l'aide du Partage du bureau Windows

Pour vous connecter à un appareil à l'aide de la technologie Partage du bureau Windows, procédez comme suit :

1. Dans l'arborescence de la console, sous l'onglet **Appareils**, sélectionnez le dossier **Appareils administrés**.
   La liste des appareils s'affiche dans l'espace de travail du dossier.
2. Dans le menu contextuel de l'appareil client auquel vous voulez vous connecter, sélectionnez l'option **Se connecter à l'appareil → Partage du bureau Windows**.
   La fenêtre **Sélection de la session du bureau**.
3. Dans la fenêtre **Sélection de la session du bureau**, sélectionnez la session du bureau qui sera utilisée pour se connecter à l'appareil.
4. Cliquez sur le bouton **OK**.

La connexion à l'appareil sera effectuée.

Paramètres du redémarrage de l'appareil client

Au cours de la session, l'installation ou la suppression du Kaspersky Security Center peut nécessiter un redémarrage de l'appareil client. Vous pouvez configurer les paramètres de redémarrage uniquement pour les appareils sous Windows.

Pour configurer le redémarrage de l'appareil client, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le groupe d'administration pour lequel il est nécessaire de configurer le redémarrage.
2. Dans l'espace de travail du groupe, sélectionnez l'onglet **Stratégies**.
3. Dans l'espace de travail, sélectionnez une stratégie de l'Agent d'administration de Kaspersky Security Center dans la liste des stratégies, puis sélectionnez l'option **Propriétés** dans le menu contextuel de la stratégie.
4. Dans la fenêtre des propriétés de la stratégie, sélectionnez la section **Administration du redémarrage**.
5. Sélectionnez l'action à exécuter si le redémarrage de l'appareil est requis :
   - Sélectionnez **Ne pas redémarrer le système d'exploitation** pour bloquer le redémarrage automatique.
   - Sélectionnez **Redémarrer le système d'exploitation automatiquement si nécessaire** pour autoriser un redémarrage automatique.
   - Sélectionnez **Confirmer l'action auprès de l'utilisateur** pour activer la demande de confirmation de redémarrage auprès de l'utilisateur.

   Vous pouvez indiquer la fréquence de la demande de redémarrage, activer le redémarrage forcé et forcer la fermeture des applications dans les sessions verrouillées sur l'appareil grâce aux cases prévues à cet effet et aux paramètres de temps dans les listes.
6. Cliquez sur le bouton **OK** pour enregistrer les modifications et fermer la fenêtre des propriétés de la stratégie.

Après cette étape, le redémarrage du système d'exploitation de l'appareil sera configuré.

Audit des actions sur un appareil client distant

L'application permet d'effectuer l'audit des actions de l'administrateur sur les appareils clients sous Windows distants. Lors de l'audit, l'application enregistre les informations relatives aux fichiers que l'administrateur a ouverts et/ou modifiés sur l'appareil. L'audit des actions de l'administrateur est accessible lorsque les conditions suivantes sont réunies :

- La licence pour le fonctionnement de Gestion des vulnérabilités et des correctifs est en cours d'utilisation.
- L'administrateur est autorisé à lancer l'accès partagé au bureau de l'appareil distant.

Pour activer l'audit des actions sur un appareil client distant, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le groupe d'administration pour lequel il est nécessaire de configurer l'audit des actions de l'administrateur.
2. Dans l'espace de travail du groupe, sélectionnez l'onglet **Stratégies**.
3. Sélectionnez la stratégie de l'Agent d'administration de Kaspersky Security Center, puis sélectionnez l'option **Propriétés** dans le menu contextuel de la stratégie.
4. Sélectionnez la section **Partage du bureau Windows** dans la fenêtre des propriétés de la stratégie.
5. Cochez la case **&Activer l'audit**.
6. Dans les listes **Masques de fichiers à suivre en cas de lecture** et **Masques de fichiers à suivre en cas de modification**, ajoutez des masques de fichiers sur lesquels l'application doit surveiller les actions pendant l'audit.

   Par défaut, l'application suit les actions effectuées sur les fichiers .txt, .rtf, .doc, .xls, .docx, .xlsx, odt, pdf.
7. Cliquez sur le bouton **OK** pour enregistrer les modifications et fermer la fenêtre des propriétés de la stratégie.

L'audit des actions de l'administrateur sur l'appareil distant d'un utilisateur se servant d'un accès partagé au poste de travail sera ainsi configuré.

Les enregistrements des actions de l'administrateur sur l'appareil distant sont conservés :

- Dans le journal des événements de l'appareil distant.
- Dans un fichier .syslog, situé dans le dossier de l'Agent d'administration sur l'appareil distant (par exemple C:\ProgramData\KasperskyLab\adminkit\1103\logs).
- Dans la base des événements du Kaspersky Security Center.

Vérification de la connexion de l'appareil client avec le Serveur d'administration

Kaspersky Security Center permet d'analyser le connexion de l'appareil client avec le Serveur d'administration automatiquement ou à la main.

L'analyse automatique de la connexion s'effectue sur le Serveur d'administration. L'analyse manuelle de la connexion s'effectue sur l'appareil.

Vérification automatique de la connexion de l'appareil client avec le Serveur d'administration

Pour lancer l'analyse automatique de la connexion de l'appareil client avec le Serveur d'administration, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le groupe d'administration dont l'appareil fait partie.
2. Dans l'espace de travail du groupe d'administration, sous l'onglet **Appareils**, sélectionnez l'appareil.
3. Dans le menu contextuel de l'appareil, sélectionnez l'option **&Analyser l'accessibilité de l'appareil**.

Finalement la fenêtre, qui contient l'information sur l'accessibilité de l'appareil, s'ouvre.

Vérification manuelle de la connexion de l'appareil client avec le Serveur d'administration. Utilitaire klnagchk

Vous pouvez vérifier la connexion et recevoir les informations détaillées sur les paramètres de connexion de l'appareil client au Serveur d'administration à l'aide de l'utilitaire klnagchk. L'utilitaire klnagchk se trouve dans le dossier d'installation de l'Agent d'administration.

Lors du lancement depuis la ligne de commande, l'utilitaire klnagchk exécute les actions suivantes selon les clés utilisées :

- Renvoyer à l'écran ou enregistrer dans le fichier journal les valeurs des paramètres de connexion de l'Agent d'administration installé sur l'appareil, utilisés afin de se connecter au Serveur d'administration.
- Enregistrer dans le fichier journal les statistiques de l'Agent d'administration (à partir de son dernier démarrage) et les résultats d'exécution de l'utilitaire, ou afficher les informations sur l'écran.
- Tenter d'établir une connexion entre l'Agent d'administration et le Serveur d'administration.

  Si la connexion n'a pas pu être établie, l'utilitaire envoie un paquet ICMP au poste sur lequel est installé le Serveur d'administration afin de vérifier l'état de l'appareil.

Pour vérifier la connexion de l'appareil client au Serveur d'administration à l'aide de l'utilitaire klnagchk,

Sur l'appareil où est installé l'Agent d'administration, démarrez l'utilitaire klnagchk à partir de la ligne de commande sous un compte d'administrateur local.

Syntaxe de l'utilitaire :

```
klnagchk [-logfile <nom de fichier>] [-sp] [-savecert <chemin vers le fichier du certificat>] [-restart][-sendhb]
```

Description des paramètres :

- `-logfile <nom du fichier>` : enregistrer les valeurs des paramètres de connexion utilisées par l'Agent d'administration pour se connecter au Serveur d'administration, ainsi que les résultats de l'exécution de l'utilitaire dans le fichier journal.

  Par défaut, les informations sont conservées dans le flux de sortie standard (stdout). Si la clé n'est pas utilisée, les paramètres, les résultats et les messages d'erreur sont affichés à l'écran.

- `-sp` : afficher le mot de passe utilisé pour authentifier l'utilisateur sur le serveur proxy.

  Cette clé est utilisée si la connexion au Serveur d'administration est effectuée via un serveur proxy.

- `-savecert <nom du fichier>` : enregistre le certificat pour l'authentification de l'accès au Serveur d'administration dans un fichier spécifié.

- `-restart` : lance l'Agent d'administration après exécution de l'utilitaire.

- `-sendhb` : lance la synchronisation de l'Agent d'administration avec le Serveur d'administration.

Après le lancement, l'utilitaire klnagchk accède aux fichiers de configuration de l'Agent d'administration et affiche les paramètres de connexion. Ces paramètres sont définis lors de l'installation de l'Agent d'administration et dans les paramètres de stratégie de l'Agent d'administration :

- `Current device` : nom de l'appareil client sur le réseau Windows.

- `Network Agent version` : numéro complet de la version d'Agent d'administration (avec correctifs) installée sur l'appareil.

- `Administration Server address` : adresse du Serveur d'administration.

- `Use SSL` : paramètre qui indique si la connexion sécurisée au Serveur d'administration est utilisée.

  Valeurs possibles :

  - 0 : la connexion sécurisée n'est pas utilisée.

  - 1 : la connexion sécurisée est utilisée.

- `Compress traffic` : paramètre qui indique si le trafic entre l'appareil client et le Serveur d'administration est compressé.

- `Numbers of the Administration Server SSL ports` : numéros des ports valides pour la communication avec le Serveur d'administration lors de l'utilisation d'une connexion sécurisée.

- `Numbers of the Administration Server ports` : numéros des ports valides pour la communication avec le Serveur d'administration lors de l'utilisation d'une connexion classique.

- `Use proxy server` : paramètre qui indique si un serveur proxy est utilisé.

  Valeurs possibles :

  - 0 : le serveur proxy n'est pas utilisé.

  - 1 : le serveur proxy est utilisé.

- `Address` : adresse et port du serveur proxy, séparés par deux points. Ce paramètre s'affiche uniquement en cas d'utilisation d'un serveur proxy.

- `User name` : nom d'utilisateur permettant d'accéder au serveur proxy. Ce paramètre s'affiche uniquement en cas d'utilisation d'un serveur proxy.

- `Password` : mot de passe permettant d'accéder au serveur proxy. Ce paramètre s'affiche uniquement en cas d'utilisation d'un serveur proxy. Pour afficher le mot de passe du serveur proxy, vous devez utiliser la clé `sp` dans la commande.

- `Administration Server certificate` : paramètre qui indique si l'appareil client dispose d'un certificat de Serveur d'administration. Par exemple, il peut ne pas exister de certificat si l'Agent d'administration ne s'est jamais correctement connecté au Serveur d'administration.

  Valeurs possibles :

  - `not installed` : l'appareil client ne possède pas de certificat de Serveur d'administration.

  - `available` : l'appareil client dispose d'un certificat de Serveur d'administration.

- `Open UDP port` : paramètre qui indique si l'Agent d'administration utilise le port UDP pour recevoir les requêtes de synchronisation du Serveur d'administration.

  Valeurs possibles :

  - 0 : le port UDP est fermé pour la réception des requêtes de synchronisation du Serveur d'administration.

  - 1 : le port UDP est ouvert pour recevoir les requêtes de synchronisation du Serveur d'administration.

- `Numbers of UDP ports` : numéros des ports UDP qui peuvent être utilisés par l'Agent d'administration.

- `Location name` : emplacement réseau de l'appareil.

- `State of network location` : paramètre qui indique si l'appareil client peut être basculé d'un profil de connexion du Serveur d'administration à un autre.

  Valeurs possibles :

  - `Enabled` : le profil de connexion du Serveur d'administration pour l'appareil client peut être modifié.

  - `Disabled` : le profil de connexion du Serveur d'administration pour l'appareil client ne peut pas être modifié.

- `Profile to use` : profil de connexion pour le Serveur d'administration.

- `Condition` : adresse IP et masque de sous-réseau du réseau auquel l'appareil client est connecté.

- `Synchronization interval (min)` : intervalle standard entre les synchronisations.

- `Connection timeout (in seconds)` : délai d'expiration de la connexion.

- `Send / receive timeout (in seconds)` : délai d'expiration de la connexion pour les opérations de lecture-écriture.

- `Device ID` : identifiant de l'appareil dans le réseau. L'`Device ID` est unique parmi les appareils clients administrés par un Serveur d'administration particulier.

- `Locations of connection gateways` : paramètres de connexion de l'appareil client au Serveur d'administration via la passerelle de connexion.

- `Location of distribution points` : paramètres de connexion de l'appareil client au Serveur d'administration via le point de distribution.

- `Connection with server` : paramètre qui indique si la passerelle de connexion dispose d'une connexion permanente au Serveur d'administration. Le paramètre s'affiche uniquement si l'appareil client agit comme une passerelle de connexion.

  Valeurs possibles :

  - `active` : la passerelle de connexion dispose d'une connexion permanente au Serveur d'administration.

  - `inactive` : la passerelle de connexion ne dispose pas de connexion permanente au Serveur d'administration.

- `Connection with server through connection gateway` : paramètre qui indique si la connexion au Serveur d'administration via une passerelle de connexion est correctement établie. Le paramètre s'affiche uniquement si l'appareil client agit comme une passerelle de connexion.

  Valeurs possibles :

  - `active` : la connexion au Serveur d'administration via une passerelle de connexion est correctement établie.

  - `inactive` : la connexion au Serveur d'administration via une passerelle de connexion n'est pas établie correctement.

De plus, le résultat de l'utilitaire klnagchk peut contenir l'une des lignes suivantes :

- `Administration Server is installed on this device` : l'utilitaire klnagchk est lancé sur l'appareil avec le Serveur d'administration.

- `This device has been assigned a connection gateway but is not yet registered on Administration Server` : l'utilitaire klnagchk est lancé sur l'appareil sur lequel l'Agent d'administration est installé, en mode passerelle de connexion. La passerelle de connexion configurée attend une connexion du Serveur d'administration, mais le Serveur d'administration ne répertorie pas l'appareil parmi les appareils administrés. Vous devez vous assurer que le Serveur d'administration amorce une connexion avec la passerelle de connexion.

- `This device is a connection gateway` : l'utilitaire klnagchk est exécuté sur l'appareil qui agit comme une passerelle de connexion.

- `Acts as a distribution point` : l'utilitaire klnagchk est exécuté sur l'appareil qui agit comme un point de distribution.

L'utilitaire klnagchk vérifie l'état du service de l'Agent d'administration. Si le service est désactivé, l'utilitaire s'arrête. Si le service est en cours d'exécution, l'utilitaire affiche les statistiques de connexion suivantes :

- `Total number of synchronization requests` : nombre de tentatives de connexion de l'appareil client au Serveur d'administration.

- `The number of successful synchronization request` : nombre de tentatives de connexion de l'appareil client au Serveur d'administration réussies.

- `Total number of synchronizations` : nombre de tentatives de synchronisation des paramètres de l'appareil client avec ceux du Serveur d'administration.

- `The number of successful synchronizations` : nombre de tentatives de synchronisation des paramètres de l'appareil client avec le Serveur d'administration réussies.

- `Date/time of the last request for synchronization` : date et heure de la dernière connexion.

Vous devez utiliser les paramètres `Total number of synchronization requests` et `The number of successful synchronization request` lors de l'analyse de la connexion entre le Serveur d'administration et l'Agent d'administration. Les paramètres de l'appareil client ne se synchronisent avec les paramètres du Serveur d'administration que si les paramètres du Serveur d'administration ont été modifiés (par exemple, si de nouvelles tâches ont été ajoutées ou des paramètres d'une stratégie ont été modifiés). Dans le cas contraire, les valeurs des paramètres `Total number of synchronizations` et `The number of successful synchronizations` restent inchangées.

Pour apprendre à résoudre les problèmes de connexion de l'Agent d'administration au Serveur d'administration, consultez la FAQ de Kaspersky Security Center.

À propos de la vérification de la durée de connexion de l'appareil avec le Serveur d'administration

Lors de la désactivation de l'appareil, l'Agent d'administration signale celle-ci au Serveur d'administration. Dans la Console d'administration, cet appareil apparaît comme désactivé. Cependant l'Agent d'administration ne parvient pas toujours à informer le Serveur d'administration. C'est pourquoi le Serveur d'administration analyse à intervalle régulier pour chaque appareil l'attribut **Connexion au Serveur d'administration** (la valeur de l'attribut s'affiche dans la Console d'administration, dans la section **Général** des propriétés de l'appareil) et le compare à la période de synchronisation des paramètres actifs de l'Agent d'administration. Si l'appareil n'a pas établi de communication pendant plus de trois périodes de synchronisation, cet appareil est signalé comme désactivé.

Identification des appareils clients sur le Serveur d'administration

L'identification des appareils clients est réalisée sur la base de leurs noms. Le nom d'un appareil est unique parmi tous les noms d'appareils connectés au Serveur d'administration.

Le nom de l'appareil est transmis au Serveur d'administration, soit lors du sondage du réseau Windows et de la détection d'un nouvel appareil dans ce réseau, soit lors de la première connexion de l'Agent d'administration, installé sur l'appareil, au Serveur d'administration. Par défaut, le nom concorde avec le nom d'appareil dans le réseau Windows (nom NetBIOS). Si un appareil est déjà enregistré avec ce nom sur le Serveur d'administration, alors un numéro d'ordre sera ajouté à la fin du nom du nouvel appareil, par exemple : **<Name>-1**, **<Name>-2**. Sous ce nom, l'appareil sera inclus dans le groupe d'administration.

Déplacement des appareils à un groupe d'administration

Vous pouvez déplacer les appareils d'un groupe d'administration vers un autre uniquement si vous possédez la permission **Modifier** dans la zone **Gestion des groupes d'administration** des groupes d'administration source et cible (ou pour le Serveur d'administration auquel ce groupe appartient).

Pour inclure un ou plusieurs appareils dans un groupe d'administration sélectionné, procédez comme suit :

1. Dans l'arborescence de la console, développez le dossier **Appareils administrés**.
2. Dans le dossier **Appareils administrés**, sélectionnez le sous-dossier correspondant au groupe dans lequel les appareils clients vont être inclus.

   Si vous voulez inclure les appareils dans le groupe **Appareils administrés**, vous pouvez ignorer cette étape.
3. Dans l'espace de travail du groupe d'administration sélectionné, sous l'onglet **Appareils**, lancez le processus d'inclusion des appareils dans le groupe en utilisant l'un des moyens suivants :

   - Ajoutez des appareils au groupe à l'aide du bouton **Déplacer les appareils vers le groupe** dans la zone d'informations de la liste des appareils
   - Dans le menu contextuel de la liste des appareils, sélectionnez l'option **Créer → Appareil**

   L'Assistant de déplacement des appareils est ensuite démarré. Suivez ses instructions et définissez le mode de déplacement des appareils dans le groupe et composez la liste des appareils appartenant au groupe.

   Si vous fournissez la liste des appareils à la main, vous pouvez utiliser l'adresse IP (ou l'intervalle IP), le nom NetBIOS ou le nom DNS en tant que l'adresse de l'appareil. Il est possible de déplacer manuellement dans la liste des appareils uniquement les appareils dont les informations ont été insérées dans la base de données du Serveur d'administration lors de la connexion de l'appareil ou lors de la recherche d'appareils.

   Pour importer la liste des appareils à partir d'un fichier, il faut indiquer le fichier au format TXT avec la liste des adresses des appareils à ajouter. Chaque adresse doit figurer sur une ligne séparée.

Après la fin de l'Assistant, les appareils sélectionnés sont inclus dans le groupe d'administration et s'affichent dans la liste des appareils sous les noms établis pour eux par le Serveur d'administration.

Il est possible de déplacer un appareil vers le groupe d'administration sélectionné en le faisant glisser à l'aide de la souris depuis le dossier **Appareils non définis** dans le dossier de ce groupe d'administration.

Modification du Serveur d'administration pour les appareils clients

Vous pouvez modifier le Serveur d'administration, sous lequel les appareils clients se trouvent, par un autre Serveur à l'aide de la tâche *Modification du Serveur d'administration*.

Pour modifier le Serveur d'administration, sous lequel les appareils clients se trouvent, par un autre Serveur, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le dossier **Tâches**.
2. Dans l'espace de travail de ce dossier, cliquez sur le bouton **Nouvelle tâche**.

   Ceci permet de lancer l'Assistant de création d'une tâche. Parcourez les étapes de l'assistant à l'aide du bouton **Suivant**.
3. À l'étape **Sélection du type de tâche** de l'assistant, sélectionnez le nœud **Serveur d'administration de Kaspersky Security Center**, développez le dossier **Avancé**, puis sélectionnez la tâche du **Modification du Serveur d'administration**.

4. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **OK** pour confirmer que vous acceptez les conditions de modification du Serveur d'administration pour les appareils clients.

5. À l'étape **Paramètres** de l'assistant, sélectionnez le Serveur d'administration que vous souhaitez utiliser pour administrer les appareils sélectionnés.

   - **Passer à un autre &Serveur d'administration principal**

     Pour déplacer les appareils clients vers un autre Serveur d'administration principal, spécifiez les paramètres de connexion au Serveur d'administration suivants :

     1. Dans le champ **Serveur d'administration**, indiquez l'adresse du nouveau Serveur d'administration principal.
     2. Dans le champ **Port**, indiquez le numéro de port pour se connecter au Serveur d'administration.

        Le numéro du port par défaut est 14000.
     3. Dans le champ **Port SSL**, indiquez le numéro du port SSL sur le Serveur d'administration principal.

        Le numéro du port par défaut est 13000.
     4. Si nécessaire, cochez la case **Utiliser un serveur proxy**.

        Si cette case est décochée, la connexion directe est utilisée pour connecter l'appareil au Serveur d'administration.

        Si cette case est décochée, définissez les paramètres du serveur proxy :

        - **Adresse du serveur proxy**
        - **Port du serveur proxy**

        Si votre serveur proxy requiert une authentification, dans les champs **Nom d'utilisateur** et **Mot de passe**, indiquez les identifiants du compte sous lequel la connexion au serveur proxy est établie. Nous vous recommandons de spécifier les informations d'identification d'un compte disposant des privilèges minimaux requis uniquement pour l'authentification sur le serveur proxy.
     5. Si nécessaire, téléchargez un nouveau certificat de Serveur d'administration.

   - **Passer à un autre Serveur virtuel sur ce Serveur principal**

     Sélectionnez cette option pour déplacer les appareils clients vers le Serveur d'administration virtuel sur le Serveur d'administration principal actuel. Pour ce faire, dans le champ **Nom du Serveur d'administration virtuel**, indiquez le nom du Serveur d'administration virtuel requis.

   Si nécessaire, indiquez le temps d'attente avant de redémarrer l'Agent d'administration.

6. À cette étape de l'assistant, sélectionnez les appareils auxquels la tâche sera attribuée :

   - **Sélectionner les appareils détectés sur le réseau par le Serveur d'administration**. Dans ce cas la tâche est affectée à un ensemble d'appareils. L'ensemble d'appareils peut reprendre aussi bien des appareils de groupes d'administration que des appareils non définis.

   - **Définir les adresses des appareils manuellement ou les importer à partir d'une liste**. Vous pouvez définir les noms NetBIOS, les noms DNS, les adresses IP, ainsi que les plages d'adresses IP auxquels il convient d'affecter la tâche.

   - **Attribuer la tâche à une sélection d'appareils**. Dans ce cas, la tâche est affectée aux appareils qui appartiennent à une sélection préalable. Vous pouvez spécifier la sélection prédéfinie ou une sélection personnalisée que vous avez créée.

   - **Attribuer la tâche à un groupe d'administration**. Dans ce cas, la tâche est affectée aux appareils qui appartiennent à un groupe d'administration déjà créé.

7. À l'étape **Sélection du compte utilisateur pour exécuter la tâche** de l'assistant, indiquez les paramètres du compte :

   - Compte par défaut

     La tâche sera lancée sous le même compte utilisateur sous lequel l'application, exécutant cette tâche, a été installée et lancée.

     Cette option est sélectionnée par défaut.

   - Indiquer un compte

     Remplissez les champs **Compte utilisateur** et **Mot de passe** pour définir les détails d'un compte à partir duquel la tâche est exécutée. Le compte doit disposer de droits suffisants pour cette tâche.

     - Compte utilisateur

       Le compte utilisateur au nom duquel la tâche sera lancée.

     - Mot de passe

       Mot de passe du compte utilisateur au nom duquel la tâche sera lancée.

8. L'étape **Planifier la tâche** de l'Assistant vous permet de programmer le lancement de la tâche. Le cas échéant, configurez les paramètres suivants :

- **Programmation :**

  Sélectionnez la programmation de l'exécution de la tâche, puis configurez la programmation sélectionnée.

  - **Chaque jour (passage à l'heure d'été non pris en charge)**

    La tâche s'exécute régulièrement, selon l'intervalle défini en jours. Cette programmation ne tient pas compte du passage à l'heure d'été. Cela signifie que lorsque les horloges sont avancées ou reculées d'une heure au début ou à la fin de l'été, l'heure de lancement réelle de la tâche ne change pas.

    Nous déconseillons d'adopter cette programmation. Elle est requise pour la rétrocompatibilité avec Kaspersky Security Center.

    La tâche démarre par défaut chaque jour à l'heure système actuelle.

  - **Par jours de la semaine**

    La tâche s'exécute régulièrement les jours définis de la semaine, à l'heure indiquée.

    Par défaut, la tâche s'exécute chaque vendredi à 18h00.

  - **Chaque mois**

    La tâche s'exécute régulièrement le jour du mois défini, à l'heure indiquée.

    Si le jour en question ne figure pas dans le mois, la tâche s'exécute le dernier jour.

    La tâche s'exécute par défaut le premier jour de chaque mois, à l'heure système actuelle.

  - **Une fois**

    La tâche est exécutée une seule fois, à la date et à l'heure indiquées (par défaut, le jour de la création de la tâche).

  - **Manuel**

    La tâche ne s'exécute pas automatiquement. Vous pouvez uniquement la lancer manuellement.

    Cette option est sélectionnée par défaut.

  - **Immédiatement**

    La tâche s'exécute immédiatement après que l'appareil devient visible sur le réseau ou immédiatement après que l'appareil est inclus dans la portée de la tâche.

- **Lancer les tâches non exécutées**

Cette option détermine le comportement d'une tâche si un appareil client n'est pas visible sur le réseau quand la tâche est sur le point de démarrer.

Si la case est Activé, lors du lancement suivant de l'application de Kaspersky sur cet appareil client, une tentative de lancement de la tâche sera faite. Si la programmation de la tâche est **Manuel**, **Une fois** ou **Immédiatement**, la tâche est immédiatement lancée dès que l'appareil apparaît sur le réseau ou immédiatement après l'inclusion de l'appareil dans la zone d'action de la tâche.

Si cette option est désactivée, seules les tâches planifiées s'exécutent sur les appareils clients. Pour les planifications **Manuel**, **Une fois** et **Immédiatement**, les tâches s'exécutent uniquement sur les appareils clients qui sont visibles sur le réseau. Par exemple, vous pouvez désactiver cette option pour une tâche qui consomme des ressources que vous voulez exécuter uniquement en dehors des heures de bureau.

Cette option est Inactif par défaut.

- Adopter un décalage aléatoire automatique pour les lancements de tâche

  Si cette option est activée, la tâche est lancée sur les appareils clients de manière aléatoire au cours d'un intervalle défini. C'est ce qu'on appelle un *lancement échelonné d'une tâche*. Un lancement échelonné de tâche permet d'éviter la communication simultanée d'un nombre important d'appareils clients avec le Serveur d'administration lors du lancement de la tâche programmée.

  Le temps du lancement aléatoire est automatiquement calculée lors de la création d'une tâche selon le nombre d'appareils clients sur lesquels la tâche est diffusée. Par la suite, la tâche démarre toujours à l'heure de lancement calculée. Toutefois, quand les paramètres de la tâche sont modifiés ou si la tâche est lancée manuellement, la valeur calculée de l'heure de lancement de la tâche est modifiée.

  Si la case n'est pas cochée, le lancement de la tâche sur les appareils clients s'opère selon la planification.

- Décaler aléatoirement le lancement de la tâche dans un intervalle de (min.)

  Si cette option est activée, la tâche est lancée sur les appareils clients de manière aléatoire au cours de l'intervalle défini. Un lancement échelonné de tâche permet d'éviter la communication simultanée d'un nombre important d'appareils clients avec le Serveur d'administration lors du lancement de la tâche programmée.

  Si la case n'est pas cochée, le lancement de la tâche sur les appareils clients s'opère selon la planification.

  Cette option est Inactif par défaut. Par défaut, la valeur de cet intervalle est de une minute.

9. À cette étape de l'assistant, spécifiez le nom de la tâche que vous créez.

10. À l'étape **Fin de la création de la tâche** de l'Assistant, cliquez sur le bouton **Terminer** pour quitter l'Assistant.

    Si vous souhaitez que la tâche démarre directement à la fin de l'Assistant, cochez la case **&Lancer la tâche à la fin de l'Assistant**.

Après la fin de la tâche, les appareils clients, pour lesquels elle a été créée, passent sous l'administration du Serveur d'administration indiqué dans les paramètres de la tâche.

Si le Serveur d'administration prend en charge la fonctionnalité d'administration de chiffrement et de protection des données, lors de la création de la tâche *Modification du Serveur d'administration*, un avertissement s'affiche. Cet avertissement signale que lors de la présence des données chiffrés sur les appareils après le passage des appareils sous l'administration d'un autre serveur, les utilisateurs auront l'accès uniquement aux données chiffrées dont ils travaillaient auparavant. Dans les autres cas, l'accès aux données chiffrées ne sera pas octroyé. La description détaillée des scénarios dont l'accès aux données chiffrées ne sera pas offert est décrite dans l'Aide en ligne de Kaspersky Endpoint Security for Windows.

Déplacement des appareils connectés au Serveur d'administration via les passerelles de connexion vers un autre Serveur d'administration

Vous pouvez déplacer des appareils connectés au Serveur d'administration via les passerelles de connexion vers un autre Serveur d'administration. Par exemple, cela peut être nécessaire si vous installez une autre version du Serveur d'administration et que vous ne souhaitez pas réinstaller l'Agent d'administration sur les appareils, car cela peut prendre du temps.

Les commandes décrites dans l'instruction doivent être exécutées sur les appareils clients sous un compte disposant de privilèges d'administrateur.

Pour déplacer un appareil connecté via la passerelle de connexion vers un autre Serveur d'administration, procédez comme suit :

1. Exécutez l'utilitaire klmover avec le paramètre `-address <adresse du serveur>` pour passer au nouveau Serveur d'administration.
2. Exécutez la commande `klnagchk -nagwait -tl 4`.
3. Exécutez les commandes suivantes pour définir une nouvelle passerelle de connexion :
   - `klscflag -ssvset -pv klnagent -s FileTransfer -n ft_gateway_mode -sv false -svt BOOL_T -ss "|ss_type = \"SS_SETTINGS\";"`
   - `klscflag -ssvset -pv klnagent -s FileTransfer -n ft_gateway_loc -sv "<gateway_ip_or_name>" -svt STRING_T -ss "|ss_type = \"SS_SETTINGS\";"`

     Ici, le paramètre `gateway_ip_or_name` est l'adresse de la passerelle de connexion accessible depuis Internet.
   - `klscflag -ssvset -pv klnagent -s FileTransfer -n ft_gateway_ssl_port -sv 13000 -svt INT_T -ss "|ss_type = \"SS_SETTINGS\";"`

     Le `13000` est le numéro de port TCP que la passerelle de connexion est en train d'écouter.
4. Exécutez la commande `klnagchk -restart -tl 4` pour démarrer le service de l'Agent d'administration.

L'appareil est déplacé vers le nouveau Serveur d'administration et connecté via la nouvelle passerelle connectée.

Clusters et matrices des serveurs

Kaspersky Security Center prend en charge la technologie de cluster. Si l'Agent d'administration transmet au Serveur d'administration les informations sur le fait que l'application installée sur l'appareil client est une partie de la matrice du serveur, alors l'appareil client devient le nœud du cluster. Le cluster sera ajouté comme un objet séparé dans le dossier **Appareils administrés** dans l'arborescence de la console avec l'icône des serveurs ( ).

Il est possible de choisir plusieurs propriétés types du cluster :

- Le cluster et toutes ses entrées se trouvent toujours dans un groupe d'administration.
- Si l'administrateur tente de déplacer une entrée quelconque du cluster, l'entrée reviendra dans l'emplacement d'origine.
- Si l'administrateur tente de déplacer le cluster dans un autre groupe, toutes ses entrées seront aussi déplacées avec celui-ci.

Démarrage, arrêt et redémarrage à distance des appareils clients

Kaspersky Security Center permet de gérer à distance les appareils clients : les démarrer, les arrêter et les redémarrer.

Pour administrer à distance les appareils clients, procédez comme suit :

1. Connectez-vous au Serveur d'administration, qui administre les appareils.
2. Créez une tâche d'administration de l'appareil par un des moyens suivants :
   - S'il faut allumer, éteindre ou redémarrer les appareils qui font partie du groupe d'administration sélectionné, créer une tâche pour le groupe sélectionné.
   - S'il faut allumer, éteindre ou redémarrer les appareils qui font partie des différents groupes d'administration ou non, créez une tâche pour l'ensemble d'appareils.

   Ceci permet de lancer l'Assistant de création d'une tâche. Suivez les instructions de l'assistant. Dans la fenêtre **Sélection du type de tâche** de l'Assistant de création d'une tâche, sélectionnez l'entrée **Kaspersky Security Center**, ouvrez le dossier **Avancé** et sélectionnez la tâche **Administration des appareils**.
3. Lancez la tâche créée.

Après la fin du fonctionnement de la tâche, la commande (démarrage, arrêt, redémarrage) sera exécutée sur les appareils sélectionnés.

À propos de l'utilisation de la connexion continue entre un appareil administré et le Serveur d'administration

Par défaut Kaspersky Security Center ne donne pas de connexions permanentes entre les appareils administrés et le Serveur d'administration. Les agents d'administration sur les appareils administrés établissent périodiquement une connexion et se synchronisent avec le Serveur d'administration. L'intervalle entre ces sessions de synchronisation est défini dans une stratégie de l'Agent d'administration et est de 15 minutes par défaut. Si une synchronisation s'impose plus tôt (par exemple, pour accélérer l'application d'une stratégie), le Serveur d'administration envoie à l'Agent d'administration un paquet réseau signé au port UDP 15000. (Le Serveur d'administration peut envoyer ce paquet sur un réseau IPv4 ou IPv6.) Si aucune connexion via UDP entre le Serveur d'administration et l'appareil administré n'est possible pour une raison quelconque, la synchronisation se déroule lors de la prochaine connexion de l'Agent d'administration au Serveur d'administration pendant la période de synchronisation.

Cependant, certaines opérations ne peuvent pas être effectuées sans une connexion précoce entre l'Agent d'administration et le Serveur d'administration. Ces opérations comprennent l'exécution et l'arrêt de tâches locales, la réception de statistiques pour une application administrée et la création d'un tunnel. Pour rendre ces opérations possibles, vous devez activer **Maintenir la connexion au Serveur &d'administration** l'option sur l'appareil administré.

À propos de la synchronisation forcée

Malgré le fait que Kaspersky Security Center synchronise automatiquement l'état, les paramètres, les tâches et les stratégies pour les appareils administrés, il existe des cas où l'administrateur doit savoir exactement si la synchronisation de cette appareil a eu lieu à ce moment.

Dans le menu contextuel des appareils administrés de la Console d'administration, l'option de menu **Toutes les tâches** contient la commande **Forcer la synchronisation**. Quand Kaspersky Security Center 15.1 exécute cette commande, le Serveur d'administration tente de contacter l'appareil. Si cette tentative réussit, la synchronisation forcée a lieu. Dans le cas contraire, la synchronisation ne sera forcée qu'après la prochaine connexion prévue entre l'Agent d'administration et le Serveur d'administration.

À propos du gestionnaire des connexions

Dans la fenêtre des propriétés de l'Agent d'administration, dans la section **Connectivité**, dans la sous-section **Calendrier de connexion**, il est possible de définir les intervalles temporaires auxquels l'Agent d'administration transmettra les données sur le Serveur d'administration.

Se connecter en cas de nécessité. Si cette option a été sélectionnée, la connexion s'établira quand l'Agent d'administration devra transférer les données sur le Serveur d'administration.

Se connecter aux intervalles indiqués. Si cette option a été sélectionnée, la connexion de l'Agent d'administration au Serveur d'administration est effectuée dans les intervalles indiqués. Plusieurs périodes de connexions peuvent être ajoutées.

Envoi d'un message aux utilisateurs des appareils

Pour envoyer un message aux utilisateurs des appareils, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez l'entrée portant le nom du Serveur d'administration requis.
2. Créez une tâche d'envoi du message aux utilisateurs des appareils par un des moyens suivants :
   - S'il faut envoyer un message aux utilisateurs des appareils qui font partie du groupe d'administration sélectionné, créez une tâche pour le groupe sélectionné.
   - S'il faut envoyer un message aux utilisateurs des appareils qui font partie de différents groupes d'administration ou qui n'appartiennent à aucun groupe, créez une tâche pour l'ensemble d'appareils.

   Ceci permet de lancer l'Assistant de création d'une tâche. Suivez les instructions de l'assistant.
3. Dans la fenêtre du type de tâche de l'Assistant de création d'une tâche, sélectionnez le nœud **Serveur d'administration de Kaspersky Security Center**, ouvrez le dossier **Avancé** et sélectionnez la tâche **Envoyer le message à l'utilisateur**. La tâche Envoi de messages aux utilisateurs est disponible uniquement sur les appareils qui tournent sous Windows. Vous pouvez également envoyer des messages via le menu contextuel de l'utilisateur dans le dossier **Comptes utilisateurs**.
4. Lancez la tâche créée.

   A la fin du fonctionnement de la tâche, le message créé sera envoyé aux utilisateurs des appareils sélectionnés. La tâche Envoi de messages aux utilisateurs est disponible uniquement sur les appareils qui tournent sous Windows. Vous pouvez également envoyer des messages via le menu contextuel de l'utilisateur dans le dossier **Comptes utilisateurs**.

Utilisation de l'application Kaspersky Security for Virtualization

Kaspersky Security Center prend en charge la possibilité de connecter les machines virtuelles au Serveur d'administration. Les machines virtuelles sont protégées par Kaspersky Security for Virtualization. Pour en savoir plus, reportez-vous à la documentation de cette application.

Configuration de la permutation des états des appareils

Vous pouvez modifier les conditions pour attribuer le statut *Critique* ou *Avertissement* à un appareil.

Pour activer le changement d'état de l'appareil sur Critique :

1. Ouvrez la fenêtre des propriétés à l'aide d'un des moyens suivants :
   - Dans le dossier **Stratégies**, dans le menu contextuel d'une stratégie du Serveur d'administration, sélectionnez **Propriétés**.
   - Dans le menu contextuel du groupe d'administration, choisissez **Propriétés**.
2. Dans la fenêtre **Propriétés** qui s'ouvre, dans le volet **Sections**, sélectionnez **État de l'appareil**.

3. Dans le volet droit, dans la section **Définir l'état comme Critique si**, cochez la case en regard d'une condition dans la liste.

   Vous pouvez modifier seulement les paramètres qui ne sont pas verrouillés dans la stratégie parent.

4. Double-cliquez sur le nom de la condition sélectionnée, puis dans la fenêtre qui s'ouvre, définissez la valeur requise pour la condition.

   Vous ne pouvez pas définir de valeurs pour les conditions suivantes : L'application de sécurité n'est pas installée, Des applications incompatibles sont installées, Vulnérabilités détectées dans les applications, Les paramètres de l'appareil mobile ne correspondent pas à la stratégie, Problèmes de sécurité non traités détectés, État de l'appareil défini par l'application, L'appareil n'est plus administré, L'application de sécurité n'est pas en cours d'exécution, La licence a expiré.

   Pour la condition **Redémarrage requis**, vous pouvez préciser les raisons du redémarrage. Nous vous recommandons de cocher les cases à côté de toutes les raisons de la liste.

5. Cliquez sur le bouton **OK**.

Lorsque les conditions spécifiées sont remplies, l'appareil administré se voit affecter l'état *Critique*.

Pour activer le changement d'état de l'appareil sur Avertissement :

1. Ouvrez la fenêtre des propriétés à l'aide d'un des moyens suivants :

   - Dans le dossier **Stratégies**, dans le menu contextuel de la stratégie de Serveur d'administration, sélectionnez **Propriétés**.
   - Dans le menu contextuel du groupe d'administration, choisissez **Propriétés**.

2. Dans la fenêtre **Propriétés** qui s'ouvre, dans le volet **Sections**, sélectionnez **État de l'appareil**.

3. Dans le volet droit, dans la section **Définir l'état comme Avertissement si**, cochez la case en regard d'une condition dans la liste.

   Vous pouvez modifier seulement les paramètres qui ne sont pas verrouillés dans la stratégie parent.

4. Double-cliquez sur le nom de la condition sélectionnée, puis dans la fenêtre qui s'ouvre, définissez la valeur requise pour la condition.

   Vous ne pouvez pas définir de valeurs pour les conditions suivantes : L'application de sécurité n'est pas installée, Des applications incompatibles sont installées, Vulnérabilités détectées dans les applications, Les paramètres de l'appareil mobile ne correspondent pas à la stratégie, Problèmes de sécurité non traités détectés, État de l'appareil défini par l'application, L'appareil n'est plus administré, L'application de sécurité n'est pas en cours d'exécution, La licence a expiré.

   Pour la condition **Redémarrage requis**, vous pouvez préciser les raisons du redémarrage. Nous vous recommandons de cocher les cases à côté de toutes les raisons de la liste.

5. Cliquez sur le bouton **OK**.

Lorsque certaines conditions spécifiées sont remplies, l'appareil administré se voit affecter l'état *Avertissement*.

Attribution des tags aux appareils et consultation des tags attribués

Kaspersky Security Center permet de désigner les tags pour les appareils. Un *tag* est un identificateur de l'appareil qui peut être utilisé pour regrouper, décrire ou rechercher des appareils. Les tags désignés pour les appareils peuvent être utilisés lors de la création de sélections d'appareils, lors de la recherche d'appareils et lors de la répartition d'appareils en groupes d'administration.

Les tags peuvent être désignés pour les appareils manuellement ou automatiquement. La désignation manuelle de tags pour un appareil s'opère dans les propriétés de l'appareil et peut être requise quand il faut marquer un appareil distinct. La désignation automatique des tags est l'œuvre du Serveur d'administration conformément aux règles spécifiées de l'attribution des tags.

Les propriétés du Serveur d'administration permettent de configurer l'attribution automatique de tags aux appareils administrés par ce Serveur d'administration. L'attribution automatique de tags aux appareils s'opère lors de l'exécution des règle définies. A chaque tag correspond une règle distincte. Les règles peuvent être appliquées aux propriétés réseau de l'appareil, au système d'exploitation de l'appareil, aux applications installées sur l'appareil ou à d'autres propriétés de l'appareil. Par exemple, vous pouvez configurer une règle selon laquelle un appareil tournant sous le système d'exploitation Windows va recevoir le tag *Win*. Vous pouvez utiliser ensuite ce tag dans la création d'une sélection d'appareils qui reprendrait les appareils tournant sous un système d'exploitation Windows et leur attribuer une tâche.

Vous pouvez utiliser aussi les tags en qualité de condition pour l'activation d'un profil de stratégie sur l'appareil administré afin que les profils de stratégie définis soient uniquement appliqués aux appareils qui possèdent les tags définis. Par exemple, si un appareil portant le tag *Courrier* apparaît dans le groupe d'administration *Utilisateurs* et que ce tag *Courrier* détermine la configuration de l'activation du profil de stratégie correspondant, cet appareil ne sera pas soumis à cette stratégie créée pour le groupe *Utilisateurs*, mais bien à son profil. Le profil de stratégie peut autoriser le lancement sur cet appareil d'applications distinctes dont le lancement est interdit par la stratégie.

Vous pouvez créer plusieurs règles d'attribution des tags. Plusieurs tags peuvent être attribués à un appareil si vous aviez créé plusieurs règles et que les conditions d'exécution de ces règles sont remplies simultanément. Vous pouvez consulter la liste de tous les tags attribués dans les propriétés de l'appareil. Chaque règle d'attribution de tag peut être activée ou désactivée. Si la règle est activée, elle s'applique aux appareils administrés par le Serveur d'administration. Si la règle n'est pas nécessaire maintenant, mais peut-être à l'avenir, il n'est pas nécessaire de l'effacer ; il suffit de décocher la case **Activer la règle**. Ainsi, la règle est désactivée et elle n'est plus appliquée tant que la case **Activer la règle** n'est pas à nouveau cochée. La désactivation d'une règle sans sa suppression peut être requise si cette règle doit être exclue temporairement de la liste des règles d'attribution des tags avant d'être activée à nouveau.

Attribution automatique de tags aux appareils

Vous pouvez créer et modifier les règles d'attribution automatique des tags dans la fenêtre des propriétés du Serveur d'administration.

Pour attribuer automatiquement des tags à des appareils, procédez comme suit :

1. Dans l'arborescence de la console, choisissez l'entrée portant le nom du Serveur d'administration pour lequel il faut créer une règle d'attribution des tags.

2. Dans le menu contextuel Serveur d'administration, sélectionnez l'option **Propriétés**.

3. Dans la fenêtre des propriétés du Serveur d'administration, sélectionnez la section **Règles d'attribution des tags**.

4. Dans la section **Règles d'attribution des tags**, cliquez sur le bouton **Ajouter**.

   La fenêtre **Nouvelle règle** s'ouvre.

5. Dans la fenêtre **Nouvelle règle**, configurez les propriétés générales de la règle :

   - Indiquez le nom de la règle.

     Le nom de la règle ne peut pas contenir plus de 255 symboles et contenir de symboles spéciaux (`"*<>?\:|`).

   - Activez ou désactivez la règle à l'aide de la case à cocher **Activer la règle**.

     La case **Activer la règle** est cochée.

   - Dans le champ **Tag**, saisissez le nom du tag.

     Le nom d'un tag ne peut pas contenir plus de 255 symboles et contenir de symboles spéciaux (`"*<>?\:|`).

6. Dans la section **Conditions**, cliquez sur le bouton **Ajouter** pour ajouter une nouvelle condition ou sur le bouton **Propriétés** pour modifier une condition existante.

   La fenêtre de l'Assistant de création d'une condition pour la règle d'attribution automatique des tags s'ouvre.

7. Dans la fenêtre **Condition d'attribution du tag**, cochez les cases correspondant aux conditions devant avoir un impact sur l'attribution des tags. Il est possible de choisir plusieurs conditions.

8. En fonction des conditions d'attribution du tag que vous avez choisies, l'Assistant affiche une fenêtre de configuration des conditions correspondantes. Configurez le déclenchement de la règle selon les conditions suivantes :

   - **Utilisation de l'appareil ou association à un &réseau spécifique** : Propriétés réseau de l'appareil, par exemple le nom de l'appareil sur le réseau Windows et l'appartenance de l'appareil au domaine ou à un sous-réseau IP.

     > Si le classement sensible à la casse est défini pour la base de données que vous utilisez pour Kaspersky Security Center, respectez la casse lorsque vous indiquez le nom DNS de l'appareil. Sinon, la règle de marquage automatique ne fonctionnera pas.

   - **Utilisation d'&Active Directory** : présence de l'appareil dans la sous-section Active Directory et appartenance de l'appareil au groupe Active Directory.

   - **Applications définies** : présence sur l'appareil de l'Agent d'administration, le type, la version et l'architecture du système d'exploitation.

   - **Machines virtuelles** : inclusion de l'appareil à un type de machine virtuelle spécifique.

   - **Application installée depuis le registre des applications** : présence sur l'appareil d'applications de différents éditeurs.

9. Après avoir configuré les conditions, saisissez le nom de la condition et quittez l'Assistant.

   Le cas échéant, il est possible d'attribuer plusieurs catégories à une règle. Dans ce cas, le tag est attribué aux appareils quand au moins une des conditions est remplie. Les conditions ajoutées sont affichées dans la fenêtre de propriétés de la règle.

10. Cliquez sur **OK** dans la fenêtre **Nouvelle règle**, puis sur le bouton **OK** dans la fenêtre des propriétés du Serveur d'administration.

Les règles créées sont exécutées sur les appareils administrés par le Serveur d'administration sélectionné. Si les paramètres de l'appareil correspondent aux conditions de la règle, cet appareil reçoit ce tag.

Consultation et configuration des tags attribués à l'appareil

Vous pouvez consulter la liste de tous les tags attribués à un appareil et accéder à la configuration des règles d'attribution automatique de tags dans la fenêtre des propriétés de l'appareil.

Pour consulter et configurer les tags attribués à un appareil, procédez comme suit :

1. Dans l'arborescence de la console ouvrez le dossier **Appareils administrés**.
2. Dans l'espace de travail du dossier **Appareils administrés**, sélectionnez l'appareil dont vous souhaitez consulter les tags attribués.
3. Dans le menu contextuel de l'appareil sélectionné, sélectionnez l'option **Propriétés**.
4. Dans la fenêtre des propriétés de l'appareil, sélectionnez la section **Tags**.

   La liste des tags attribués à l'appareil sélectionné, ainsi que le mode d'attribution (manuel ou selon une règle) s'affichent.
5. Le cas échéant, exécutez une des actions suivantes :
   - Pour passer à la configuration des règles d'attribution des tags, cliquez sur le lien **Configurer les règles d'attribution automatique de tags**.
   - Pour renommer un tag, sélectionnez le tag, puis cliquez sur le bouton **Renommer**.
   - Pour supprimer un tag, sélectionnez le tag, puis cliquez sur le bouton **Supprimer**.
   - Pour ajouter un tag manuellement, saisissez le tag dans le champ de la partie inférieure de la section **Tags**, puis cliquez sur le bouton **Ajouter**.
6. Cliquez sur le bouton **Appliquer** si vous avez introduit des modifications dans la section **Tags** afin que ces modifications entrent en vigueur.
7. Cliquez sur le bouton **OK**.

Si vous avez supprimé ou renommé un tag dans les propriétés de l'appareil, cette modification ne s'applique pas aux règles d'attribution des tags définies dans les propriétés du Serveur d'administration. La modification est appliquée uniquement à l'appareil dont les propriétés ont été modifiées.

Diagnostic à distance des appareils clients. Utilitaire de diagnostic à distance Kaspersky Security Center

L'utilitaire de diagnostic à distance Kaspersky Security Center (ci-après : utilitaire de diagnostic à distance) est conçue pour exécuter à distance des opérations suivantes sur les appareils clients :

- Activation et désactivation du traçage, modification du niveau de traçage, téléchargement du fichier de traçage.
- Téléchargement des informations relatives au système et des paramètres des applications.

- Téléchargement des journaux des événements.
- Génération d'un fichier dump pour une application.
- Lancement du diagnostic et téléchargement des rapports du diagnostic.
- Lancement et arrêt des applications.

Vous pouvez utiliser les journaux des événements et les rapports de diagnostic téléchargés depuis un appareil client pour résoudre vous-même un problème. Un expert du Support Technique de Kaspersky peut également vous demander de télécharger les fichiers de traçage, les fichiers dump, les journaux des événements et les rapports de diagnostic d'un appareil client pour que Kaspersky puisse réaliser une analyse plus poussée.

L'utilitaire de diagnostic à distance s'installe automatiquement sur l'appareil conjointement avec la Console d'administration.

Connexion de l'utilitaire de diagnostic à distance à l'appareil client

Pour connecter l'utilitaire de diagnostic à distance à l'appareil client, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez n'importe quel groupe d'administration.
2. Dans l'espace de travail, sous l'onglet **Appareils**, dans le menu contextuel de n'importe quel appareil, sélectionnez l'option **Outils externes → Diagnostic à distance**.

   Finalement, la fenêtre principale de l'utilitaire de diagnostic à distance s'ouvrira.
3. Dans le champ droit de la fenêtre principale de l'utilitaire de diagnostic à distance, définissez les moyens de connexion à l'appareil :
   - **Accès à l'aide des outils du réseau Microsoft Windows**.
   - **Accès à l'aide des outils du Serveur d'administration**.
4. Si dans le premier champ de la fenêtre d'utilitaire, vous avez sélectionné **Accès à l'aide des outils du réseau Microsoft Windows**, procédez comme suit :
   - Dans le champ **Appareil**, indiquez l'adresse de l'appareil auquel vous devez vous connecter

     L'adresse d'appareil peut être une adresse IP, un nom NetBIOS ou DNS.

     Par défaut, l'adresse de l'appareil est indiqué, dont l'utilitaire a été lancé depuis son menu contextuel.
   - Indiquez le compte utilisateur pour vous connecter à l'appareil :
     - **Se connecter au nom de l'utilisateur en cours** (sélectionné par défaut). Connectez-vous à l'aide du compte utilisateur actuel.
     - **Utiliser, lors de la connexion, le nom d'utilisateur et le mot de passe fournis**. Connectez-vous à l'aide d'un compte utilisateur fourni. Indiquez **Nom d'utilisateur** et **Mot de passe** du compte utilisateur nécessaire.

     La connexion à l'appareil est possible uniquement sous le compte utilisateur de l'administrateur local de l'appareil.

5. Si dans le premier champ, vous avez sélectionné **Accès à l'aide des outils du Serveur d'administration**, procédez comme suit :

   - Dans le champ **Serveur d'administration**, indiquez l'adresse du Serveur d'administration depuis lequel vous souhaitez vous connecter à l'appareil.

     L'adresse du Serveur peut être une adresse IP, un nom NetBIOS ou DNS.

     Par défaut l'adresse du Serveur d'administration, depuis lequel l'utilitaire a été lancé, est indiquée.

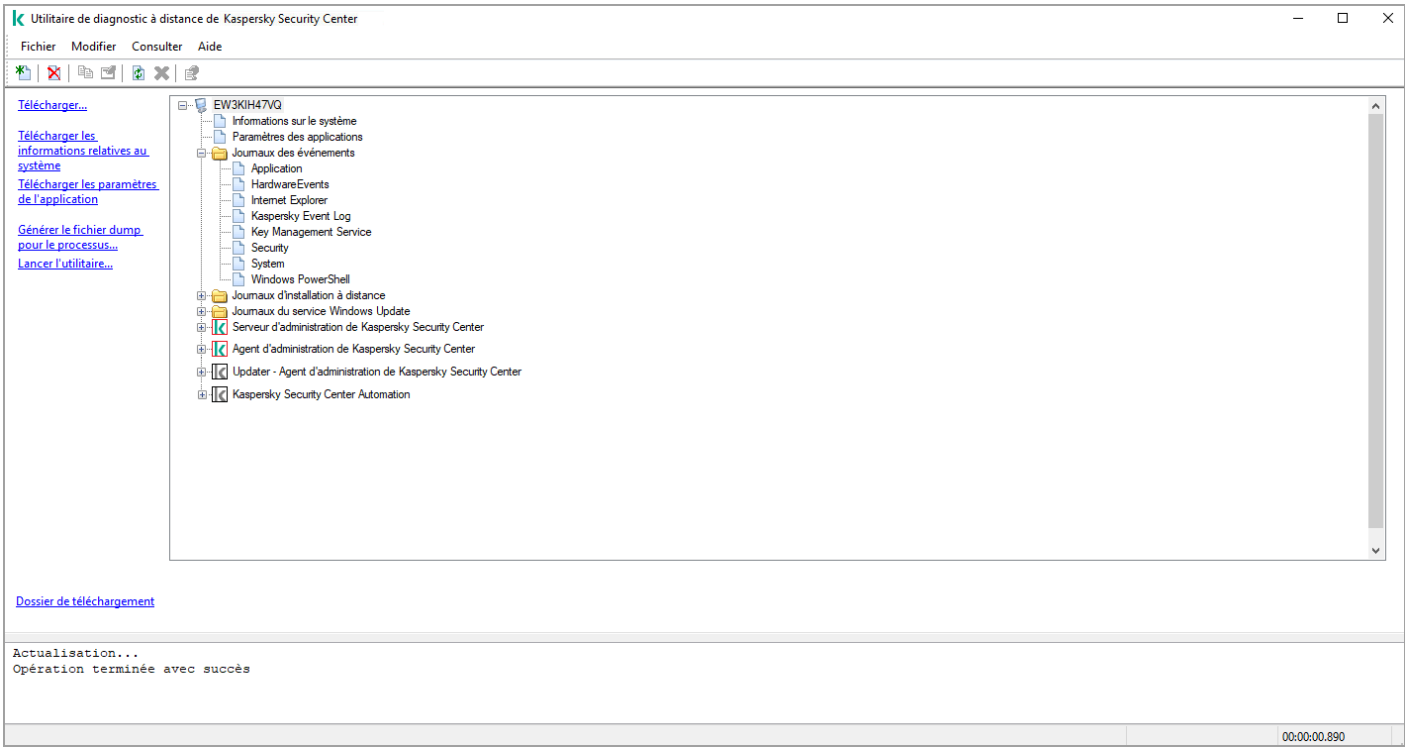
   - Si nécessaire, cochez les cases **Utiliser SSL**, **Compresser le trafic** et **L'appareil appartient au Serveur d'administration secondaire**.

     Si la case **L'appareil appartient au Serveur d'administration secondaire** est cochée, vous pouvez renseigner le champ **L'appareil appartient au Serveur d'administration secondaire** avec le nom du Serveur d'administration secondaire qui administre l'appareil en cliquant sur le bouton **Parcourir**.

6. Pour vous connecter à l'appareil, cliquez sur le bouton **Se connecter**.

> Vous devez autoriser l'utilisation de la vérification en deux étapes si la vérification en deux étapes est activée pour votre compte.

Cette action ouvre la fenêtre de diagnostic à distance de l'appareil (cf. ill. ci-après). La partie gauche de la fenêtre reprend les liens pour exécuter les opérations de diagnostic de l'appareil. La partie droite de la fenêtre reprend l'arborescence des objets de l'appareil avec lesquels l'utilitaire peut fonctionner. La partie inférieure de la fenêtre affiche le processus d'exécution des opérations de l'utilitaire.



Utilitaire de diagnostic à distance. Fenêtre du diagnostic à distance de l'appareil

L'utilitaire de diagnostic à distance enregistre les fichiers téléchargés des appareils sur le bureau de l'appareil, depuis lequel il était lancé.

Génération d'un fichier dump pour une application

Le fichier de vidage de l'application vous permet de consulter les paramètres de l'application exécutée sur l'appareil client à un moment donné. Ce fichier contient également des informations sur les modules chargés pour une application.

L'obtention de fichiers de vidage à partir d'appareils Linux n'est pas prise en charge.

L'utilitaire kldumper est utilisé pour obtenir les fichiers de vidage via le diagnostic à distance. Cet utilitaire est conçu pour obtenir les fichiers de vidage des processus des applications Kaspersky à la demande des experts du Support technique. Vous trouverez plus de détails sur les exigences relatives à l'utilisation de l'utilitaire kldumper dans la Base de connaissances de Kaspersky Security Center.

Pour créer un fichier de vidage pour une application :

1. Dans l'espace de travail du dossier **Appareils administrés**, sous l'onglet **Appareils**, ouvrez le menu contextuel de l'appareil nécessaire, puis sélectionnez **Outils externes → Diagnostic à distance**.

   La fenêtre **Utilitaire de diagnostic à distance de Kaspersky Security Center** s'ouvre.

2. Connectez l'utilitaire de diagnostic à distance à l'appareil client.

   Cette action ouvre la fenêtre de diagnostic à distance de l'appareil.

3. Dans la partie gauche de la fenêtre, cliquez sur le lien **Générer le fichier dump pour le processus**

4. Dans la fenêtre **Génération du fichier dump du processus** qui s'ouvre, indiquez le fichier exécutable de l'application pour lequel vous souhaitez générer le fichier dump.

5. Cliquez sur le bouton **OK**.

Les archives avec le fichier de vidage de l'application sont téléchargées.

Si l'application indiquée n'est pas exécutée sur l'appareil client, le dossier « result » contenu dans l'archive téléchargée sera vide.

Si l'application indiquée fonctionne, mais que le téléchargement échoue avec une erreur ou que le dossier « result » est vide dans l'archive téléchargée, consultez la Base de connaissances de Kaspersky Security Center.

Activation et désactivation du traçage, téléchargement du fichier de traçage

Pour activer le traçage sur un appareil distant :

1. Lancez l'utilitaire de diagnostic à distance et connectez-vous à l'appareil nécessaire.

2. Dans l'arborescence des objets de l'appareil, sélectionnez l'application pour laquelle vous souhaitez activer le traçage.

   > Activation et désactivation du traçage des applications avec l'autodéfense sont possibles uniquement lors de la connexion à l'appareil via les outils du Serveur d'administration.

   Si vous souhaitez activer le traçage pour l'Agent d'administration, vous pouvez le faire pendant la création de la tâche Installation des mises à jour requises et correction des vulnérabilités. Dans ce cas, l'Agent d'administration enregistre les informations de traçage même si le traçage a été désactivé pour l'Agent d'administration dans l'utilitaire de diagnostic à distance.

3. Pour activer le traçage :

   a. Dans la partie gauche de la fenêtre de l'utilitaire de diagnostic à distance, cliquez sur **Activer le traçage**.

   b. Dans la fenêtre **Sélection du niveau de traçage** qui s'ouvre, nous conseillons de conserver les valeurs par défaut pour les paramètres. Le cas échéant, un expert du Support Technique vous guidera au cours du processus de configuration. Les paramètres suivants sont disponibles :

   - **Niveau de traçage**

     Le niveau de traçage définit le volume de détails repris dans le fichier de traçage.

   - **Traçage sur la base d'une rotation** (disponible uniquement pour Kaspersky Endpoint Security)

     L'application écrase les informations de traçage afin d'empêcher l'augmentation excessive de la taille du fichier de traçage. Indiquez le nombre maximal de fichiers à utiliser pour stocker les informations de traçage ainsi que la taille maximale de chaque fichier. Quand le nombre maximum de fichiers de traçage de la taille maximale est atteint, le fichier de traçage le plus ancien est supprimé afin de pouvoir écrire un nouveau fichier de traçage.

   c. Cliquez sur le bouton **OK**.

4. Pour Kaspersky Endpoint Security, un expert du Support Technique peut vous demander d'activer le traçage Xperf pour les informations relatives aux performances du système.

   Pour activer le traçage Xperf :

   a. Dans la partie gauche de la fenêtre de l'utilitaire de diagnostic à distance, cliquez sur **Activer le traçage Xperf**.

   b. Dans la fenêtre **Sélection du niveau de traçage** qui s'ouvre, en fonction de la demande de l'expert du Support Technique, sélectionnez un des niveaux de traçage suivants :

   - **Niveau faible**

     Un fichier de traçage de ce genre contient le minimum d'informations sur le système.

     Cette option est sélectionnée par défaut.

   - **Niveau profond**

     Un fichier de traçage de ce type contient plus de détails que les fichiers de traçage du niveau *Clair* et qui peut être sollicité par les experts du Support Technique lorsqu'un fichier de traçage du niveau *Clair* ne suffit pas à évaluer les performances. Le fichier de traçage *Profond* contient les informations techniques relatives au système, dont les informations relatives au matériel, au système d'exploitation, à la liste des processus et des applications lancés et arrêtés, aux événements utilisés pour l'évaluation des performants et aux événements de l'outil d'évaluation du système Windows.

   c. Sélectionnez l'un des types de traçage ci-dessous :

   - **Type élémentaire**

Les informations de traçage sont obtenues pendant le fonctionnement de l'application Kaspersky Endpoint Security.

Cette option est sélectionnée par défaut.

- **Type au redémarrage**

  Les informations de traçage sont reçues au du démarrage du système d'exploitation sur l'appareil administré. Ce type de traçage est efficace lorsque le problème qui affecte les performances du système se produit après que l'appareil est allumé et avant le démarrage de Kaspersky Endpoint Security.

d. Vous pourriez également être invité à activer l'option **Traçage sur la base d'une rotation** pour empêcher l'augmentation excessive de la taille du fichier de traçage. Définissez ensuite la taille maximale de chaque fichier de traçage. Quand le fichier atteint la taille maximale, les informations de traçage les plus anciennes sont écrasées par les nouvelles.

e. Cliquez sur le bouton **OK**.

Dans certains cas, pour activer le traçage de l'application de sécurité, il faut relancer cette application et sa tâche.

L'utilitaire de diagnostic à distance active le traçage pour l'application sélectionnée.

Pour télécharger un fichier de traçage depuis une application :

1. Exécutez l'utilitaire de diagnostic à distance, puis connectez-vous à l'appareil requis, conformément aux explications du point "Connexion de l'utilitaire de diagnostic à distance à l'appareil client".
2. Dans l'entrée de l'application, ouvrez le dossier **Fichiers de traçage** et sélectionnez le fichier requis.
3. Dans la partie gauche de la fenêtre de l'utilitaire de diagnostic à distance, cliquez sur **Télécharger le fichier entier**.

   Pour les fichiers de grande taille, il existe une possibilité de télécharger les dernières parties du traçage.

   Vous pouvez supprimer le fichier de traçage sélectionné. La suppression du fichier de traçage est possible après la désactivation du traçage.

Le fichier sélectionné est téléchargé dans l'emplacement indiquée dans la partie inférieure de la fenêtre.

Pour désactiver le traçage sur un appareil distant :

1. Exécutez l'utilitaire de diagnostic à distance, puis connectez-vous à l'appareil requis, conformément aux explications du point "Connexion de l'utilitaire de diagnostic à distance à l'appareil client".
2. Dans l'arborescence des objets de l'appareil, sélectionnez l'application pour laquelle vous souhaitez désactiver le traçage.

   Activation et désactivation du traçage des applications avec l'autodéfense sont possibles uniquement lors de la connexion à l'appareil via les outils du Serveur d'administration.

3. Dans la partie gauche de la fenêtre de l'utilitaire de diagnostic à distance, cliquez sur **Désactiver le traçage**.

L'utilitaire de diagnostic à distance désactive le traçage pour l'application sélectionnée.

Téléchargement des paramètres de l'application

Pour télécharger les paramètres des applications depuis l'appareil distant, procédez comme suit :

1. Exécutez l'utilitaire de diagnostic à distance, puis connectez-vous à l'appareil requis, conformément aux explications du point "Connexion de l'utilitaire de diagnostic à distance à l'appareil client".

2. Dans l'arborescence des objets de la fenêtre de l'utilitaire de diagnostic à distance, sélectionnez l'entrée supérieure avec le nom de l'appareil.

3. Dans la partie gauche de la fenêtre de l'utilitaire de diagnostic à distance, sélectionnez l'action requise parmi les options suivantes :

   - **Télécharger les informations relatives au système**
   - **Télécharger les paramètres de l'application**
   - **Générer le fichier dump pour le processus**

     Dans la fenêtre, ouverte à l'aide du lien, indiquez le fichier exécutable de l'application pour laquelle il faut créer le fichier dump.

   - **Lancer l'utilitaire**

     Dans la fenêtre, ouverte à l'aide du lien, indiquez le fichier exécutable de l'utilitaire sélectionné et les paramètres de son lancement.

Finalement, l'utilitaire sélectionné sera téléchargé et lancé sur l'appareil.

Téléchargement des journaux des événements

Pour télécharger le journal des événements depuis l'appareil distant, procédez comme suit :

1. Exécutez l'utilitaire de diagnostic à distance, puis connectez-vous à l'appareil requis, conformément aux explications du point "Connexion de l'utilitaire de diagnostic à distance à l'appareil client".

2. Dans le dossier **Journaux des événements système** de l'arborescence des objets de l'appareil, sélectionnez le journal pertinent.

3. Téléchargez le journal sélectionné d'un clic sur le lien **Charger le journal des événements <nom du journal des événements>** dans la partie droite de la fenêtre de l'utilitaire de diagnostic à distance.

Le journal des événements sélectionné est téléchargé dans l'emplacement indiqué dans le volet inférieur.

Téléchargement de plusieurs éléments d'information de diagnostic

L'utilitaire de diagnostic à distance de Kaspersky Security Center permet de télécharger plusieurs éléments d'information de diagnostic dont les journaux des événements, les informations système, les fichiers de traçage et les fichiers dump.

Pour télécharger informations diagnostiques depuis l'appareil distant, procédez comme suit :

1. Exécutez l'utilitaire de diagnostic à distance, puis connectez-vous à l'appareil requis, conformément aux explications du point "Connexion de l'utilitaire de diagnostic à distance à l'appareil client".
2. Dans la partie gauche de la fenêtre de l'utilitaire de diagnostic à distance, cliquez sur **Télécharger**.
3. Cochez les cases en regard des éléments que vous souhaitez télécharger.
4. Cliquez sur **Démarrer**.

Chaque élément sélectionné est téléchargé dans l'emplacement défini dans le volet inférieur.

Lancement du diagnostic et téléchargement des résultats

Pour lancer le diagnostic de l'application sur l'appareil distant et télécharger les résultats, procédez comme suit :

1. Exécutez l'utilitaire de diagnostic à distance, puis connectez-vous à l'appareil requis, conformément aux explications du point "Connexion de l'utilitaire de diagnostic à distance à l'appareil client".
2. Dans l'arborescence des objets de l'appareil, sélectionnez l'application nécessaire.
3. Lancez le diagnostic en cliquant sur le lien **Poser le diagnostic** dans la partie gauche de la fenêtre de l'utilitaire de diagnostic à distance.

   Finalement, dans l'entrée de l'application sélectionnée, le rapport de diagnostic apparaîtra dans l'arborescence des objets.
4. Sélectionnez le rapport de diagnostic récemment généré dans l'arborescence des objets et téléchargez-le en cliquant sur le lien **Dossier de téléchargement**.

Le rapport sélectionné est téléchargé dans l'emplacement indiqué dans le volet inférieur.

Lancement, arrêt ou relancement des applications

Le lancement, l'arrêt et le relancement des applications sont possibles uniquement à la connexion à l'appareil par les outils du Serveur d'administration.

Pour lancer, arrêter ou relancer une application, procédez comme suit :

1. Exécutez l'utilitaire de diagnostic à distance, puis connectez-vous à l'appareil requis, conformément aux explications du point "Connexion de l'utilitaire de diagnostic à distance à l'appareil client".
2. Dans l'arborescence des objets de l'appareil, sélectionnez l'application nécessaire.
3. Sélectionnez une action dans la partie gauche de la fenêtre de l'utilitaire de diagnostic à distance :
   - **Arrêter l'application**
   - **Relancer l'application**
   - **Lancer l'application**

Selon l'action sélectionnée, l'application sera lancée, arrêtée ou relancée.

Appareils protégés au niveau UEFI

Un *Appareil protégé au niveau UEFI* est un appareil avec une solution ou une application Kaspersky pour UEFI intégrée au niveau du BIOS. La protection intégrée assure la sécurité de l'appareil au début du lancement du système quand la protection des appareils qui ne sont pas dotés de l'application intégrée commence à fonctionner uniquement après le lancement de l'application de sécurité. Kaspersky Security Center prend en charge l'administration de ces appareils.

Pour modifier les paramètres de connexion des appareils protégés au niveau UEFI, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez l'entrée portant le nom du Serveur d'administration requis.
2. Dans le menu contextuel Serveur d'administration, sélectionnez l'option **Propriétés**.
3. Dans la fenêtre des propriétés du Serveur d'administration, choisissez la section **Paramètres de connexion au Serveur → Ports Supplémentaires**.
4. Dans la section **Ports supplémentaires**, modifiez les paramètres nécessaires :
   - Ouvrir le port pour les appareils protégés au niveau UEFI et KasperskyOS

     Les appareils protégés au niveau UEFI peuvent se connecter au Serveur d'administration.

   - Port pour les appareils protégés au niveau UEFI et KasperskyOS

     Vous pouvez modifier le numéro de port si l'option **Ouvrir le port pour les appareils protégés au niveau UEFI et KasperskyOS** est activée. Le numéro de port par défaut est 13294.
5. Cliquez sur le bouton **OK**.

Paramètres de l'appareil administré

Pour voir les paramètres de l'appareil administré :

1. Dans l'arborescence de la console sélectionnez le dossier **Appareils administrés**.
2. Dans l'espace de travail du dossier, sélectionnez un appareil.
3. Dans le menu contextuel de l'appareil, sélectionnez l'option **Propriétés**.

La fenêtre des propriétés de l'appareil sélectionné s'ouvre, avec la section **Général** sélectionnée.

Général

La section **Général** contient les informations générales sur l'appareil client. La boîte de dialogue affiche des informations mises à jour lors de la dernière synchronisation de l'appareil client avec le Serveur d'administration :

- **Nom**

  Champ à consulter et à modifier le nom de l'appareil client dans le groupe d'administration.

- **Description**

  Champ de saisie d'une description complémentaire de l'appareil client.

- **Domaine Windows**

  Domaine Windows ou groupe de travail auquel appartient l'appareil.

- **Nom NetBIOS**

  Nom de l'appareil client sur le réseau Windows.

- **Nom DNS**

  Nom du domaine DNS de l'appareil client.

- **Adresse IP**

  Adresse IP de l'appareil.

- **Groupe**

  Groupe d'administration contenant l'appareil client.

- **Dernière mise à jour**

  Date de la dernière mise à jour des bases antivirus ou des applications sur l'appareil.

- **Heure de la dernière connexion**

  Date et heure où l'appareil a été visible sur le réseau pour la dernière fois.

- **Connexion au Serveur d'administration**

  Date et heure de la dernière connexion de l'Agent d'administration installé sur l'appareil client au Serveur d'administration.

- **Maintenir la connexion au Serveur &d'administration**

  Si cette option est activée, la connectivité continue entre l'appareil administré et le Serveur d'administration est conservée. Vous pouvez utiliser cette option si vous n'utilisez pas des serveurs push, qui fournissent une telle connectivité.

  Si cette option est désactivée et les serveurs push ne sont pas utilisés, l'appareil administré se connecte uniquement au Serveur d'administration pour synchroniser les données ou transmettre des informations.

  Le total des appareils pour lesquels l'option **Maintenir la connexion au Serveur &d'administration** a été sélectionnée ne peut être supérieur à 300.

  Cette option est désactivée par défaut sur les appareils administrés. Cette option est activée par défaut sur l'appareil sur lequel le Serveur d'administration est installé et reste activée même si vous essayez de la désactiver.

Protection

La section **Protection** affiche des informations relatives à l'état actuel de la protection antivirus sur l'appareil client :

- **État de l'appareil**

  État de l'appareil client formé d'après les critères d'état de la protection antivirus et de l'activité réseau de l'appareil, tels que déterminés par l'administrateur.

- **Tous les problèmes**

  Ce tableau reprend la liste complète des problèmes détectés par les applications administrées installées sur l'appareil client. Chaque problème est accompagné d'un état que l'application recommande d'attribuer à l'appareil pour ce problème.

- **Protection en temps réel**

  État actuel de la protection en temps réel de l'appareil client.

  Quand l'état change sur l'appareil, le nouvel état est affiché dans la fenêtre des propriétés des appareils uniquement après la synchronisation de l'appareil client avec le Serveur d'administration.

- **Dernière analyse à la demande**

  Date et heure de la dernière analyse des logiciels malveillants sur l'appareil client.

- **Nombre total de détections de menaces**

  Nombre total de menaces détectées sur l'appareil client depuis l'installation de l'application de sécurité (première analyse de l'appareil) ou depuis la dernière remise à zéro du compteur.

- **Menaces actives**

  Nombre de fichiers non traités sur l'appareil client.

  Ce champ ne tient pas compte du nombre de fichiers non traités pour les appareils mobiles.

- **État de chiffrement des disques**

  État actuel de chiffrement des fichiers sur les disques locaux de l'appareil. Pour obtenir une description des états, consultez l'aide de Kaspersky Endpoint Security for Windows.

Applications

La section **Applications** affiche la liste des applications Kaspersky installées sur l'appareil client. Cette section contient le bouton Démarrer ( ) et le bouton d'arrêt ( ) qui permettent de lancer et d'arrêter l'application Kaspersky sélectionnée (à l'exception de l'Agent d'administration). Ces boutons sont activés si le port 15000 UDP est disponible sur l'appareil géré pour recevoir des notifications push du Serveur d'administration. Si l'appareil géré ne peut pas recevoir de notifications push, mais que le mode de connexion permanente au Serveur d'administration est activé (l'option **Maintenir la connexion au Serveur &d'administration** est activée dans la section **Général**), les boutons Démarrer et Arrêter sont également disponibles. La section **Applications** contient également les boutons suivants :

- **Événements**

  Le bouton qui permet de consulter la liste des événements survenus sur l'appareil client lors du fonctionnement de l'application, ainsi que les résultats d'exécution des tâches pour cette application.

- **Statistiques**

  Le bouton qui permet de consulter les statistiques actuelles sur le fonctionnement de l'application.

- **Propriétés**

  Le bouton qui permet d'obtenir les informations sur l'application et de configurer l'application.

Tâches

L'onglet **Tâches** permet d'administrer les tâches de l'appareil client : consulter la liste des tâches existantes, créer des tâches, supprimer, lancer ou suspendre des tâches, modifier leurs paramètres, consulter les résultats de l'exécution. La liste des tâches est fournie sur la base des données réceptionnées pendant la dernière session de synchronisation client avec le serveur d'administration. Le Serveur d'administration questionne l'appareil client au sujet de l'état courant de tâche.

Les boutons Démarrer ( ), Arrêter ( ) et Supprimer ( ) sont activés si le port 15000 UDP est disponible sur l'appareil géré pour recevoir des notifications push du Serveur d'administration. Si l'appareil géré ne peut pas recevoir de notifications push, mais que le mode de connexion permanente au Serveur d'administration est activé (l'option **Maintenir la connexion au Serveur &d'administration** est activée dans la section **Général**), les boutons Démarrer, Arrêter et Supprimer sont également disponibles.

Si la connexion n'est pas établie, l'état de la tâche n'est pas affiché et les boutons sont désactivés.

Événements

L'onglet **Événements** affiche les événements enregistrés sur le Serveur d'administration pour l'appareil client sélectionné.

Tags

L'onglet **Tags** permet d'administrer la liste des mots-clés utilisés pour effectuer la recherche d'appareils clients : consulter la liste des tags existants, désigner les tags de la liste, configurer des règles de désignation automatique des tags, ajouter de nouveaux tags, renommer d'anciens tags et supprimer des tags.

Informations sur le système

La section **Informations générales sur le système** fournit des informations relatives à l'application installée sur l'appareil client.

Registre des applications

La section **Registre des applications** permet de consulter le registre des applications installées sur l'appareil client, ainsi que leurs mises à jour, et de configurer l'affichage du registre des applications.

Les informations relatives aux applications installées sont présentées si l'Agent d'administration installé sur l'appareil client transmet les informations nécessaires au Serveur d'administration. Les paramètres de transfert des informations sur le Serveur d'administration peuvent être configurés dans la fenêtre des propriétés de l'Agent d'administration ou de sa stratégie, dans la section **Stockages**.

- **Afficher uniquement les applications de sécurité incompatibles**

  Si l'option est activée, la liste des applications affiche uniquement les applications de sécurité qui ne sont pas compatibles avec les applications de Kaspersky.

  Cette option est Inactif par défaut.

- **Afficher les mises à jour**

  Si l'option est activée, la liste des applications affiche non seulement les applications, mais aussi les paquets des mises à jour y installés.

  Pour afficher la liste des mises à jour, 100 Ko de trafic sont nécessaires. Si vous fermez la liste et la rouvrez, vous devrez à nouveau dépenser 100 Ko de trafic.

  Cette option est Inactif par défaut.

- **Exporter dans un fichier**

  Cliquez sur ce bouton pour exporter la liste des applications installées sur l'appareil vers un fichier CSV ou TXT.

- **Historique**

  Cliquez sur ce bouton pour afficher les événements liés à l'installation d'applications sur l'appareil. Les informations suivantes sont affichées :

  - Date et heure d'installation de l'application sur l'appareil
  - Nom de l'application
  - Version de l'application

- **Propriétés**

  Cliquez sur ce bouton pour afficher les propriétés de l'application sélectionnée dans la liste des applications installées sur l'appareil. Les informations suivantes sont affichées :

  - Nom de l'application
  - Version de l'application
  - Fournisseur de l'application

Fichiers exécutables

La section **Fichiers exécutables** affiche les fichiers exécutables détectés sur l'appareil client.

Registre du matériel

La section **Registre du matériel** permet de consulter les informations sur le matériel installé sur l'appareil client. Vous pouvez afficher ces informations pour les appareils Windows et Linux.

Assurez-vous que l'utilitaire lshw est installé sur les appareils Linux à partir desquels vous souhaitez récupérer les détails du matériel. Les détails du matériel récupérés depuis les machines virtuelles peuvent être incomplets en fonction de l'hyperviseur utilisé.

Si l'Agent d'administration est installé sur un appareil exécutant Windows, il envoie au Serveur d'administration les informations suivantes sur le matériel de l'appareil :

- Mémoire vive
- Appareils de stockage de masse
- Carte mère
- Processeur

- Adaptateurs réseau
- Surveillance
- Adaptateur vidéo
- Carte son

Si l'Agent d'administration est installé sur un appareil exécutant Linux ou macOS, il envoie au Serveur d'administration les informations suivantes sur le matériel de l'appareil, si ces informations sont fournies par le système d'exploitation :

- Volume total de mémoire vive
- Volume total des appareils de stockage de masse
- Carte mère
- Processeur
- Adaptateurs réseau

Sessions

La section **Sessions** s'affiche uniquement pour les appareils Windows et contient les informations sur le propriétaire de l'appareil client, ainsi que sur les comptes utilisateurs qui ont utilisé l'appareil client sélectionné.

Les informations sur les utilisateurs des domaines sont rédigées sur base des données d'Active Directory. Pour les utilisateurs locaux, les données proviennent de Windows Security Account Manager installé sur l'appareil client.

- **Propriétaire de l'appareil**

  Le champ **Propriétaire de l'appareil** contient le nom de l'utilisateur que l'administrateur peut contacter en cas d'impossibilité d'effectuer une action sur l'appareil client.

  Les boutons **Désigner** et **Propriétés** permettent de sélectionner le propriétaire de l'appareil et de consulter les informations sur l'utilisateur désigné comme propriétaire de l'appareil.

  Le bouton avec la croix rouge permet de supprimer le propriétaire actuel de l'appareil.

La liste contient comptes utilisateurs qui utilisent l'appareil client.

- **Nom**

  Nom de l'appareil dans le réseau.

- **Nom du participant**

  Nom d'utilisateur (domaine ou local) employé pour la connexion au système sur cet appareil.

- **Compte utilisateur**

  Compte utilisateur qui s'est connecté au système sur cet appareil.

- **Email**

  Adresse email de l'utilisateur.

- **Téléphone**

  Numéro de téléphone de l'utilisateur.

Problèmes de sécurité

L'onglet **Problèmes de sécurité** permet de consulter, de modifier et de créer des problèmes de sécurité pour l'appareil client. Les problèmes de sécurité peuvent être créés automatiquement, à l'aide des applications administrées de Kaspersky installées sur l'appareil client, ou manuellement par l'administrateur. Ainsi, si un utilisateur transfère toujours des applications malveillantes de son disque amovible personnel vers d'autres appareils, l'administrateur peut créer un problème de sécurité. L'administrateur peut fournir une brève description du cas et recommandés des actions, (comme des mesures disciplinaires à adopter contre un utilisateur) dans le texte du problème de sécurité et il peut ajouter un lien vers le ou les utilisateurs.

Un problème de sécurité pour lequel les actions nécessaires ont été exécutées est un problème *traité*. La présence de problèmes de sécurité non traités peut être sélectionnée comme condition pour faire passer l'état de l'appareil à *Critique* ou *Avertissement*.

La section contient la liste des problèmes de sécurité créés pour l'appareil. Les problèmes de sécurité sont classés par niveau de gravité et par type. C'est l'application Kaspersky qui crée le problème de sécurité qui en définit le type. Les problèmes de sécurité traités peuvent être identifiés dans la liste en cochant la case de la colonne **Traité**.

Vulnérabilités dans les applications

La section **Vulnérabilités dans les applications** permet de consulter les informations relatives aux vulnérabilités d'applications tierces installées sur les appareils clients. La barre de recherche en haut de la liste permet de rechercher des vulnérabilités sur la base de nom.

- **Exporter dans un fichier**

  Le bouton **Exporter dans un fichier** permet d'enregistrer la liste des vulnérabilités dans un fichier. Par défaut, l'application exporte la liste des vulnérabilités dans un fichier au format CSV.

- **Afficher uniquement les vulnérabilités qui peuvent être corrigées**

  Si l'option est activée, la section reprend les vulnérabilités qui peuvent être éliminées par un correctif.

  Si l'option est désactivée, la section reprend les vulnérabilités qui peuvent être éliminées par un correctif et celles pour lesquelles il n'existe pas de correctifs.

  Cette option est activée par défaut.

- **Propriétés**

  Sélectionnez une vulnérabilité logicielle dans la liste et cliquez sur le bouton **Propriétés** pour afficher les propriétés de la vulnérabilité dans l'application sélectionnée dans une fenêtre distincte. Dans la fenêtre, vous pouvez effectuer l'une des opérations suivantes :

  - Ignorer la vulnérabilité logicielle sur cet appareil administré (dans la Console d'administration ou dans la Kaspersky Security Center Web Console).
  - Afficher la liste des correctifs recommandés pour la vulnérabilité.
  - Spécifier manuellement les mises à jour logicielles permettant de corriger la vulnérabilité (dans la Console d'administration ou dans la Kaspersky Security Center Web Console).
  - Afficher les instances de vulnérabilité.
  - Afficher la liste des tâches existantes pour corriger la vulnérabilité et créer de nouvelles tâches pour corriger la vulnérabilité.

Mises à jour non installées

Cette section permet de consulter la liste des mises à jour du logiciel, non installées détectées sur l'appareil. Les informations sur les mises à jour facultatives de Microsoft Windows Update ne sont pas envoyées au Serveur d'administration.

- **Afficher les mises à jour installées**

  Si l'option est activée, la liste des mises à jour affiche aussi les mises à jour non installées et les mises à jour déjà installées sur l'appareil client.

  Cette option est Inactif par défaut.

Stratégies actives

Cette section affiche une liste des stratégies d'application Kaspersky actuellement attribuées à cet appareil.

- Exporter dans un fichier

  Le bouton **Exporter dans un fichier** permet d'enregistrer la liste des stratégies actives dans un fichier. Par défaut, l'application exporte la liste des stratégies dans un fichier au format CSV.

Profils de stratégies actifs

- Profils de stratégies actifs

  La liste permet de consulter les informations sur les profils de stratégie actifs sur les appareils clients. À l'aide du champ de recherche situé au-dessus de la liste, vous pouvez rechercher les profils de stratégie actuels par nom de stratégie ou par nom de profil de stratégie.

- Exporter dans un fichier

  Le bouton **Exporter dans un fichier** permet d'enregistrer la liste des profils de stratégie actifs dans un fichier. Par défaut, l'application exporte la liste des profils de stratégie dans un fichier au format CSV.

Points de distribution

Cette section présente la liste des points de distribution avec lesquels l'appareil interagit.

- Exporter dans un fichier

  Le bouton **Exporter dans un fichier** vous permet d'enregistrer dans le fichier la liste des points de distribution avec lesquels l'appareil interagit. Par défaut, l'application exporte la liste des appareils dans un fichier au format CSV.

- Propriétés

  Le bouton **Propriétés** vous permet de consulter et de configurer les paramètres du point de distribution avec lequel l'appareil interagit.

Paramètres généraux de la stratégie

Général

La section **Général** permet de modifier l'état de la stratégie et de configurer l'héritage des paramètres de la stratégie :

- Le groupe **État de la stratégie** permet de sélectionner l'un des modes de stratégie :
  - Stratégie active

    Si cette option a été sélectionnée, la stratégie devient active.

    Cette option est sélectionnée par défaut.

  - Stratégie pour les utilisateurs autonomes

    Si cette option a été sélectionnée, la stratégie agit lorsque l'appareil est déconnecté du réseau de l'entreprise.

  - Stratégie inactive

    Si cette option a été sélectionnée, la stratégie devient inactive, mais elle est conservée dans le dossier **Stratégies**. Elle pourra être activée en fonction des besoins.

- Le groupe de paramètres **Héritage des paramètres** permet de configurer l'héritage de la stratégie :
  - Hériter les paramètres de la stratégie parent

    Si cette option est activée, les valeurs des paramètres de la stratégie sont héritées depuis la stratégie du groupe de niveau supérieur et sont verrouillées.

    Cette option est activée par défaut.

  - &Imposer l'héritage des paramètres aux stratégies enfants

    Une fois que les modifications dans la stratégie sont appliquées, les opérations suivantes sont exécutées :

    - Les valeurs des paramètres de la stratégie seront diffusées dans les stratégies des sous-groupes d'administration, dans les stratégies enfant.
    - Dans le bloc **Héritage des paramètres** de la section **Général** de la fenêtre des propriétés de chaque stratégie enfant, la case **Hériter des paramètres de la stratégie parent** est automatiquement cochée.

    Quand la case est cochée, les valeurs des paramètres des stratégies enfants sont verrouillées.

    Cette option est Inactif par défaut.

Configuration de l'événement

La section **Configuration de l'événement** permet de configurer l'enregistrement des événements dans le journal et les notifications relatives à ceux-ci. Les événements sont répartis par niveau d'importance sur différents onglets :

- **Critique**

  L'onglet **Critique** ne s'affiche pas dans les propriétés de la stratégie de l'Agent d'administration.

- **Erreur de fonctionnement**
- **Avertissement**
- **Information**

Sous chaque onglet, la liste des événements reprend les types d'événements et la condition de conservation sur le serveur d'administration par défaut (en jours). Un clic sur le bouton **Propriétés** permet de définir les paramètres d'enregistrement des événements dans le journal et de notification des événements sélectionnés dans la liste. Par défaut, les paramètres de notification courants spécifiés pour l'ensemble du Serveur d'administration servent pour tous les types d'événements. Cependant, vous pouvez modifier des paramètres spécifiques aux types d'événements requis.

Par exemple, sur le **Avertissement** onglet, vous pouvez configurer le type d'événement **Un problème de sécurité est survenu**. De tels événements peuvent se produire, par exemple, lorsque le espace disque libre d'un point de distribution est inférieure à 2 Go (au moins 4 Go sont nécessaires pour installer des applications et télécharger des mises à jour à distance). Pour configurer l'événement **Un problème de sécurité est survenu**, sélectionnez-le et cliquez sur le bouton **Propriétés**. Après cela, vous pouvez spécifier où stocker les événements survenus et comment les notifier.

Si l'Agent d'administration a détecté un problème de sécurité, vous pouvez gérer ce problème en utilisant les paramètres d'un appareil administré.

Pour sélectionner plusieurs types d'événements, utilisez les touches **Shift** ou **Ctrl** et pour sélectionner tous les types, utilisez le bouton **Tout sélectionner**.

Paramètres de la stratégie de l'Agent d'administration

Pour configurer les paramètres de la stratégie de l'Agent d'administration, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le dossier **Stratégies**.
2. Dans l'espace de travail du dossier, choisissez la stratégie de l'Agent d'administration.
3. Dans le menu contextuel de la stratégie, sélectionnez l'option **Propriétés**.

La fenêtre des propriétés de la stratégie de l'Agent d'administration s'ouvre.

Consultez le tableau comparatif détaillant comment les paramètres ci-dessous s'appliquent, en fonction du type de système d'exploitation utilisé.

Général

La section **Général** permet de modifier l'état de la stratégie et de configurer l'héritage des paramètres de la stratégie :

- Le groupe **État de la stratégie** permet de sélectionner l'un des modes de stratégie :
  - Stratégie active

    Si cette option a été sélectionnée, la stratégie devient active.

    Cette option est sélectionnée par défaut.

  - Stratégie pour les utilisateurs autonomes

    Si cette option a été sélectionnée, la stratégie agit lorsque l'appareil est déconnecté du réseau de l'entreprise.

  - Stratégie inactive

    Si cette option a été sélectionnée, la stratégie devient inactive, mais elle est conservée dans le dossier **Stratégies**. Elle pourra être activée en fonction des besoins.

- Le groupe de paramètres **Héritage des paramètres** permet de configurer l'héritage de la stratégie :
  - Hériter les paramètres de la stratégie parent

    Si cette option est activée, les valeurs des paramètres de la stratégie sont héritées depuis la stratégie du groupe de niveau supérieur et sont verrouillées.

    Cette option est activée par défaut.

  - &Imposer l'héritage des paramètres aux stratégies enfants

    Une fois que les modifications dans la stratégie sont appliquées, les opérations suivantes sont exécutées :
    - Les valeurs des paramètres de la stratégie seront diffusées dans les stratégies des sous-groupes d'administration, dans les stratégies enfant.
    - Dans le bloc **Héritage des paramètres** de la section **Général** de la fenêtre des propriétés de chaque stratégie enfant, la case **Hériter des paramètres de la stratégie parent** est automatiquement cochée.

    Quand la case est cochée, les valeurs des paramètres des stratégies enfants sont verrouillées.

    Cette option est Inactif par défaut.

Configuration de l'événement

La section **Configuration de l'événement** permet de configurer l'enregistrement des événements dans le journal et les notifications relatives à ceux-ci. Les événements sont répartis par niveau d'importance sur différents onglets :

- **Critique**

  L'onglet **Critique** ne s'affiche pas dans les propriétés de la stratégie de l'Agent d'administration.

- **Erreur de fonctionnement**
- **Avertissement**
- **Information**

Sous chaque onglet, la liste des événements reprend les types d'événements et la condition de conservation sur le serveur d'administration par défaut (en jours). Un clic sur le bouton **Propriétés** permet de définir les paramètres d'enregistrement des événements dans le journal et de notification des événements sélectionnés dans la liste. Par défaut, les paramètres de notification courants spécifiés pour l'ensemble du Serveur d'administration servent pour tous les types d'événements. Cependant, vous pouvez modifier des paramètres spécifiques aux types d'événements requis.

Par exemple, sur le **Avertissement** onglet, vous pouvez configurer le type d'événement **Un problème de sécurité est survenu**. De tels événements peuvent se produire, par exemple, lorsque le espace disque libre d'un point de distribution est inférieure à 2 Go (au moins 4 Go sont nécessaires pour installer des applications et télécharger des mises à jour à distance). Pour configurer l'événement **Un problème de sécurité est survenu**, sélectionnez-le et cliquez sur le bouton **Propriétés**. Après cela, vous pouvez spécifier où stocker les événements survenus et comment les notifier.

Si l'Agent d'administration a détecté un problème de sécurité, vous pouvez gérer ce problème en utilisant les paramètres d'un appareil administré.

Pour sélectionner plusieurs types d'événements, utilisez les touches **Shift** ou **Ctrl** et pour sélectionner tous les types, utilisez le bouton **Tout sélectionner**.

Paramètres

La section **Paramètres** vous permet de configurer les paramètres de la stratégie de l'Agent d'administration :

- **Distribuer les fichiers uniquement via les points de distribution**

  Si cette option est activée, les agents d'administration sur les Appareils administrés récupèrent les mises à jour à partir des points de distribution uniquement.

  Si cette option est désactivée, les agents d'administration sur les appareils administrés récupèrent les mises à jour des points de distribution ou du Serveur d'administration.

  > Notez que les applications de sécurité sur les Appareils administrés récupèrent les mises à jour sur la source définie dans la tâche de mise à jour pour chaque application de sécurité. Si vous activez l'option **Distribuer les fichiers uniquement via les points de distribution**, assurez-vous que Kaspersky Security Center est défini comme source des mises à jour dans les tâches de mise à jour.

  Cette option est Inactif par défaut.

- **Taille maximale de la file d'attente d'événements (Mo)**

  Le champ permet d'indiquer l'espace maximal sur le disque, que la file d'attente d'événements peut occuper.

  La valeur par défaut est égale à 2 Mo.

- **&L'application est autorisée à récupérer des données étendues de stratégie sur l'appareil**

  L'Agent d'administration installé sur un appareil administré transfère des informations sur la stratégie d'application de sécurité appliquée à l'application de sécurité (par exemple, Kaspersky Endpoint Security for Windows). Vous pouvez afficher les informations transférées dans l'interface de l'application de sécurité.

  L'Agent d'administration transfère les informations suivantes :

  - Heure de remise de la stratégie à l'appareil administré.
  - Nom de la stratégie active au moment de la remise de la stratégie à l'appareil administré.
  - Nom de la stratégie pour les utilisateurs autonomes au moment de la remise de la stratégie à l'appareil administré (non disponible pour l'Agent d'administration pour Linux).
  - Nom et chemin d'accès complet au groupe d'administration qui contenait l'appareil administré au moment de la remise de la stratégie à l'appareil administré.
  - Liste des profils de stratégie actifs avec leurs noms et priorités au moment de la livraison de la stratégie à l'appareil administré.

  Vous pouvez utiliser les informations pour vous assurer que la bonne stratégie est appliquée à l'appareil et à des fins d'élimination des défaillances. Cette option est Inactif par défaut.

- **Protéger le service de l'Agent &d'administration contre la suppression ou l'arrêt non autorisé et empêcher la modification des paramètres**

  Lorsque cette option est activée, après l'installation de l'Agent d'administration sur un appareil administré, le module ne peut pas être supprimé ou reconfiguré sans les privilèges requis. Il est impossible d'arrêter le service de l'Agent d'administration. Cette option n'a aucun effet sur les contrôleurs de domaine.

  Activez cette option pour protéger l'Agent d'administration sur les postes de travail exploités avec des privilèges d'administrateur local.

  Cette option est Inactif par défaut.

- **Utiliser un mot de passe de désinstallation**

  Si cette option est activée, à l'aide du bouton **Modifier** vous pouvez indiquer le mot de passe pour l'utilitaire klmover et la désinstallation à distance de l'Agent d'administration.

  Cette option est Inactif par défaut.

Stockages

La section **Stockages** permet de sélectionner les types des objets dont les informations seront envoyées sur le Serveur d'administration par l'Agent d'administration :

- **Détails sur les mises à jour Windows Update**

  Si cette option est activée, les informations sur les mises à jour Microsoft Windows qui doivent être installées sur les appareils clients sont envoyées au Serveur d'administration.

  Parfois, même si l'option est désactivée, les mises à jour sont affichées dans les propriétés de l'appareil dans la section **Mises à jour disponibles**. Cela peut se produire si, par exemple, les appareils de l'organisation présentent des vulnérabilités qui pourraient être corrigées par ces mises à jour.

  Cette option est activée par défaut. Il est disponible uniquement pour Windows.

  Les informations sur les mises à jour facultatives de Microsoft Windows Update ne sont pas envoyées au Serveur d'administration.

- **Détails sur les vulnérabilités dans les applications et les mises à jour correspondantes**

  Si cette option est activée, les informations sur les vulnérabilités des logiciels tiers (y compris les logiciels Microsoft), détectées sur les appareils administrés, et sur les mises à jour du logiciel destinées à corriger les vulnérabilités des logiciels tiers (à l'exception des logiciels Microsoft) sont envoyées au Serveur d'administration.

  La sélection de cette option (**Détails sur les vulnérabilités dans les applications et les mises à jour correspondantes**) augmente la charge du réseau, la charge du disque du Serveur d'administration et la consommation des ressources de l'Agent d'administration.

  Cette option est activée par défaut. Il est disponible uniquement pour Windows.

  Pour administrer les mises à jour des logiciels Microsoft, utilisez l'option **Détails sur les mises à jour Windows Update**.

- **Informations sur le registre du matériel**

  L'Agent d'administration installé sur un appareil envoie des informations sur le matériel de l'appareil au Serveur d'administration. Vous pouvez consulter les détails sur le matériel dans les propriétés de l'appareil.

  Assurez-vous que l'utilitaire lshw est installé sur les appareils Linux à partir desquels vous souhaitez récupérer les détails du matériel. Les détails du matériel récupérés depuis les machines virtuelles peuvent être incomplets en fonction de l'hyperviseur utilisé.

- **Détails sur les applications installées**

  Si l'option est activée, les informations sur les applications installées sur les appareils clients sont envoyées au Serveur d'administration.

  Cette option est activée par défaut.

- **Inclure les informations sur les correctifs**

  Les informations sur les correctifs des applications installées sur les appareils clients sont envoyées au Serveur d'administration. L'activation de cette option peut augmenter la charge sur le Serveur d'administration et le SGBD, et causer une augmentation du volume de la base de données.

  Cette option est activée par défaut. Il est disponible uniquement pour Windows.

Si la stratégie de l'Agent d'administration bloque la modification ce certains paramètres de cette section, vous ne pouvez pas modifier ceux-ci.

Mises à jour et vulnérabilités du logiciel

La section **Mises à jour et vulnérabilités du logiciel** permet de configurer la recherche et la distribution des mises à jour Windows et de rechercher les vulnérabilités parmi les fichiers exécutables :

- **&Utiliser le Serveur d'administration comme serveur WSUS**

  Si l'option est activée, les mises à jour Windows sont téléchargées sur le Serveur d'administration. Le Serveur d'administration présente de manière centralisée les mises à jour téléchargées aux services Windows Update sur les appareils clients à l'aide des Agents d'administration.

  Si l'option est désactivée, le Serveur d'administration n'est pas utilisé pour télécharger les mises à jour Windows. Le cas échéant, les appareils clients reçoivent les mises à jour Windows de manière autonome.

  Cette option est Inactif par défaut.

- La section **Autoriser les utilisateurs à administrer l'installation des mises à jour Windows Update** permet de limiter les mises à jour Windows que les utilisateurs peuvent installer sur leurs appareils manuellement à l'aide de Windows Update.

  Sur les appareils exécutés sous Windows 10, si Windows Update a déjà trouvé des mises à jour pour l'appareil, la nouvelle option que vous sélectionnez sous **Autoriser les utilisateurs à gérer l'installation des mises à jour de Windows Update** ne sera appliquée qu'une fois les mises à jour installées.

  Sélectionnez une option dans la liste déroulante :

  - **Autoriser les utilisateurs à installer toutes les mises à jour Windows Update applicables**

    Les utilisateurs peuvent installer toutes les mises à jour Microsoft Windows Update applicables à leurs appareils.

    Sélectionnez cette option si vous ne voulez pas exécuter l'installation de contrôle des mises à jour.

    Lorsque l'utilisateur installe des mises à jour Microsoft Windows Update manuellement, les mises à jour peuvent être téléchargées depuis les serveurs de Microsoft au lieu des Serveurs d'administration. Ceci est possible si le Serveur d'administration n'a pas encore téléchargé ces mises à jour. Le téléchargement des mises à jour depuis les serveurs de Microsoft génère un trafic supplémentaire.

  - **Autoriser les utilisateurs à installer uniquement les mises à jour Windows Update autorisées**

Les utilisateurs peuvent installer toutes les mises à jour Microsoft Windows Update applicables à leurs appareils et que vous avez approuvées.

Par exemple, vous souhaitez d'abord vérifier l'installation des mises à jour dans un environnement d'essai et vous assurer qu'elles ne perturbent pas le fonctionnement des appareils avant d'autoriser l'installation de ces mises à jour confirmées sur les appareils clients.

Lorsque l'utilisateur installe des mises à jour Microsoft Windows Update manuellement, les mises à jour peuvent être téléchargées depuis les serveurs de Microsoft au lieu des Serveurs d'administration. Ceci est possible si le Serveur d'administration n'a pas encore téléchargé ces mises à jour. Le téléchargement des mises à jour depuis les serveurs de Microsoft génère un trafic supplémentaire.

- **Ne pas autoriser les utilisateurs à installer les mises à jour Windows Update**

  Les utilisateurs ne peuvent pas installer manuellement les mises à jour Microsoft Windows Update sur leurs appareils. Toutes les mises à jour applicables sont installées selon votre configuration.

  Choisissez cette option, si vous voulez administrer centralement l'installation des mises à jour.

  Par exemple, il se peut que vous souhaitiez optimiser la programmation des mises à jour afin de ne pas surcharger le réseau. Vous pouvez programmer les mises à jour en dehors des heures de travail afin qu'elles n'interfèrent pas avec la productivité de l'utilisateur.

- Le groupe de paramètres **Mode de recherche des mises à jour Windows Update** permet de sélectionner le mode de recherche des mises à jour :

  - **Actif**

    Si cette option a été sélectionnée, le Serveur d'administration à l'aide de l'Agent d'administration initie la demande de l'Agent de mises à jour Windows sur l'appareil client à la source des mises à jour : Windows Update Servers or WSUS. Ensuite, l'Agent d'administration transmet sur le Serveur d'administration les informations obtenues en provenance de l'Agent de mises à jour Windows.

    L'option ne prend effet que si l'option **Se connecter au serveur de mise à jour pour mettre à jour les données** de la tâche *Recherche de vulnérabilités et de mises à jour requises* est sélectionnée.

    Cette option est sélectionnée par défaut.

  - **Passif**

    Si cette option a été sélectionnée, l'Agent d'administration transmet périodiquement sur le Serveur d'administration les informations sur les mises à jour obtenues lors de la dernières synchronisation de l'Agent de mises à jour Windows avec la source des mises à jour. Si la synchronisation de l'Agent de mises à jour Windows avec la source des mises à jour n'est pas exécutée, les données sur les mises à jour sur le Serveur d'administration vieillissent.

    Sélectionnez cette option si vous souhaitez obtenir des mises à jour à partir du cache mémoire de la source des mises à jour.

  - **Désactivé**

    Si cette option a été sélectionnée, le Serveur d'administration ne formule aucune requête d'informations sur les mises à jour.

    Sélectionnez cette option si, par exemple, vous souhaitez d'abord tester les mises à jour sur votre appareil local.

- **Analyser les fichiers exécutables à la recherche de vulnérabilités lors du lancement**

  Si cette option est activée, lors du lancement des fichiers exécutables, leur analyse sur la présence des vulnérabilités est exécutée.

  Cette option est activée par défaut.

Administration du redémarrage

Dans la section **Administration du redémarrage**, vous pouvez définir l'action à exécuter si le système d'exploitation d'un appareil administré doit être redémarré en vue d'une utilisation, d'une installation ou une désinstallation correctes d'une application :

- **Ne pas redémarrer le système d'exploitation**

  Le système d'exploitation ne sera pas redémarré.

- **Redémarrer le système d'exploitation automatiquement si nécessaire**

  Le système d'exploitation sera automatiquement redémarré si nécessaire.

- **Confirmer l'action auprès de l'utilisateur**

  L'application demandera à l'utilisateur d'autoriser le redémarrage du système d'exploitation.

  Cette option est sélectionnée par défaut.

  - **Répéter la demande toutes les (min)**

    Si l'option est activée, l'application invite l'utilisateur à autoriser le redémarrage du système d'exploitation à la fréquence indiquée dans le champ situé à côté de la case. Par défaut, la fréquence de répétition est fixée à 5 minutes.

    Si l'option est désactivée, l'application ne redemande pas l'autorisation de redémarrer le système d'exploitation plusieurs fois.

    Cette option est activée par défaut.

  - **Forcer le redémarrage au bout de (min.)**

    Si l'option est activée, après interrogation de l'utilisateur, le redémarrage forcé du système d'exploitation aura lieu à la fin du délai indiqué dans le champ situé à côté de la case.

    Si l'option est désactivée, il n'y aura pas de redémarrage forcé.

    Cette option est activée par défaut.

  - **Délai d'attente avant la fermeture forcée des ap&plications dans les sessions bloquées (min)**

    Arrêt forcé des applications lorsque l'appareil de l'utilisateur est verrouillé (arrêt manuel ou automatique après une période d'inactivité).

    Si cette option est activée, les applications en cours sur l'appareil verrouillé seront fermées de force à la fin du délai indiqué dans le champ situé à côté de la case.

    Si cette option est activée, les applications en cours sur l'appareil verrouillé ne seront pas fermées.

    Cette option est Inactif par défaut.

Partage du bureau Windows

La section **Partage du bureau Windows** permet d'activer et de configurer l'audit des actions de l'administrateur sur un appareil distant quand l'accès au bureau est partagé :

- **&Activer l'audit**

  Si cette option est activée, l'audit des actions de l'administrateur sur l'appareil distant est activé. Les enregistrements des actions de l'administrateur sur l'appareil distant sont conservés :

  - Dans le journal des événements de l'appareil distant
  - Dans un fichier .syslog, situé dans le dossier d'installation de l'Agent d'administration sur l'appareil distant
  - Dans la base des événements du Kaspersky Security Center

  L'audit des actions de l'administrateur est accessible lorsque les conditions suivantes sont réunies :

  - La licence pour le fonctionnement de Gestion des vulnérabilités et des correctifs est en cours d'utilisation
  - L'administrateur est autorisé à lancer l'accès partagé au bureau de l'appareil distant

  Si cette option est désactivée, l'audit des actions de l'administrateur sur l'appareil distant est désactivé.

  Cette option est Inactif par défaut.

- **Masques de fichiers à suivre en cas de lecture**

  La liste contient des masques de fichiers. Lorsque l'audit est activé, l'application suit les fichiers lus par l'administrateur qui correspondent à ces masques et elle enregistre les informations relatives aux fichiers lus. La liste n'est accessible que si la case **Activer l'audit** est cochée. Il est possible de modifier les masques de fichiers et d'en ajouter à la liste. Les nouveaux masques de fichiers doivent être ajoutés sur une nouvelle ligne.

  Par défaut, les masques de fichiers indiqués sont : *.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt et *.pdf.

- **Masques de fichiers à suivre en cas de modification**

  La liste contient les masques des fichiers de l'appareil distant. Lorsque l'audit est activé, l'application suit les fichiers modifiés par l'administrateur qui correspondent à ces masques et elle enregistre les informations relatives aux fichiers modifiés. La liste n'est accessible que si la case **Activer l'audit** est cochée. Il est possible de modifier les masques de fichiers et d'en ajouter à la liste. Les nouveaux masques de fichiers doivent être ajoutés sur une nouvelle ligne.

  Par défaut, les masques de fichiers indiqués sont : *.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt et *.pdf.

Administration des correctifs et des mises à jour

Dans la section **Administration des correctifs et des mises à jour**, vous pouvez configurer la réception et la diffusion des mises à jour et l'installation des correctifs vers les appareils administrés :

- **Installer automatiquement les mises à jour et les correctifs nécessaires pour les modules dont l'état est Non défini**

  Si la case est Activé, les correctifs de Kaspersky avec l'état d'approbation *Non défini* s'installent automatiquement sur les appareils administrés juste après avoir été téléchargés depuis les serveurs de mises à jour.

  Si l'option est désactivée, les correctifs de Kaspersky chargés avec l'état *Non défini* sont installés après que l'administrateur a modifié leur état pour qu'il soit *Approuvé*.

  Cette option est activée par défaut.

- **&Télécharger au préalable les mises à jour et les bases antivirus depuis le Serveur d'administration (recommandé)**

  Si la case est Activé, le modèle hors ligne de téléchargement des mises à jour est désactivé. Quand le serveur d'administration reçoit des mises à jour, il signale à l'Agent d'administration (sur les appareils où il est installé) les mises à jour qui seront requises pour les applications administrées. Quand l'Agent d'administration reçoit des informations sur les mises à jour, il télécharge les fichiers nécessaires au préalable sur le Serveur d'administration. Lors de la première connexion à Agent d'administration, le Serveur d'administration initialise le téléchargement des mises à jour. Une fois que l'Agent d'administration sur l'appareil client a téléchargé toutes les mises à jour, celles-ci deviennent accessibles aux applications situées sur ce même appareil.

  Lorsque l'application administrée sur l'appareil client s'adresse à l'Agent d'administration pour obtenir des mises à jour, l'Agent vérifie s'il a les mises à jour nécessaires. Si des mises à jour ont été reçues du Serveur d'administration au plus tôt 25 heures après la requête de l'application administrée, l'Agent d'administration ne se connecte pas au Serveur d'administration et fournit à l'application administrée des mises à jour du cache local. Il se peut que la connexion au Serveur d'administration ne soit pas établie lorsque l'Agent d'administration fournit les mises à jour aux applications sur les appareils client, mais la connexion n'est pas requise pour la mise à jour.

  Si l'option est désactivée, le modèle hors ligne de téléchargement des mises à jour n'est pas utilisé. Les mises à jour sont distribuées conformément à la programmation de la tâches de téléchargement des mises à jour.

  Cette option est activée par défaut.

Connectivité

La section **Connectivité** inclut trois sous-sections imbriquées :

- **Réseau**
- **Profils de connexion** (uniquement pour Windows et macOS)
- **Calendrier de connexion**

La sous-section **Réseau** permet de configurer les paramètres de connexion au Serveur d'administration, d'activer l'utilisation du port UDP et d'indiquer son numéro. Les options suivantes sont proposées :

- Dans le groupe de paramètres **Connexion au Serveur d'administration**, vous pouvez configurer les paramètres de connexion au Serveur d'administration et indiquer l'intervalle de synchronisation des appareils clients avec le Serveur d'administration :

  - Compresser le trafic réseau

    Si cette option est activée, la vitesse de transfert des données de l'Agent d'administration sera augmentée, le volume des informations transmises sera réduit et la charge sur le Serveur d'administration sera diminuée.

    La charge sur le processeur central de l'ordinateur client peut augmenter.

    Cette case est cochée par défaut.

  - &Ouvrir les ports de l'Agent d'administration dans le pare-feu Microsoft Windows

    Si l'option est activée, les ports, indispensables au bon fonctionnement de l'Agent d'administration, sont ajoutés à la liste des exclusions du pare-feu Microsoft Windows.

    Cette option est activée par défaut.

  - Utiliser SSL

    Si l'option est activée, la connexion au Serveur d'administration est établie via le port sécurisé à l'aide du protocole SSL.

    Cette option est activée par défaut.

  - Utiliser la passerelle de connexion sur le point de distribution (le cas échéant) dans les paramètres de connexion par défaut

    Si l'option est activée, la passerelle de connexion du point de distribution est utilisée avec les paramètres spécifiés par les propriétés du groupe d'administration.

    Cette option est activée par défaut.

- Utiliser un port UDP

  Si vous avez besoin que l'Agent d'administration se connecte au Serveur d'administration via un port UDP, activez l'option **Utiliser le port UDP** et indiquez le **Numéro de port UDP**. Cette option est activée par défaut. Par défaut, la connexion au Serveur d'administration est exécutée via le port UDP 15000.

- **Port UDP**

  Champ à saisir le numéro du port UDP. Le numéro de port par défaut est 15000.

  La forme d'écriture décimale est utilisée.

  Si un appareil client fonctionne sous le système d'exploitation Windows XP Service Pack 2, le pare-feu incorporé verrouillera le port UDP 15000. Ce port doit être ouvert à la main.

- **Utiliser le point de distribution pour forcer la connexion au Serveur d'administration**

  Sélectionnez cette option si vous avez sélectionné l'option **Utiliser ce point de distribution comme serveur push** dans la fenêtre des paramètres du point de distribution. Sinon, le point de distribution n'agira pas comme un serveur push.

La section **Profils de connexion** permet d'indiquer les paramètres d'emplacement réseau, de configurer les profils de connexion au Serveur d'administration, d'activer le mode de l'utilisateur autonome quand le Serveur d'administration n'est pas disponible.

- **Paramètres d'emplacement réseau**

  Les paramètres d'emplacement réseau définissent les caractéristiques du réseau auquel l'appareil client est connecté et spécifient les règles de commutation de l'Agent d'administration d'un profil de connexion du Serveur d'administration sur l'autre en cas de modification des caractéristiques du réseau.

- **Profils de connexion au Serveur d'administration**

  Cette section permet de consulter et d'ajouter des profils de connexion de l'Agent d'administration au Serveur d'administration. Cette section permet également de rédiger des règles de déplacement de l'Agent d'administration vers un autre Serveur d'administration si les événements suivants se produisent :

  - Connexion de l'appareil client à un autre réseau local
  - Déconnexion de l'appareil du réseau local de l'organisation
  - Modification de l'adresse de la passerelle de connexion ou modification de l'adresse du serveur DNS

  Les profils des connexions ne sont pris en charge que pour les appareils fonctionnant sous Windows et macOS.

- **Activer le mode de l'utilisateur autonome quand le Serveur d'administration n'est pas disponible**

  Si l'option est activée, en cas de connexion via ce profil, les applications installées sur l'appareil client vont utiliser les profils de stratégie pour les appareils qui se trouvent en mode de l'utilisateur autonome et les stratégies pour utilisateurs autonomes. Si aucune stratégie pour les utilisateurs autonomes n'est définie pour l'application, c'est la stratégie active qui sera utilisée.

  Si l'option est activée, les applications utiliseront les stratégies actives.

  Cette option est Inactif par défaut.

La sous-section **Calendrier de connexion** vous permet d'indiquer les intervalles de temps pendant lesquels l'Agent d'administration va transférer les données sur le Serveur d'administration :

- **Se connecter en cas de nécessité**

  Si cette option a été sélectionnée, la connexion s'établira quand l'Agent d'administration devra transférer les données sur le Serveur d'administration.

  Cette option est sélectionnée par défaut.

- **Se connecter aux intervalles indiqués**

  Si cette option a été sélectionnée, la connexion de l'Agent d'administration au Serveur d'administration est effectuée dans les intervalles indiqués. Plusieurs périodes de connexions peuvent être ajoutées.

Points de distribution

La section **Points de distribution** inclut quatre sous-sections imbriquées :

- **Sondages du réseau**
- **Paramètres de connexion à Internet**
- **Proxy KSN**
- **Mises à jour**

La sous-section **Sondages du réseau** permet de configurer le sondage automatique du réseau. Vous pouvez activer trois types de sondage, à savoir le sondage réseau, le sondage de plage IP et le sondage Active Directory :

- **Autoriser le sondage du réseau**

  Si l'option est activée, le Serveur d'administration sonde automatiquement le réseau en respectant la planification défini en cliquant sur les liens **Planifier le sondage rapide** et **Planifier le sondage complet**.

  Si cette option est désactivée, le Serveur d'administration sonde le réseau à l'intervalle indiqué dans le champ **Fréquence des sondages du réseau (min.)**.

  L'intervalle de recherche d'appareils pour les versions de l'Agent d'administration antérieures à 10.2 peut être configuré dans les champs **Fréquence des sondages des domaines Windows (min.)** (pour un sondage rapide du réseau Windows) et **Fréquence des sondages du réseau (min.)** (pour un sondage complet du réseau Windows).

  Cette option est Inactif par défaut.

- **Autoriser le sondage de la plage IP**

  Si l'option est activée, le point de distribution sonde automatiquement les plages IP en fonction de planification que vous avez configurée en cliquant sur le bouton **Planifier le sondage**.

  Si cette option est désactivée, le point de distribution ne sonde pas les plages IP.

  La fréquence de sondage des plages IP pour les versions de l'Agent d'administration antérieures à la version 10.2 peut être configurée dans le champ **Période de sondage (min.)**. Le champ est disponible si l'option est activée.

  Cette option est Inactif par défaut.

- **Utilisez &Zeroconf polling (sur les plateformes Linux uniquement ; les plages d'adresses IP spécifiées manuellement seront ignorées)**

  Si cette option est activée, le point de distribution sonde automatiquement le réseau avec les appareils IPv6 en utilisant la mise en réseau sans configuration (également appelé *Zeroconf*). Dans ce cas, le sondage de plage IP activé est ignoré, car le point de distribution sonde l'ensemble du réseau.

  Pour commencer à utiliser Zeroconf, les conditions suivantes doivent être remplies :

  - Le point de distribution doit exécuter Linux.
  - Vous devez installer l'utilitaire avahi-browse sur le point de distribution.

  Si cette option est désactivée, le point de distribution ne sonde pas les réseaux avec des appareils IPv6.

  Cette option est Inactif par défaut.

- **Autoriser le sondage d'Ac&tive Directory**

  Si l'option est activée, le point de distribution sonde automatiquement Active Directory en fonction de la configuration définie en cliquant sur le lien **Planifier le sondage**.

  Si cette option est désactivée, le Serveur d'administration ne sonde pas Active Directory.

  La fréquence de sondage d'Active Directory pour les versions de l'Agent d'administration antérieures à la version 10.2 est définie dans le champ **Période de sondage (min.)**. Le champ est disponible si l'option est activée.

  Cette option est Inactif par défaut.

Si vos points de distribution utilisent un serveur proxy pour se connecter à Internet, vous pouvez renseigner les paramètres suivants dans la sous-section **Paramètres de connexion Internet** :

- **Utiliser un serveur proxy**

  Si la case est cochée, le champ de saisie permet de configurer la connexion au serveur proxy.

  Celle-ci est décochée par défaut.

- **Adresse du serveur proxy**

  Adresse du serveur proxy.

- **Numéro de port**

  Numéro du port utilisé pour la connexion.

- **Ne pas utiliser le serveur proxy pour les adresses locales**

  Si cette option est activée, le serveur proxy ne sera pas utilisé lors de la connexion aux appareils sur le réseau local.

  Cette option est Inactif par défaut.

- **Authentification du serveur proxy**

  Si la case est cochée, les champs de saisie permettent d'indiquer les identifiants pour l'authentification sur le serveur proxy.

  Celle-ci est décochée par défaut.

- **Nom d'utilisateur**

  Le compte utilisateur au nom duquel la connexion au serveur proxy sera effectuée.

- **Mot de passe**

  Mot de passe du compte utilisateur au nom duquel la tâche sera lancée.

Dans la sous-section **Proxy KSN**, vous pouvez configurer l'application pour utiliser le point de distribution afin de transmettre les requêtes KSN depuis les appareils administrés :

- **Activer le proxy KSN du côté du point de distribution**

  Le service KSN proxy est exécuté sur l'appareil qui est utilisé en tant que points de distribution. Utilisez cette fonction pour rediffuser et optimiser le trafic sur le réseau.

  Le point de distribution envoie les statistiques KSN, lesquelles sont répertoriées dans la Déclaration de Kaspersky Security Network, à Kaspersky. Par défaut, la Déclaration KSN se trouve dans %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\ksneula.

  Cette option est Inactif par défaut. L'activation de cette option prend effet uniquement si les options **Utiliser le Serveur d'administration comme serveur proxy** et **J'accepte les termes du Kaspersky Security Network** sont activées dans la fenêtre Propriétés du Serveur d'administration.

  Vous pouvez affecter un nœud d'un cluster actif-passif à un point de distribution et activer le serveur proxy KSN sur ce nœud.

- **&Transférer les demandes KSN au Serveur d'administration**

  Le point de distribution transfère les requêtes KSN depuis les appareils administrés vers le Serveur d'administration.

  Cette option est activée par défaut.

- **Accéder à KSN Cloud/KPSN directement via Internet**

  Le point de distribution transfère les requêtes KSN depuis les appareils administrés vers le Cloud KSN ou KPSN. Les requêtes KSN générées sur le point de distribution lui-même sont également envoyées directement à KSN Cloud ou à KPSN.

  Les points de distribution sur lesquels l'Agent d'administration version 11 (ou antérieure) est installé ne peuvent pas accéder directement à KPSN. Si vous souhaitez reconfigurer les points de distribution pour envoyer des demandes KSN à KPSN, activez l'option **&Transférer les demandes KSN au Serveur d'administration** pour chaque point de distribution.

  Les points de distribution sur lesquels l'Agent d'administration version 12 (ou version ultérieure) est installé peuvent accéder directement à KPSN.

- **Port TCP**

  Le numéro du port TCP que les appareils administrés utilisent pour se connecter au serveur proxy KSN. Le numéro du port par défaut est 13111.

- **Utiliser un port UDP**

  Si vous avez besoin que l'Agent d'administration se connecte au Serveur d'administration via un port UDP, activez l'option **Utiliser le port UDP** et indiquez le **Numéro de port UDP**. Cette option est activée par défaut. Par défaut, la connexion au Serveur d'administration est exécutée via le port UDP 15000.

Dans la sous-section **Mises à jour**, vous pouvez spécifier si l'Agent d'administration doit télécharger les fichiers différentiels en activant ou en désactivant l'option **Télécharger des fichiers diff**. (Par défaut, l'option est activée.)

Historique des révisions

L'onglet **Historique des révisions** permet de consulter l'historique des révisions de la stratégie de l'Agent d'administration. Vous pouvez comparer les révisions, consulter les révisions et réaliser des opérations avancées comme enregistrer les révisions dans un fichier, revenir à la révision antérieur et ajouter et modifier les descriptions des révisions.

Administration des comptes utilisateurs

Cette section contient des informations sur les comptes utilisateurs et les rôles des utilisateurs pris en charge par l'application. Elle comprend les instructions nécessaires à la création de comptes utilisateur et de rôles des utilisateurs Kaspersky Security Center.

Le Kaspersky Security Center permet d'administrer les comptes utilisateurs et groupes de comptes. L'application prend en charge trois types de comptes utilisateur :

- Comptes utilisateur pour les employés de l'entreprise. Le Serveur d'administration reçoit les données relatives aux comptes utilisateur de ces utilisateurs de domaine lors du balayage du controleur de domaine de l'entreprise.
- Comptes des utilisateurs locaux. Les comptes locaux sur les appareils administrés, ainsi que les comptes locaux sur l'appareil sur lequel le Serveur d'administration est installé.
- Comptes des utilisateurs internes de Kaspersky Security Center. Vous pouvez créer des comptes d'utilisateurs internes. Ces comptes sont utilisés uniquement dans Kaspersky Security Center.

Utilisation des comptes utilisateurs

Le Kaspersky Security Center permet d'administrer les comptes utilisateurs et groupes de comptes. L'application prend en charge deux types de comptes utilisateur :

- Comptes utilisateur pour les employés de l'entreprise. Le Serveur d'administration reçoit les données relatives aux comptes utilisateur de ces utilisateurs lors du balayage du réseau de l'entreprise.
- Comptes utilisateurs des utilisateurs internes. Appliqués pour l'utilisation des Serveurs d'administration virtuels. Les comptes des utilisateurs internes sont créés et utilisés uniquement à l'intérieur de Kaspersky Security Center.

Vous pouvez consulter la liste des comptes utilisateurs d'une des manières suivantes :

- Dans l'arborescence de la console, accédez à **Avancé** → **Comptes utilisateurs**.
- Dans l'arborescence de la console, accédez à **Appareils administrés** → onglet **Appareils** → lien <nom de l'appareil> → section **Sessions**.

  La section **Sessions** affiche les comptes utilisateurs avec des sessions actives sur les appareils fonctionnant sous Windows.

La liste des comptes utilisateurs s'affiche correctement si les conditions suivantes sont remplies :

- Utilisez l'Agent d'administration de la même version que le Serveur d'administration ou d'une version ultérieure.
- Le sondage d'Active Directory est activé pour afficher les comptes des utilisateurs du domaine.
- Sur les appareils administrés fonctionnant sous Windows, le service **Server (LanmanServer)** est exécuté.

Les comptes utilisateurs et groupes de comptes vous permettent d'exécuter les actions suivantes :

- Configurer les privilèges d'accès des utilisateurs aux fonctions de l'application à l'aide de rôles.
- Envoyer des messages aux utilisateurs via email et les SMS.
- Consulter la liste des appareils mobiles d'un utilisateur.
- Émettre et installer des certificats sur les appareils mobiles d'un utilisateur.
- Consulter la liste des certificats octroyés à l'utilisateur.
- Désactivez la vérification en deux étapes d'un compte utilisateur.

Ajout d'un compte d'un utilisateur interne

Pour ajouter un nouveau compte d'utilisateur interne à Kaspersky Security Center, procédez comme suit :

1. Ouvrez le dossier **Comptes utilisateurs** dans l'arborescence de la console.
   Le dossier **Comptes utilisateurs** est un sous-dossier par défaut du dossier **Avancé**.
2. Dans l'espace de travail, cliquez sur le bouton **Ajouter un utilisateur**.

3. Dans la fenêtre **Nouvel utilisateur** qui s'ouvre, définissez les paramètres du nouveau compte utilisateur :

- Un nom d'utilisateur ( )

  > Soyez attentif au moment de saisir le nom d'utilisateur. Une fois que vous l'aurez enregistré, vous ne pourrez plus le modifier.

- **Description**
- **Nom complet**
- **Adresse email principale**
- **Numéro de téléphone principal**
- **Mot de passe** pour connecter l'utilisateur à Kaspersky Security Center

  Le mot de passe doit remplir les conditions suivantes :

  - Le mot de passe doit compter entre 8 et 256 caractères.
  - Le mot de passe doit compter des caractères d'au moins trois des groupes ci-dessous :
    - Lettres majuscules (A-Z)
    - Lettre minuscules (a-z)
    - Chiffres (0-9)
    - Caractères spéciaux (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
  - Le mot de passe ne peut pas contenir d'espaces, de caractères Unicode ou de la combinaison « . » et « @ » lorsque « . » est placé devant « @ ».

  Pour voir le mot de passe saisi, maintenez le bouton **Afficher** enfoncé.

  > Le nombre de tentatives de saisie du mot de passe par l'utilisateur est limité. Par défaut, le nombre maximal de tentatives de saisie du mot de passe autorisées est égal à 10. Vous pouvez modifier le nombre de tentatives de saisie du mot de passe autorisées, comme décrit au point "Modification du nombre de tentatives de saisie du mot de passe autorisées".

  > Si l'utilisateur saisit incorrectement le mot de passe le nombre de fois indiqué, le compte utilisateur associé est bloqué pour une heure. Dans la liste des comptes utilisateurs, l'icône utilisateur ( ) d'un compte bloqué est grisée (non disponible). Il est possible de débloquer le compte utilisateur uniquement en modifiant le mot de passe.

- Le cas échéant, cochez la case **Désactiver le compte utilisateur** pour empêcher l'utilisateur de se connecter à l'application. Vous pouvez désactiver un compte, par exemple si vous souhaitez le créer d'abord, mais que vous préférez l'activer plus tard.
- Sélectionnez la case **Demander le mot de passe lorsque les paramètres du compte sont modifiés** à cocher si vous souhaitez activer une option supplémentaire pour protéger un compte d'utilisateur contre

toute modification non autorisée. Si cette option est activée, la modification des paramètres du compte utilisateur nécessite l'autorisation de l'utilisateur avec le droit Modifier les ACL des objets de la zone fonctionnelle **Caractéristiques générales : Autorisations utilisateur**.

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

Le compte utilisateur créé apparaît dans l'espace de travail du dossier **Comptes utilisateurs**.

Modification d'un compte d'un utilisateur interne

Pour modifier le compte d'un utilisateur interne dans Kaspersky Security Center, procédez comme suit :

1. Ouvrez le dossier **Comptes utilisateurs** dans l'arborescence de la console.

   Le dossier **Comptes utilisateurs** est un sous-dossier par défaut du dossier **Avancé**.

2. Dans l'espace de travail, double-cliquez sur le compte de l'utilisateur interne que vous souhaitez modifier.

3. Dans la fenêtre **Propriétés: <user name>** qui s'ouvre, modifiez les paramètres du compte utilisateur :

- **Description**
- **Nom complet**
- **Adresse email principale**
- **Numéro de téléphone principal**
- **Mot de passe** pour connecter l'utilisateur à Kaspersky Security Center

  Le mot de passe doit remplir les conditions suivantes :

  - Le mot de passe doit compter entre 8 et 256 caractères.
  - Le mot de passe doit compter des caractères d'au moins trois des groupes ci-dessous :
    - Lettres majuscules (A-Z)
    - Lettre minuscules (a-z)
    - Chiffres (0-9)
    - Caractères spéciaux (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
  - Le mot de passe ne peut pas contenir d'espaces, de caractères Unicode ou de la combinaison « . » et « @ » lorsque « . » est placé devant « @ ».

  Pour voir le mot de passe saisi, maintenez le bouton **Afficher** enfoncé.

  > Le nombre de tentatives de saisie du mot de passe par l'utilisateur est limité. Par défaut, le nombre maximal de tentatives de saisie du mot de passe autorisées est égal à 10. Vous pouvez modifier le nombre de tentatives de saisie du mot de passe autorisées, comme décrit au point "Modification du nombre de tentatives de saisie du mot de passe autorisées".

  > Si l'utilisateur saisit incorrectement le mot de passe le nombre de fois indiqué, le compte utilisateur associé est bloqué pour une heure. Dans la liste des comptes utilisateurs, l'icône utilisateur ( ) d'un compte bloqué est grisée (non disponible). Il est possible de débloquer le compte utilisateur uniquement en modifiant le mot de passe.

- Le cas échéant, cochez la case **Désactiver le compte utilisateur** pour empêcher l'utilisateur de se connecter à l'application. Vous pouvez désactiver un compte après qu'un employé a arrêté de travailler pour l'entreprise, par exemple.
- Sélectionnez l'option **Demander le mot de passe lorsque les paramètres du compte sont modifiés** si vous souhaitez activer une option supplémentaire pour protéger un compte d'utilisateur contre toute modification non autorisée. Si cette option est activée, la modification des paramètres du compte utilisateur nécessite l'autorisation de l'utilisateur avec le droit Modifier les ACL des objets de la zone fonctionnelle **Caractéristiques générales : Autorisations utilisateur**.

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

Le compte utilisateur modifié apparaît dans l'espace de travail du dossier **Comptes utilisateurs**.

Modification du nombre de tentatives de saisie du mot de passe autorisées

L'utilisateur de Kaspersky Security Center a droit à un nombre limité d'erreur lors de la saisie du mot de passe. Une fois cette limite atteinte, le compte utilisateur est bloqué pendant une heure.

Par défaut, le nombre maximal de tentatives autorisées est de 10. Vous pouvez modifier le nom de tentatives de saisie du mot de passe autorisées, comme décrit dans cette section.

Pour modifier le nombre de tentatives autorisées de saisie du mot de passe, procédez comme suit :

1. Ouvrez le registre système de l'appareil sur lequel le Serveur d'administration est installé, par exemple, à l'aide de la commande regedit dans le menu **Démarrer** → **Exécuter**.
2. Accédez à la clé suivante :
   - Pour les systèmes 32 bits :
     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags
   - Pour les systèmes 64 bits :
     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1093\1.0.0.0\ServerF
3. Si la valeur SrvSplPpcLogonAttempts n'est pas présente, créez-la. Le type de valeur est DWORD.
   Par défaut, cette valeur n'est pas créée après l'installation de Kaspersky Security Center.
4. Indiquez le nombre requis de tentatives dans la valeur SrvSplPpcLogonAttempts.
5. Cliquez sur le bouton **OK** afin d'enregistrer les modifications.
6. Relancez le service du Serveur d'administration.

Le nombre maximal de tentatives autorisées de saisie du mot de passe est modifié.

Configuration du contrôle de l'originalité du nom de l'utilisateur interne

Vous pouvez configurer le contrôle de l'originalité du nom de l'utilisateur interne Kaspersky Security Center au moment de l'ajouter dans l'application. Le contrôle de l'originalité du nom de l'utilisateur interne peut être exécuté seulement sur le Serveur d'administration virtuel ou le Serveur d'administration principal pour lequel un compte utilisateur est créé ou sur tous les Serveurs d'administration virtuels et le Serveur d'administration principal. Par défaut, le contrôle de l'originalité du nom de l'utilisateur interne est exécuté sur tous les Serveurs d'administration virtuels et sur le Serveur d'administration principal.

Pour activer le contrôle de l'originalité du nom de l'utilisateur interne dans le cadre du Serveur d'administration virtuel ou du Serveur d'administration principal, procédez comme suit :

1. Ouvrez le registre système de l'appareil sur lequel le Serveur d'administration est installé, par exemple, à l'aide de la commande regedit dans le menu **Démarrer** → **Exécuter**.
2. Rendez-vous dans la section :
   - Pour les systèmes 32 bits :

     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\.core\.independent\KLLIM
   - Pour les systèmes 64 bits :

     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\.core\.independent\
3. Pour la clé LP_InterUserUniqVsScope (DWORD), sélectionnez la valeur 00000001.

   Par défaut, la valeur 0 est indiquée pour cette clé.
4. Relancez le service du Serveur d'administration.

Le contrôle de l'originalité du nom sera exécuté seulement sur le Serveur d'administration virtuel où l'utilisateur interne a été créé ou sur le Serveur d'administration principal si l'utilisateur interne a été créé sur le Serveur d'administration principal.

Pour activer le contrôle de l'originalité du nom de l'utilisateur interne sur tous les Serveur d'administration virtuels et sur le Serveur d'administration principal, procédez comme suit :

1. Ouvrez le registre système de l'appareil sur lequel le Serveur d'administration est installé, par exemple, à l'aide de la commande regedit dans le menu **Démarrer** → **Exécuter**.
2. Rendez-vous dans la section :
   - Pour les systèmes 64 bits :

     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\.core\.independent\
   - Pour les systèmes 32 bits :

     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\.core\.independent\KLLIM
3. Pour la clé LP_InterUserUniqVsScope (DWORD), sélectionnez la valeur 00000000.

   Par défaut, la valeur 0 est indiquée pour cette clé.
4. Relancez le service du Serveur d'administration.

Le contrôle de l'originalité du nom sera exécuté sur tous les Serveurs d'administration virtuels et sur le Serveur d'administration principal.

Ajout d'un groupe de sécurité

Vous pouvez ajouter des groupes de sécurité (groupes d'utilisateurs), configurer en toute flexibilité le contenu des groupes et l'accès d'un groupe de sécurité à diverses fonctions de l'application. Ces groupes de sécurité peuvent être nommés en fonction de leurs attributs. Par exemple, le nom peut correspondre à l'emplacement des utilisateurs dans le bureau ou au nom de la sous-section structurelle à laquelle ceux-ci sont rattachés au sein d'une entreprise.

Un seul utilisateur peut appartenir à plusieurs groupes de sécurité. Le compte utilisateur administré par un Serveur d'administration virtuel peut faire partie uniquement des groupes de sécurité de ce serveur virtuel et avoir des droits d'accès uniquement à celui-ci.

Pour ajouter un groupe de sécurité, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le dossier **Comptes utilisateurs**.

   Le dossier **Comptes utilisateurs** est un sous-dossier par défaut du dossier **Avancé**.

2. Cliquez sur le bouton **Ajouter un groupe de sécurité**.

   La fenêtre **Ajouter un groupe de sécurité** s'ouvre.

3. Dans la fenêtre **Ajouter un groupe de sécurité**, dans la section **Général**, indiquez le nom du groupe.

   Le nom du groupe ne peut pas contenir plus de 255 symboles et les caractères *, <, >, ?, \, :, |. Le nom du groupe doit être unique.

   Vous pouvez saisir la description du groupe dans le champ de saisie **Description**. La saisie du champ **Description** est facultative.

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

Le groupe de sécurité ajouté s'affiche dans le dossier **Comptes utilisateurs** dans l'arborescence de la console. Vous pouvez ajouter des utilisateurs au groupe créé.

Ajout d'un utilisateur dans le groupe

Pour ajouter un utilisateur dans le groupe, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le dossier **Comptes utilisateurs**.

   Le dossier **Comptes utilisateurs** est un sous-dossier par défaut du dossier **Avancé**.

2. Dans la liste de comptes utilisateurs et de groupes, sélectionnez le groupe auquel ajouter un utilisateur.

3. Dans la fenêtre des propriétés du groupe, sélectionnez la section **Utilisateurs du groupe** et cliquez sur le bouton **Ajouter**.

   Suite à cette action, la fenêtre s'ouvre avec une liste d'utilisateurs.

4. Dans la liste, sélectionnez l'utilisateur que vous souhaitez ajouter au groupe.

5. Cliquez sur le bouton **OK**.

L'utilisateur est ajouté au groupe et affiché dans la liste des utilisateurs du groupe.

Configuration des droits d'accès aux fonctionnalités de l'application. Restriction d'accès selon un rôle

Kaspersky Security Center fournit des possibilités d'accès selon un rôle aux fonctionnalités de Kaspersky Security Center et des applications Kaspersky administrées.

Vous pouvez configurer les droits d'accès aux fonctionnalités de l'application pour les utilisateurs de Kaspersky Security Center de l'une des manières suivantes :

- Configurer les privilèges de chaque utilisateur ou groupe d'utilisateurs séparément.
- Créer des rôles types d'utilisateurs avec un ensemble de privilèges configurés au préalable et attribuer ces rôles aux utilisateurs en fonction de leurs responsabilités.

Le rôle d'utilisateur (désigné également par le terme rôle) est un ensemble prédéfini de droits d'accès aux fonctionnalités de Kaspersky Security Center ou des applications Kaspersky administrées. Un rôle peut être attribué à un utilisateur ou à un ensemble d'utilisateurs.

L'application des rôles des utilisateurs vise à simplifier et à raccourcir les procédures courantes de configuration des droits d'accès des utilisateurs aux fonctionnalités de l'application. Les droits d'accès des rôles sont configurés en fonction des tâches types et de la responsabilité des utilisateurs.

Ces rôles peuvent être nommés en fonction de leurs attributs. Il est possible de créer un nombre illimité de rôles dans l'application.

Vous pouvez utiliser les rôles d'utilisateurs prédéfinis avec un ensemble de droits déjà configurés, ou créer des rôles et configurer vous-même les droits requis.

Droits d'accès aux fonctionnalités de l'application

Le tableau ci-dessous présente les fonctionnalités de Kaspersky Security Center avec les droits d'accès pour gérer les tâches associées, les rapports, les paramètres et effectuer les actions utilisateur associées.

Pour exécuter les actions utilisateur répertoriées dans le tableau, un utilisateur doit avoir le droit spécifié en regard de l'action.

Les droits **Lire**, **Écrire** et **Exécuter** s'appliquent à toute tâche, rapport ou paramètre. En plus de ces droits, un utilisateur doit disposer du droit **Réalisez des opérations sur les sélections d'appareils** pour gérer les tâches, les rapports ou les paramètres sur les sélections d'appareils.

Toutes les tâches, rapports, paramètres et paquets d'installation qui manquent dans le tableau appartiennent à la zone fonctionnelle **Fonctions générales : Fonctionnalité de base**.

Zone fonctionnelle	Droit	Action utilisateur : droit requis pour exécuter l'action	Tâche	Rapport	Autres
Fonctions générales : Administration des groupes d'administration	**Écrire**	• Ajouter un appareil à un groupe d'administration : **Écrire** • Supprimer un appareil d'un groupe d'administration : **Écrire** • Ajouter un groupe d'administration à un autre groupe d'administration : **Écrire** • Supprimer un groupe d'administration d'un autre groupe d'administration : **Écrire**	Aucun	Aucun	Aucun
Fonctions générales : Accéder aux objets quel que soit leur ACL	**Lire**	Obtenir un accès Lire à tous les objets : **Lire**	Aucun	Aucun	Aucun

Zone fonctionnelle	Droit	Action utilisateur : droit requis pour exécuter l'action	Tâche	Rapport	Autres
Fonctions générales : Fonctionnalité de base	• **Lire** • **Écrire** • **Exécuter** • **Réalisez des opérations sur les sélections d'appareils**	• Règles de déplacement des appareils (création, modification ou suppression) pour le Serveur virtuel : **Écrire**, **Réalisez des opérations sur les sélections d'appareils** • Définir le certificat personnalisé du protocole mobile (LWNGT) : **Lire** • Définir le certificat personnalisé du protocole mobile (LWNGT) : **Écrire** • Obtenir la liste des réseaux définis par NLA : **Lire** • Ajouter, modifier ou supprimer une liste de réseaux définie par NLA : **Écrire** • Afficher la liste de contrôle d'accès des groupes : **Lire** • Afficher le journal des événements Kaspersky : **Lire** • Afficher la clé de récupération pour restaurer l'accès à un disque dur chiffré par le chiffrement de disque BitLocker : **Exécuter**	• " Télécharger les mises à jour dans le stockage du Serveur d'administration " • "Livrer des rapports" • "Diffusion du paquet d'installation" • "Installation des applications sur les Serveurs d'administration secondaires à distance"	• "Rapport sur l'état de la protection" • "Rapport sur les menaces" • "Rapport sur les appareils les plus infectés" • "Rapport sur l'état des bases antivirus" • "Rapport sur les erreurs" • "Rapport sur les attaques réseau" • " Rapport de synthèse sur les applications de sécurité des systèmes de messagerie installées " • " Rapport de synthèse sur les applications de défense de périmètre installés " • "Rapport de synthèse sur les types d'application installés" • "Rapport sur les utilisateurs des appareils infectés" • " Rapport d'incidents " • "Rapport sur les événements" • " Rapport de fonctionnement des Points de distribution " • " Rapport sur les Serveurs d'administration secondaires " • " Rapport sur les événements du Contrôle des appareils " • "Rapport sur les vulnérabilités" • "Rapport sur les applications interdites" • "Rapport sur le fonctionnement du Contrôle Internet" • " Rapport de l'état de chiffrement des	Aucun

Zone fonctionnelle	Droit	Action utilisateur : droit requis pour exécuter l'action	Tâche	Rapport	Autres
				appareils administrés " • " Rapport de l'état de chiffrement des appareils de stockage de masse " • " Rapport sur les erreurs de chiffrement des fichiers " • " Rapport sur le blocage de l'accès aux fichiers chiffrés " • " Rapport sur les privilèges d'accès aux appareils chiffrés " • " Rapport sur les droits effectifs de l'utilisateur " • "Rapport sur les privilèges"	
Fonctions générales : Objets supprimés	• **Lire** • **Écrire**	• Afficher les objets supprimés dans la corbeille : **Lire** • Supprimer des objets de la corbeille : **Écrire**	Aucun	Aucun	Aucun
Fonctions générales : Traitement des événements	• **Supprimer les événements** • **Modifier les paramètres de notification des événements** • **Modifier les paramètres d'enregistrement des événements dans le journal** • **Écrire**	• Modifier les paramètres d'enregistrement des événements : **Modifier les paramètres d'enregistrement des événements dans le journal** • Modifier les paramètres de notification d'événements **Modifier les paramètres de notification des événements** • Supprimer des événements : **Supprimer les événements**	Aucun	Aucun	Paramètres : • Paramètres de propagation de virus : nombre de détections de virus nécessaires pour créer un événement d'épidémie virale • Paramètres de propagation de virus : période de temps pour l'évaluation des détections de virus • Le nombre maximal d'événements stockés dans la base de données • Période de stockage des événements des appareils supprimés

Zone fonctionnelle	Droit	Action utilisateur : droit requis pour exécuter l'action	Tâche	Rapport	Autres
Fonctions générales : Opérations avec le Serveur d'administration	• **Lire** • **Écrire** • **Exécuter** • **Modifier les ACL d'objet** • **Réalisez des opérations sur les sélections d'appareils**	• Spécifier les ports du Serveur d'administration pour la connexion de l'Agent d'administration : **Écrire** • Spécifier les ports du proxy d'activation lancé sur le Serveur d'administration : **Écrire** • Spécifier les ports du proxy d'activation pour les appareils mobiles lancé sur le Serveur d'administration : **Écrire** • Spécifier les ports du serveur Web pour la distribution des paquets autonomes : **Écrire** • Spécifier les ports du serveur Web pour la distribution des profils MDM : **Écrire** • Spécifier les ports SSL du Serveur d'administration pour la connexion via Kaspersky Security Center Web Console : **Écrire** • Spécifier les ports du Serveur d'administration pour la connexion mobile : **Écrire** • Modifier le nombre maximal d'événements stockés dans la base de données du Serveur d'administration : **Écrire** • Spécifier le nombre maximum d'événements pouvant être envoyés par le Serveur d'administration : **Écrire** • Spécifier la période pendant laquelle les événements peuvent être envoyés par le Serveur d'administration : **Écrire**	• "Sauvegarde des données du Serveur d'administration" • "Maintenance de la base de données"	Aucun	Aucun

Zone fonctionnelle	Droit	Action utilisateur : droit requis pour exécuter l'action	Tâche	Rapport	Autres
Fonctions générales : Déploiement de l'application Kaspersky	• **Administration des correctifs de Kaspersky** • **Lire** • **Écrire** • **Exécuter** • **Réalisez des opérations sur les sélections d'appareils**	Approuver ou refuser l'installation du correctif : **Administration des correctifs de Kaspersky**	Aucun	• "Rapport sur les clés de licence utilisées par le Serveur d'administration virtuel" • "Rapport sur les versions des applications Kaspersky" • "Rapport sur les applications incompatibles" • "Rapport sur les versions des mises à jour du module logiciel Kaspersky" • " Rapport sur le déploiement de la protection "	Paquet d'installation : " Kaspersky "
Fonctions générales : Administration des clés de licence	• **Exporter le fichier clé** • **Écrire**	• Exporter le fichier clé : **Exporter le fichier clé** • Modifier les paramètres de clé de licence du Serveur d'administration : **Écrire**	Aucun	Aucun	Aucun
Fonctions générales : Administration des rapports mise en œuvre	• **Lire** • **Écrire**	• Créer des rapports quel que soit leur ACL : **Écrire** • Exécuter des rapports quel que soit leur ACL : **Lire**	Aucun	Aucun	Aucun
Fonctions générales : Hiérarchie des Serveurs d'administration	**Configurer la hiérarchie des Serveurs d'administration**	Enregistrer, mettre à jour ou supprimer des Serveurs d'administration secondaires : **Configurer la hiérarchie des Serveurs d'administration**	Aucun	Aucun	Aucun

Zone fonctionnelle	Droit	Action utilisateur : droit requis pour exécuter l'action	Tâche	Rapport	Autres
Fonctions générales : Autorisations utilisateur	**Modifier les ACL d'objet**	• Modifier les propriétés Sécurité de n'importe quel objet : **Modifier les ACL d'objet** • Gérer les rôles utilisateur : **Modifier les ACL d'objet** • Gérer les utilisateurs internes : **Modifier les ACL d'objet** • Gérer les groupes de sécurité : **Modifier les ACL d'objet** • Gérer les alias : **Modifier les ACL d'objet**	Aucun	Aucun	Aucun
Fonctions générales : Serveurs d'administration virtuels	• **Administrer les serveurs virtuels** • **Lire** • **Écrire** • **Exécuter** • **Réalisez des opérations sur les sélections d'appareils**	• Obtenir la liste des Serveurs d'administration virtuels : **Lire** • Obtenir des informations sur le Serveur d'administration virtuel : **Lire** • Créer, mettre à jour ou supprimer un Serveur d'administration virtuel : **Administrer les serveurs virtuels** • Déplacer un Serveur d'administration virtuel vers un autre groupe : **Administrer les serveurs virtuels** • Définir les autorisations du Serveur virtuel d'administration : **Administrer les serveurs virtuels**	Aucun	" Rapport sur les résultats de l'installation des mises à jour du logiciel tiers "	Aucun
Fonctions générales : Gestion des clés de chiffrement	• **Lire** • **Écrire**	• Exporter les clés de chiffrement : **Lire** • Importer les clés de chiffrement : **Écrire**	Aucun	Aucun	Aucun

Zone fonctionnelle	Droit	Action utilisateur : droit requis pour exécuter l'action	Tâche	Rapport	Autres
Administration des appareils mobiles : Général	• **Connexion des nouveaux appareils** • **Envoi uniquement des commandes d'information sur les appareils mobiles** • **Envoi des commandes sur les appareils mobiles** • **Administrer les certificats** • **Lire** • **Écrire**	• Obtenir les données de restauration du service de gestion des clés : **Lire** • Supprimer les certificats utilisateur : **Administrer les certificats** • Obtenir la partie publique du certificat utilisateur : **Lire** • Vérifier si l'infrastructure à clé publique est activée : **Lire** • Vérifier le compte d'infrastructure à clé publique : **Lire** • Obtenir des modèles d'infrastructure à clé publique : **Lire** • Obtenir des modèles d'infrastructure de clé publique par certificat d'utilisation de clé étendue : **Lire** • Vérifier si le certificat d'infrastructure à clé publique est révoqué : **Lire** • Mettre à jour les paramètres d'émission des certificats utilisateur : **Administrer les certificats** • Obtenir les paramètres d'émission de certificat utilisateur : **Lire** • Obtenir des paquets par nom d'application et par version : **Lire** • Définir ou annuler le certificat utilisateur : **Administrer les certificats** • Renouveler le certificat utilisateur : **Administrer les certificats** • Définir la balise de certificat utilisateur : **Administrer les certificats**	Aucun	Aucun	Aucun

Zone fonctionnelle	Droit	Action utilisateur : droit requis pour exécuter l'action	Tâche	Rapport	Autres
		• Exécuter la génération du paquet d'installation MDM ; annuler la génération du paquet d'installation MDM : **Connexion des nouveaux appareils**			
Administration du système : Connectivité	• **Démarrage des sessions RDP** • **Connectez-vous aux sessions RDP existantes** • **Initier le creusement** • **Enregistrer les fichiers des appareils sur le poste de travail de l'administrateur** • **Lire** • **Écrire** • **Exécuter** • **Réalisez des opérations sur les sélections d'appareils**	• Créer une session de partage du bureau : **Démarrage des sessions RDP** • Créer une session RDP : **Connectez-vous aux sessions RDP existantes** • Créer un tunnel : **Initier le creusement** • Enregistrer la liste des réseaux de contenu : **Enregistrer les fichiers des appareils sur le poste de travail de l'administrateur**	Aucun	" Rapport sur les utilisateurs de l'appareil "	Aucun
Administration du système : Inventaire du matériel	• **Lire** • **Écrire** • **Exécuter** • **Réalisez des opérations sur les sélections d'appareils**	• Obtenir ou exporter un objet d'inventaire matériel : **Lire** • Ajouter, définir ou supprimer un objet d'inventaire matériel : **Écrire**	Aucun	• " Rapport sur le registre du matériel " • " Rapport sur les changements de configuration " • " Rapport sur le matériel "	Aucun
Administration du système : Administration d'accès au réseau	• **Lire** • **Écrire**	• Afficher les paramètres CISCO : **Lire** • Modifier les paramètres CISCO : **Écrire**	Aucun	Aucun	Aucun
Administration du système : Déploiement du système d'exploitation	• **Déploiement des serveurs PXE** • **Lire** • **Écrire** • **Exécuter** • **Réalisez des opérations sur les sélections d'appareils**	• Déployer les serveurs PXE : **Déploiement des serveurs PXE** • Afficher une liste de serveurs PXE : **Lire** • Démarrer ou arrêter le processus d'installation sur les clients PXE : **Exécuter** • Gérer les pilotes pour WinPE et les images du système d'exploitation : **Écrire**	" Créer un paquet d'installation sur l'image du système d'exploitation de l'appareil de référence "	Aucun	Paquet d'installation : " OS Image "

Zone fonctionnelle	Droit	Action utilisateur : droit requis pour exécuter l'action	Tâche	Rapport	Autres
Administration du système : Gestion des vulnérabilités et des correctifs	• **Lire** • **Écrire** • **Exécuter** • **Réalisez des opérations sur les sélections d'appareils**	• Afficher les propriétés des correctifs tiers : **Lire** • Modifier les propriétés des correctifs tiers : **Écrire**	• " Synchronisation de Windows Update " • " Installer les mises à jour de Windows Update " • " Corriger les vulnérabilités " • "Installation des mises à jour requises et correction des vulnérabilités"	"Rapport sur les mises à jour des logiciels"	Aucun
Administration du système : Installation à distance	• **Lire** • **Écrire** • **Exécuter** • **Réalisez des opérations sur les sélections d'appareils**	• Afficher les propriétés du paquet d'installation tiers basé sur la gestion des vulnérabilités et des correctifs : **Lire** • Modifier les propriétés du paquet d'installation tiers basé sur la gestion des vulnérabilités et des correctifs : **Écrire**	Aucun	Aucun	Paquets d'installation : • " Application personnalisée " • " Paquet VAPM "
Administration du système : Inventaire des applications	• **Lire** • **Écrire** • **Exécuter** • **Réalisez des opérations sur les sélections d'appareils**	Aucun	Aucun	• " Rapport sur les applications installées " • " Rapport sur l'historique du registre des applications " • " Rapport sur l'état des groupes des applications sous licence " • " Rapport sur les clés de licence des applications tierces "	Aucun

À propos des rôles d'utilisateurs prédéfinis

Les rôles d'utilisateurs attribués aux utilisateurs de Kaspersky Security Center leur fournissent des ensembles d'autorisations d'accès aux fonctionnalités des applications.

Les utilisateurs créés sur un Serveur virtuel ne peuvent pas se voir attribuer un rôle sur le Serveur d'administration.

Vous pouvez utiliser les rôles d'utilisateurs prédéfinis avec un ensemble de droits déjà configurés, ou créer des rôles. Dans ce cas, vous devez définir vous-même la portée du rôle et attribuer les droits d'accès aux fonctionnalités de Kaspersky Security Center. Certains des rôles d'utilisateurs prédéfinis disponibles dans Kaspersky Security Center peuvent être associés à des fonctions spécifiques, par exemple, **Auditeur**, **Responsable de la sécurité**, **Superviseur** (ces rôles sont présents dans Kaspersky Security Center à partir de la version 11). Les droits d'accès de ces rôles sont préconfigurés conformément aux tâches standard et à l'étendue des tâches des fonctions associées. Le tableau ci-dessous montre comment les rôles suivants peuvent être associés à des fonctions spécifiques.

Exemples de rôles pour des fonctions particulières

Rôle	Commentaire
Auditeur	Autorise la consultation et l'exécution de toutes les tâches créées sur les appareils sélectionnés connectés au Serveur d'administration via l'Agent d'administration avec des privilèges d'administrateur local (root pour Linux). Nous recommandons d'attribuer ce rôle prudemment et à un nombre limité d'utilisateurs qui en ont besoin pour l'accomplissement de leurs tâches officielles.
Superviseur	Autorise toutes les opérations d'affichage, n'autorise pas les autres opérations. Vous pouvez attribuer ce rôle à un responsable de la sécurité et à d'autres responsables chargé de la sécurité de l'information dans votre organisation.
Responsable de la sécurité	Autorise toutes les informations de consultation, autorise la gestion des rapports, octroie des permissions restreintes dans les domaines **Administration du système** : **Connectivité**. Vous pouvez attribuer ce rôle à la personne chargée de la sécurité de l'information dans votre organisation.

Le tableau ci-dessous montre les droits d'accès attribués à chaque rôle d'utilisateur prédéfini.

Droits d'accès des rôles utilisateur prédéfinis

Rôle	Description

Administrateur du Serveur d'administration	Permet toutes les opérations dans les domaines fonctionnels suivants :
	• **Caractéristiques générales** :
	  • **Fonctionnalité de base**
	  • **Traitement des événements**
	  • **Hiérarchie des Serveurs d'administration**
	  • **Serveurs d'administration virtuels**
	• **Administration du système :**
	  • **Connectivité**
	  • **Inventaire du matériel**
	  • **Inventaire des applications**
	
	Accorde les droits de **lecture** et d'**écriture** dans la zone fonctionnelle **Caractéristiques générales : Gestion des clés de chiffrement**.

Opérateur du Serveur d'administration	Accorde les droits de **lecture** et d' **exécution** dans tous les domaines fonctionnels suivants :
	• **Caractéristiques générales** :
	  • **Fonctionnalité de base**
	  • **Serveurs d'administration virtuels**
	• **Administration du système :**
	  • **Connectivité**
	  • **Inventaire du matériel**
	  • **Inventaire des applications**

Rôle	Description
Auditeur	Permet toutes les opérations dans les zones fonctionnelles, dans **Fonctions générales** : • **Accéder aux objets quel que soit leur ACL** • **Objets supprimés** • **Administration des rapports mise en œuvre** Vous pouvez attribuer ce rôle à une personne qui réalise un audit de votre organisation.

Administrateur d'installation	Permet toutes les opérations dans les domaines fonctionnels suivants :
	• **Caractéristiques générales** :
	  • **Fonctionnalité de base**
	  • **Déploiement de logiciels Kaspersky**
	  • **Gestion des clés de licence**
	• **Administration du système :**
	  • **Déploiement du système d'exploitation**
	  • **Gestion des vulnérabilités et des correctifs**
	  • **Installation à distance**
	  • **Inventaire des applications**
	Accorde les droits de **lecture** et d'**exécution** dans la zone fonctionnelle **Fonctionnalités générales : Serveurs d'administration virtuelle**.

Opérateur d'installation	Accorde les droits de **lecture** et d' **exécution** dans tous les domaines fonctionnels suivants :
	• **Caractéristiques générales** :
	  • **Fonctionnalité de base**
	  • **Déploiement de logiciels Kaspersky** (accorde également les **correctifs Manage Kaspersky** directement dans cette zone)
	  • **Serveurs d'administration virtuels**
	• **Administration du système :**
	  • **Déploiement du système d'exploitation**
	  • **Gestion des vulnérabilités et des correctifs**
	  • **Installation à distance**
	  • **Inventaire des applications**

Administrateur Kaspersky Endpoint Security	Permet toutes les opérations dans les domaines fonctionnels suivants : • **Caractéristiques générales : fonctionnalité de base** • Zone Kaspersky Endpoint Security, y compris toutes les fonctionnalités Accorde les droits de **lecture** et d'**écriture** dans la zone fonctionnelle **Caractéristiques générales : Gestion des clés de chiffrement**.
Opérateur Kaspersky Endpoint Security	Accorde les droits de **lecture** et d' **exécution** dans tous les domaines fonctionnels suivants : • **Caractéristiques générales : fonctionnalité de base** • Zone Kaspersky Endpoint Security, y compris toutes les fonctionnalités
Administrateur principal	Permet toutes les opérations dans les domaines fonctionnels, *à l'exception* des zones suivantes dans **Fonctions générales** : • **Accéder aux objets quel que soit leur ACL** • **Administration des rapports mise en œuvre** Accorde les droits de **lecture** et d'**écriture** dans la zone fonctionnelle **Caractéristiques générales : Gestion des clés de chiffrement**.

Rôle	Description

Opérateur principal	Accorde les droits de **lecture** et d' **exécution** (le cas échéant) dans tous les domaines fonctionnels suivants :
	• **Caractéristiques générales** :
	  • **Fonctionnalité de base**
	  • **Objets supprimés**
	  • **Opérations sur le Serveur d'administration**
	  • **Déploiement de l'application Kaspersky**
	  • **Serveurs d'administration virtuels**
	• **Administration des appareils mobiles : généralités**
	• **Gestion du système**, y compris toutes les fonctionnalités
	• Zone Kaspersky Endpoint Security, y compris toutes les fonctionnalités

Administrateur Administration des appareils mobiles	Permet toutes les opérations dans les domaines fonctionnels suivants : • **Caractéristiques générales : fonctionnalité de base** • **Administration des appareils mobiles : généralités**
Opérateur Administration des appareils mobiles	Accorde les droits de **lecture** et d'**exécution** dans la zone fonctionnelle **Fonctionnalités générales** : **Fonctionnalité de base**. Accorde des commandes de **lecture** et d'**envoi uniquement d'informations aux appareils mobiles** dans la zone fonctionnelle **Administration des appareils mobiles** : **Général**.
Responsable de la sécurité	Autorise toutes les opérations dans les domaines fonctionnels suivants, dans **Fonctions générales** : • **Accéder aux objets quel que soit leur ACL** • **Administration des rapports mise en œuvre** Accorde les droits **Lire**, **Écrire**, **Exécuter**, **Enregistrer les fichiers des appareils sur le poste de travail de l'administrateur** et **Réaliser des opérations sur les sélections d'appareils** dans la zone fonctionnelle **Administration du système : Connectivité**. Vous pouvez attribuer ce rôle à la personne chargée de la sécurité de l'information dans votre organisation.
Utilisateur du Self Service Portal	Autorise toutes les opérations dans la zone fonctionnelle **Administration des appareils mobiles : Self Service Portal**. Cette fonctionnalité n'est pas prise en charge par Kaspersky Security Center 11 ni par les versions ultérieures.
Superviseur	Accorde le droit de **lecture** dans les **fonctionnalités générales** : **objets d'accès quelles que soient leurs ACL** et **fonctionnalités générales** : **Administration des rapports mise en œuvre**. Vous pouvez attribuer ce rôle à un responsable de la sécurité et à d'autres responsables chargé de la sécurité de l'information dans votre organisation.
Administrateur de gestion des vulnérabilités et des correctifs	Permet toutes les opérations dans les zones fonctionnelles **Fonctionnalités générales** : **Fonctionnalité de base** et **Gestion du système** (y compris toutes les fonctionnalités).
Opérateur de gestion des vulnérabilités et des correctifs	Accorde les droits de **lecture** et d'**exécution** (le cas échéant) dans les zones fonctionnelles **Fonctionnalités générales** : **Fonctionnalités de base** et **Gestion du système** (y compris toutes les fonctionnalités).

Ajout d'un rôle d'utilisateur

Pour ajouter un rôle utilisateur, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez l'entrée portant le nom du Serveur d'administration requis.
2. Dans le menu contextuel Serveur d'administration, sélectionnez l'option **Propriétés**.

3. Dans la fenêtre des propriétés du Serveur d'administration, dans le volet **Sections**, sélectionnez **Rôles d'utilisateurs**, puis cliquez sur le bouton **Ajouter**.

   La section **Rôles d'utilisateurs** est disponible si l'option **Afficher les sections avec les paramètres de sécurité** est activée.

4. Dans la fenêtre des propriétés du **Nouveau rôle**, configurez le rôle :

   - Dans le volet **Sections**, sélectionnez **Général**, puis indiquez le nom du rôle.

     Le nom du rôle ne peut pas contenir plus de 100 caractères.

   - Sélectionnez la section **Privilèges**, puis configurez l'ensemble de privilèges en cochant les cases **Autoriser** et **Interdire** en regard des fonctions de l'application.

   Si vous utilisez le Serveur d'administration principal, vous pouvez activer l'option **Relayer la liste des rôles vers les serveurs d'administration secondaires**.

5. Cliquez sur le bouton **OK**.

Le rôle est ajouté.

Les rôles d'utilisateurs créés pour le Serveur d'administration apparaissent dans la fenêtre des propriétés du serveur, dans la section **Rôles d'utilisateurs**. Vous pouvez modifier et supprimer les rôles utilisateurs, et attribuer des rôles à des groupes de sécurité ou à des utilisateurs isolés.

Attribution d'un rôle à un utilisateur ou à un groupe de sécurité

Pour attribuer un rôle à un utilisateur ou à un groupe d'utilisateurs, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez l'entrée portant le nom du Serveur d'administration requis.
2. Dans le menu contextuel Serveur d'administration, sélectionnez l'option **Propriétés**.
3. Dans la fenêtre des propriétés du Serveur d'administration, sélectionnez la section **Sécurité**.

   La section **Sécurité** est disponible lorsque la case **Afficher les sections avec les paramètres de sécurité** est cochée dans la fenêtre de configuration de l'interface.

4. Dans le champ **Noms de groupes ou d'utilisateurs**, sélectionnez l'utilisateur ou le groupe d'utilisateurs auquel vous souhaitez attribuer un rôle.

   Si l'utilisateur ou le groupe d'utilisateurs ne s'affiche pas dans le champ, ajoutez-le en cliquant sur le bouton **Ajouter**.

   Si vous ajoutez l'utilisateur avec le bouton **Ajouter**, vous pouvez sélectionner le type d'authentification de l'utilisateur (Microsoft Windows ou Kaspersky Security Center). L'authentification par le Kaspersky Security Center permet de sélectionner les compte utilisateur des utilisateurs internes enregistrés qui manipulent les Serveurs d'administration virtuels.

5. Ouvrez l'onglet **Rôles** et cliquez sur le bouton **Ajouter**.

   La fenêtre **Rôles d'utilisateurs** s'ouvre. Les rôles utilisateur créés s'affichent dans la fenêtre.

6. Sélectionnez le rôle à attribuer au groupe de sécuité dans la fenêtre **Rôles d'utilisateurs**.

7. Cliquez sur le bouton **OK**.

Le rôle comprenant l'ensemble de privilèges concernant l'utilisation du Serveur d'administration sera ainsi attribué à l'utilisateur ou au groupe de sécurité. Les rôles attribués apparaissent dans l'onglet **Rôles** de la section **Sécurité** de la fenêtre des propriétés du Serveur d'administration.

Attribution des permissions aux utilisateurs et aux groupes

Vous pouvez attribuer aux utilisateurs et aux groupes des permissions pour utiliser différentes fonctions du Serveur d'administration et des applications de Kaspersky pour lesquelles vous disposez de plug-ins d'administration, par exemple, Kaspersky Endpoint Security for Windows.

Pour attribuer des permissions à un utilisateur ou à un groupe d'utilisateurs, procédez comme suit :

1. Dans l'arborescence de la console, choisissez un des :

   - Développez l'entrée **Serveur d'administration**, puis sélectionnez le sous-dossier portant le nom du Serveur d'administration requis.

   - Sélectionnez le groupe d'administration.

2. Dans le menu contextuel du Serveur d'administration ou du groupe d'administration, sélectionnez l'option **Propriétés**.

3. Dans la fenêtre des propriétés du Serveur d'administration (ou la fenêtre des propriétés du groupe d'administration) qui s'ouvre, dans le volet de gauche **Sections**, sélectionnez **Sécurité**.

   La section **Sécurité** est disponible lorsque la case **Afficher les sections avec les paramètres de sécurité** est cochée dans la fenêtre de configuration de l'interface.

4. Dans la section **Sécurité**, sélectionnez un utilisateur ou un groupe dans la liste **Noms de groupes ou d'utilisateurs**.

5. Dans la liste des permissions de la partie inférieure de l'espace de travail, sous l'onglet **Privilèges**, configurez l'ensemble des privilèges de l'utilisateur ou du groupe :

   a. Cliquez sur les signes (+) pour développer les entrées de la liste et accéder aux permissions.

   b. Cochez les cases **Autoriser** et **Interdire** en regard des permissions qui vous intéressent.

   Exemple 1 : développez l'entrée **Accéder aux objets, quel que soit leur ACL** ou l'entrée **Objets supprimés**, puis sélectionnez **Lire**.

   Exemple 2 : développez l'entrée **Fonctionnalité de base**, puis cochez la case **Écrire**.

6. Une fois que vous avez défini l'ensemble des privilèges, cliquez sur **Appliquer**.

L'ensemble des privilèges pour les utilisateurs ou les groupes d'utilisateurs sont alors configurés.

Les permissions du Serveur d'administration (ou du groupe d'administration) sont réparties dans les catégories suivantes :

- Fonctions générales :
  - Gestion des groupes d'administration
  - Accéder aux objets quel que soit leur ACL
  - Fonctionnalité de base
  - Objets supprimés
  - Traitement des événements
  - Opérations avec le Serveur d'administration (uniquement dans la fenêtre des propriétés du Serveur d'administration)
  - Déploiement d'applications Kaspersky
  - Gestion des clés de licence
  - Administration des rapports mise en œuvre
  - Hiérarchie des Serveurs
  - Droits d'utilisateurs
  - Serveurs d'administration virtuels
- Administration des appareils mobiles :
  - Général
- Administration du système :
  - Connectivité
  - Inventaire du matériel
  - Administration d'accès au réseau
  - Déploiement du système d'exploitation
  - Administration des vulnérabilités et des correctifs
  - Installation à distance
  - Inventaire des applications

Si aucune des options **Autoriser** ou **Interdire** n'est sélectionnée pour une permission, cette permission est considérée comme *non définie* : elle persiste tant qu'elle n'a pas été explicitement autorisée ou interdite pour l'utilisateur.

Les privilèges d'un utilisateur sont la somme des éléments suivants :

- Propres privilèges de l'utilisateur
- Privilèges de tous les rôles attribués à cet utilisateur
- Privilèges de tous les groupe de sécurité auxquels l'utilisateur appartient
- Les privilèges de tous les rôles attribués aux groupes de sécurité auxquels l'utilisateur appartient

Si au moins un de ces ensembles de privilèges a la valeur **Interdire** pour une permission, celle-ci n'est pas accordée à l'utilisateur, même si d'autres ensembles l'autorisent ou ne la définissent pas.

Propagation des rôles d'utilisateurs sur les Serveurs d'administration secondaires

Par défaut, les liste des rôles d'utilisateurs des Serveurs d'administration principaux et secondaires sont indépendantes. Vous pouvez configurer l'application afin qu'elle propage automatiquement les rôles d'utilisateurs créés sur le Serveur d'administration principal à l'ensemble des Serveurs d'administration secondaires. Les rôles d'utilisateurs peuvent également être propagés depuis un Serveur d'administration secondaire à ses propres Serveurs d'administration secondaires.

Pour propager les rôles d'utilisateurs depuis le Serveur d'administration principal aux Serveurs d'administration secondaires :

1. Ouvrez la fenêtre principale de l'application.
2. Exécutez une des actions suivantes :
   - Dans l'arborescence de la console, cliquez-droit sur le nom du Serveur d'administration, puis sélectionnez **Propriétés** dans le menu contextuel.
   - Si vous disposez d'une stratégie de Serveur d'administration active, accédez à l'espace de travail du dossier **Stratégies**, cliquez-droit sur cette stratégie, puis sélectionnez **Propriétés** dans le menu contextuel.
3. Dans la fenêtre des propriétés du Serveur d'administration ou dans la fenêtre des paramètres de la stratégie, dans le volet **Sections**, sélectionnez **Rôles d'utilisateurs**.

   La section **Rôles d'utilisateurs** est disponible si l'option **Afficher les sections avec les paramètres de sécurité** est activée.

4. Activez l'option **Relayer la liste des rôles aux Serveurs d'administration secondaires**.
5. Cliquez sur le bouton **OK**.

   L'application copie les rôles d'utilisateurs du Serveur d'administration principal sur les Serveurs d'administration secondaires.

Quand l'option **Relayer la liste des rôles aux Serveurs d'administration secondaires** est activée et que les rôles d'utilisateurs sont propagés, ces rôles ne peuvent être ni modifiés, ni supprimés sur les Serveurs d'administration secondaires. Quand vous créez un rôle ou modifiez un rôle existant sur le Serveur d'administration principal, les modifications sont appliquées automatiquement aux Serveurs d'administration secondaires. Quand vous supprimez un rôle d'utilisateur sur le Serveur d'administration principal, ce rôle demeure sur les Serveurs d'administration secondaires, mais il peut alors modifié ou supprimé.

Les rôles propagés sur le Serveur d'administration secondaire depuis le Serveur d'administration primaire sont accompagnés d'un cadenas (🔒). Il est impossible de modifier ces rôles sur le Serveur d'administration secondaire.

Si vous créez un rôle sur le Serveur d'administration principal et s'il existe un rôle portant ce nom sur son Serveur d'administration secondaire, le nouveau rôle est copié sur ce Serveur d'administration secondaire avec un index ajouté à son nom, par exemple ~~1, ~~2 (l'index peut être aléatoire).

Quand vous désactivez l'option **Relayer la liste des rôles aux Serveurs d'administration secondaires**, tous les rôles d'utilisateurs demeurent sur les Serveurs d'administration secondaires, mais deviennent indépendants des rôles sur le Serveur d'administration principal. Une fois qu'ils sont devenus indépendants, ces rôles d'utilisateurs sur les Serveurs d'administration secondaires peuvent être modifiés ou supprimés.

Désignation d'un utilisateur comme propriétaire de l'appareil

Vous pouvez désigner un utilisateur comme propriétaire de l'appareil pour associer les deux. Si des actions doivent être effectuées sur l'appareil (par exemple une mise à jour de la configuration matérielle), l'administrateur peut en informer le propriétaire de l'appareil et convenir d'actions avec lui.

Pour désigner un appareil comme propriétaire de l'appareil, procédez comme suit :

1. Dans l'arborescence de la console sélectionnez le dossier **Appareils administrés**.
2. Dans l'espace de travail du dossier, dans l'onglet **Appareils**, sélectionnez l'appareil pour lequel un propriétaire doit être désigné.
3. Dans le menu contextuel de l'appareil, sélectionnez l'option **Propriétés**.
4. Dans la fenêtre des propriétés de l'appareil, sélectionnez **Informations sur le système** → **Sessions**.
5. Cliquez sur le bouton **Désigner** en regard du champ **Propriétaire de l'appareil**.
6. Dans la fenêtre **Choix de l'utilisateur**, sélectionnez l'utilisateur à désigner comme propriétaire de l'appareil et cliquez sur **OK**.
7. Cliquez sur le bouton **OK**.

Suite à cette action, le propriétaire de l'appareil est désigné. Par défaut, le champ **Propriétaire de l'appareil** contient la valeur d'Active Directory et est mis à jour à chaque sondage d'Active Directory. Vous pouvez consulter la liste des propriétaires des appareils dans **Rapport sur les propriétaires des appareils**. Il est possible de créer un rapport à l'aide de l'Assistant de création du modèle du rapport.

Diffusion des messages aux utilisateurs

Pour envoyer un message par email à l'utilisateur, procédez comme suit :

1. Dans l'arborescence de la console, dans le dossier **Comptes utilisateurs**, sélectionnez un utilisateur.

   Le dossier **Comptes utilisateurs** est un sous-dossier par défaut du dossier **Avancé**.
2. Dans le menu contextuel de l'utilisateur, sélectionnez l'option **Notifier par email**.
3. Remplissez les champs requis dans la fenêtre **Envoyer le message à l'utilisateur**, puis cliquez sur le bouton **OK**.

Le message sera envoyé à l'email repris dans les propriétés de l'utilisateur.

Pour envoyer un message SMS à l'utilisateur, procédez comme suit :

1. Dans l'arborescence de la console, dans le dossier **Comptes utilisateurs**, sélectionnez un utilisateur.
2. Dans le menu contextuel de l'utilisateur, sélectionnez l'option **Envoyer un SMS**.
3. Remplissez les champs requis dans la fenêtre **Texte SMS**, puis cliquez sur le bouton **OK**.

Le SMS sera envoyé au numéro de l'appareil mobile repris dans les propriétés de l'utilisateur.

Consultation de la liste des appareils mobiles de l'utilisateur

Pour consulter la liste des appareils mobiles de l'utilisateur, procédez comme suit :

1. Dans l'arborescence de la console, dans le dossier **Comptes utilisateurs**, sélectionnez un utilisateur.

   Le dossier **Comptes utilisateurs** est un sous-dossier par défaut du dossier **Avancé**.
2. Dans le menu contextuel du compte utilisateur, sélectionnez l'option **Propriétés**.
3. Dans la fenêtre des propriétés du compte utilisateur, sélectionnez la section **Appareils mobiles**.

La section **Appareils mobiles** permet de consulter la liste des appareils mobiles de l'utilisateur et les informations qui les concernent. Le bouton **Exporter dans un fichier** permet d'enregistrer la liste des appareils mobiles dans un fichier.

Installation du certificat pour l'utilisateur

Vous pouvez installer trois types de certificats pour l'utilisateur :

- Certificat partagé indispensable pour identifier l'appareil mobile de l'utilisateur.
- Certificat de messagerie nécessaire pour la configuration de la messagerie d'entreprise sur l'appareil mobile de l'utilisateur.
- Certificat VPN nécessaire pour la configuration du réseau privé virtuel sur l'appareil mobile de l'utilisateur.

Pour octroyer le certificat à l'utilisateur et l'installer, procédez comme suit :

1. Dans l'arborescence de la console, ouvrez le dossier **Comptes utilisateurs** et sélectionnez un compte utilisateur.

   Le dossier **Comptes utilisateurs** est un sous-dossier par défaut du dossier **Avancé**.
2. Dans le menu contextuel du compte utilisateur, sélectionnez l'option **Installer le certificat**.

L'Assistant d'installation des certificats démarre. Suivez les instructions de l'assistant.

Une fois l'Assistant d'installation des certificats terminé, le certificat est créé et installé pour l'utilisateur. Vous pouvez consulter la liste des certificats utilisateur installé et l'exporter dans un fichier.

Consultation de la liste des certificats octroyés à l'utilisateur

Pour consulter la liste de tous les certificats octroyés à l'utilisateur, procédez comme suit :

1. Dans l'arborescence de la console, dans le dossier **Comptes utilisateurs**, sélectionnez un utilisateur.

   Le dossier **Comptes utilisateurs** est un sous-dossier par défaut du dossier **Avancé**.

2. Dans le menu contextuel du compte utilisateur, sélectionnez l'option **Propriétés**.

3. Dans la fenêtre des propriétés du compte utilisateur, sélectionnez la section **Certificats**.

La section **Certificats** permet de consulter la liste des certificats de l'utilisateur et les informations qui les concernent. Le bouton **Exporter dans un fichier** permet d'enregistrer la liste des certificats dans un fichier.

À propos de l'administrateur du Serveur d'administration virtuel

Un administrateur du réseau d'entreprise administré via un Serveur d'administration virtuel lance Kaspersky Security Center Web Console sous le compte utilisateur défini dans cette fenêtre afin de voir les détails de la protection antivirus.

Dans le cas de besoin, il est possible de créer plusieurs comptes utilisateur d'administrateurs du Serveur virtuel.

Les utilisateurs créés sur un Serveur virtuel ne peuvent pas se voir attribuer un rôle sur le Serveur d'administration.

L'administrateur du Serveur d'administration virtuel est un utilisateur interne de Kaspersky Security Center. Les informations sur les utilisateurs internes ne sont pas transmises au système d'exploitation. Kaspersky Security Center effectue l'authentification des utilisateurs internes.

Installation à distance des systèmes d'exploitation et des applications

Kaspersky Security Center permet de créer les images des systèmes d'exploitation et de les déployer sur les appareils clients par le réseau, ainsi que d'exécuter l'installation à distance des applications de Kaspersky et d'autres éditeurs.

Pour créer des images de systèmes d'exploitation, installez les outils de déploiement Windows ADK et les outils Module complémentaire Windows PE pour Windows ADK sur le Serveur d'administration. Vous pouvez créer une image de n'importe quelle version du système d'exploitation Windows qui répond aux exigences du Kaspersky Security Center.

Kaspersky Security Center ne prend pas en charge les versions 64 bits de Windows ADK et de Windows PE.

Prise des images des systèmes d'exploitation

Kaspersky Security Center permet de tirer l'image du système d'exploitation des appareils et de les transférer au Serveur d'administration. Finalement, les images des systèmes d'exploitation reçues sont conservées sur le Serveur d'administration dans le dossier partagé. L'image du système d'exploitation d'un appareil de référence est capturée, puis créée par une tâche de création du paquet d'installation.

La fonctionnalité de prise de l'image du système d'exploitation a des particularités suivantes :

- Il est interdit de prendre l'image du système d'exploitation de l'appareil sur lequel le Serveur d'administration est installé.
- Pendant la prise de l'image du système d'exploitation, la remise à zéro des paramètres de l'appareil d'étalon se passe par l'utilitaire sysprep.exe. Si vous souhaitez restaurer les paramètres de l'appareil d'étalon, cochez la case **Conserver la copie de sauvegarde de l'état de l'appareil** dans l'Assistant de création de la tâche de capture de l'image du système d'exploitation.
- Durant la prise de l'image, le redémarrage de l'appareil d'étalon est exécuté.

Déploiement des images des systèmes d'exploitation sur les nouveaux appareils

Vous pouvez utiliser les images reçues pour le déploiement sur les nouveaux appareils dans le réseau sur lesquels le système d'exploitation n'a pas encore été installé. Pour ce but, la technologie Preboot eXecution Environment (PXE) est utilisée. Vous sélectionnez un appareil en réseau qui sera utilisé en tant que serveur PXE. Cet appareil doit répondre aux exigences suivantes :

- L'Agent d'administration doit être installé sur l'appareil.
- Le serveur DHCP ne doit pas fonctionner sur l'appareil parce que le serveur PXE utilise les mêmes ports que DHCP.
- Le segment du réseau qui fait partie de l'appareil ne doit pas avoir d'autres serveurs PXE.

Les conditions suivantes doivent être remplies pour déployer un système d'exploitation :

- Une carte réseau doit être installée sur l'appareil.
- L'appareil doit être connecté au réseau.
- L'option Network boot doit être sélectionnée dans le BIOS lors du démarrage de l'appareil.

Le déploiement du système d'exploitation est exécuté dans la séquence suivante :

1. L'appareil client établit une connexion avec le serveur PXE pendant le processus d'amorçage.
2. L'appareil client démarre dans l'environnement de préinstallation Windows (WinPE).

   Pour inclure l'appareil dans l'environnement WinPE, la configuration de la composition des pilotes pour l'environnement WinPE peut être requise.

3. L'appareil client est enregistré sur le Serveur d'administration.

4. L'administrateur désigne à l'appareil client le paquet d'installation avec l'image du système d'exploitation.

   L'administrateur peut ajouter les pilotes requis au paquet d'installation contenant l'image du système d'exploitation. L'administrateur peut également définir un fichier de configuration contenant les paramètres du système d'exploitation (fichier de réponse) à appliquer lors de l'installation.

5. Le déploiement du système d'exploitation est exécuté sur l'appareil client.

L'administrateur peut manuellement indiquer les adresses MAC des appareils clients non connectés et désigner à ceux-ci le paquet d'installation avec l'image du système d'exploitation. Quand les appareils clients indiqués se connectent au serveur PXE, l'installation du système d'exploitation est automatiquement exécutée sur ces appareils.

Déploiement des images des systèmes d'exploitation sur les appareils avec le système d'exploitation déjà installé

Le déploiement des images du système d'exploitation sur les appareils clients qui possèdent déjà le système d'exploitation de travail est exécuté à l'aide de la tâche d'installation à distance pour les ensembles d'appareils.

Notez qu'une nouvelle installation du système d'exploitation est effectuée. Toutes les données seront supprimées.

Installation des applications de Kaspersky et d'autres éditeurs du logiciel

L'administrateur peut créer les paquets d'installation de toutes les applications, y compris les applications indiquées par l'utilisateur, et installer ces applications sur les appareils clients à l'aide de la tâche d'installation à distance.

Création des images des systèmes d'exploitation

La création des images des systèmes d'exploitation est exécutée à l'aide de la tâche de prise d'image du système d'exploitation de l'appareil d'étalon.

Pour créer la tâche de prise d'image du système d'exploitation, procédez comme suit :

1. Dans l'arborescence de la console, dans le dossier **Installation à distance**, sélectionnez le sous-dossier **Paquets d'installation**.

2. Cliquez sur le bouton **Créer un paquet d'installation**, pour exécuter l'Assistant de création du paquet d'installation.

3. Dans la fenêtre **Sélection du type de paquet d'installation**, cliquez sur le bouton **Créer un paquet d'installation avec l'image du système d'exploitation**.

4. Suivez les instructions de l'assistant.

   Suite à l'exécution de l'Assistant, la tâche du Serveur d'administration **Création du paquet d'installation à partir de l'image du système d'exploitation** de l'appareil de référence est créée. Il est possible de consulter la tâche dans le dossier **Tâches**.

Suite à l'exécution de la tâche **Création du paquet d'installation à partir de l'image du système d'exploitation de l'appareil de référence**, le paquet d'installation est créé. Ce paquet peut être utilisé pour déployer le système d'exploitation sur les appareils clients à l'aide du serveur PXE ou à l'aide de la tâche d'installation à distance. Il est possible d'afficher le paquet d'installation dans le dossier **Paquets d'installation**.

Installation d'images des systèmes d'exploitation

Kaspersky Security Center permet de déployer sur les appareils du réseau de l'entreprise des images wim des versions de systèmes d'exploitation Windows® pour serveurs et postes de travail.

L'image du système d'exploitation qui convient au déploiement à l'aide des outils de Kaspersky Security Center peut être obtenue via les moyens suivants :

- Importation du fichier install.wim inclus dans le paquet de distribution Windows.
- Prise de l'image depuis l'appareil d'étalon.

Deux scénarios de déploiement de l'image du système d'exploitation sont pris en charge :

- Le déploiement sur un appareil « propre », à savoir un appareil sans système d'exploitation.
- Le déploiement sur un appareil sous un système d'exploitation Windows.

Utiliser l'Environnement de préinstallation Windows (Windows PE) pour capturer et déployer les images du système d'exploitation. Il faut ajouter à WinPE tous les pilotes indispensables au fonctionnement adéquat de tous les appareils. En règle générale, il faut ajouter les pilotes de la carte réseau et du contrôleur de stockage.

Pour pouvoir exécuter les scénarios de déploiement et de prise de l'image, les conditions suivantes doivent être remplies :

- Kit d'installation automatisée Windows (WAIK) version 2.0 ou ultérieure, ou Windows ADK avec le module complémentaire Windows PE pour Windows ADK doit être installé sur le Serveur d'administration. Si vous prévoyez l'installation ou la prise d'images sur Windows XP, il faut installer WAIK.
- Le réseau sur lequel se trouve l'appareil doit avoir un serveur DHCP.
- Le dossier partagé du Serveur d'administration doit être accessible en lecture depuis le réseau dans lequel se trouve l'appareil. Si le dossier partagé se trouve sur un Serveur d'administration, l'accès est requis pour le compte utilisateur KlPxeUser (ce compte utilisateur est créé automatiquement à l'étape d'exécution du programme d'installation du Serveur d'administration). Si le dossier se trouve en dehors du Serveur d'administration, l'accès est requis pour tous.

Lors de la sélection de l'image du système d'exploitation à installer, l'administrateur doit indiquer clairement l'architecture du processeur de l'appareil : x86 ou x86-64.

Configuration de l'adresse du serveur proxy KSN

Par défaut, le nom de connexion ou l'adresse IP du Serveur d'administration coïncide avec l'adresse du serveur proxy KSN. Si vous modifiez le nom de connexion ou l'adresse IP du Serveur d'administration, vous devez spécifier l'adresse correcte du serveur proxy KSN pour éviter une perte de connexion entre les appareils hôtes et KSN.

Pour configurer l'adresse du serveur proxy KSN, procédez comme suit :

1. Dans l'arborescence de la console, accédez à **Avancé** → **Installation à distance** → **Paquets d'installation**.
2. Dans le menu contextuel **Paquets d'installation**, sélectionnez **Propriétés**.
3. Dans la fenêtre qui s'ouvre, indiquez la nouvelle adresse du serveur proxy KSN dans l'onglet **Général**.
4. Cliquez sur le bouton **Appliquer**.

À partir de maintenant, l'adresse indiquée est utilisée comme adresse du serveur proxy KSN. Nous vous recommandons d'activer l'option **Utiliser le proxy KSN** pour optimiser le trafic sur le réseau.

Ajout des pilotes pour l'environnement de préinstallation Windows (WinPE)

Pour ajouter les pilotes pour l'environnement de préinstallation Windows (WinPE), procédez comme suit :

1. Dans l'arborescence de la console du dossier **Installation à distance**, sélectionnez le sous-dossier **Déploiement des images des appareils**.
2. Dans l'espace de travail du dossier **Déploiement des images des appareils**, cliquez sur le bouton **Actions supplémentaires** et dans la liste déroulante, choisissez l'option **Configurer la composition des pilotes pour l'environnement de préinstallation Windows (WinPE)**.

   La fenêtre **Pilotes pour l'environnement de préinstallation Windows** s'ouvre.
3. Dans la fenêtre **Pilotes pour l'environnement de préinstallation Windows**, cliquez sur le bouton **Ajouter**.

   La fenêtre **Sélection du pilote** s'ouvre.
4. Dans la fenêtre **Sélection du pilote**, sélectionnez un pilote dans la liste.

   Si le pilote dont vous avez besoin ne figure pas dans la liste, cliquez sur le bouton **Ajouter**, et dans la fenêtre **Ajout du pilote** qui s'ouvre, indiquez le nom du pilote, ainsi que le dossier du paquet de distribution du pilote.

   Vous pouvez choisir le dossier en cliquant sur le dossier **Parcourir**.

   Dans la fenêtre **Ajout du pilote**, cliquez sur **OK**.
5. Dans la fenêtre **Sélection du pilote**, cliquez sur le bouton **OK**.

   Le pilote sera ajouté dans le stockage du Serveur d'administration. Une fois ajouté au stockage, le pilote s'affiche dans la fenêtre **Sélection du pilote**.
6. Dans la fenêtre **Pilotes pour l'environnement de préinstallation Windows**, cliquez sur le bouton **OK**.

Le pilote sera ajouté dans l'environnement de préinstallation Windows (WinPE).

Ajout des pilotes dans le paquet d'installation avec l'image du système d'exploitation

Pour ajouter des pilotes dans le paquet d'installation avec l'image du système d'exploitation, procédez comme suit :

1. Dans l'arborescence de la console, dans le dossier **Installation à distance**, sélectionnez le sous-dossier **Paquets d'installation**.
2. Dans le menu contextuel du paquet d'installation contenant une image du système d'exploitation, sélectionnez l'option **Propriétés**.

   La fenêtre des propriétés du paquet d'installation s'ouvre.
3. Dans la fenêtre des propriétés du paquet d'installation, sélectionnez la section **Pilotes complémentaires**.
4. Cliquez sur le bouton **Ajouter** dans la section **Pilotes complémentaires**.

   La fenêtre **Sélection du pilote** s'ouvre.
5. Dans la fenêtre **Sélection du pilote**, sélectionnez les pilotes que vous souhaitez ajouter au paquet d'installation avec l'image du système d'exploitation.

   De nouveaux pilotes peuvent être ajoutés dans le stockage du Serveur d'administration, par un clic sur le bouton **Ajouter** dans la fenêtre **Sélection du pilote**.
6. Cliquez sur le bouton **OK**.

Les pilotes ajoutés s'affichent dans la section **Pilotes complémentaires** dans la fenêtre des propriétés du paquet d'installation avec l'image du système d'exploitation.

Configuration des paramètres de l'utilitaire sysprep.exe

L'utilitaire sysrep.exe est utilisé pour préparer l'appareil à la création de l'image du système d'exploitation de celui-ci.

Pour configurer la requête de l'utilitaire sysprep.exe, procédez comme suit :

1. Dans l'arborescence de la console, dans le dossier **Installation à distance**, sélectionnez le sous-dossier **Paquets d'installation**.
2. Dans le menu contextuel du paquet d'installation contenant une image du système d'exploitation, sélectionnez l'option **Propriétés**.

   La fenêtre des propriétés du paquet d'installation s'ouvre.
3. Dans la fenêtre des propriétés du paquet d'installation, sélectionnez la section **Paramètres de sysprep.exe**.

4. Dans la section **Paramètres de sysprep.exe**, indiquez un fichier de configuration à utiliser lors du déploiement du système d'exploitation sur l'appareil client :

   - **Utiliser le fichier de configuration par défaut**. Sélectionnez cette option pour utiliser le fichier-réponse créé par défaut pendant la prise de l'image du système d'exploitation.
   - **Définir les valeurs d'&utilisateur des paramètres principaux**. Sélectionnez cette option pour définir les valeurs des paramètres à l'aide de l'interface d'utilisateur.
   - **Définir le fichier de configuration**. Sélectionnez cette option pour utiliser votre propre fichier-réponse.

5. Cliquez sur le bouton **Appliquer** pour que les modifications apportées entrent en vigueur.

Déploiement des systèmes d'exploitation sur les nouveaux appareils dans le réseau

Pour déployer le système d'exploitation sur les nouveaux appareils qui ne possèdent pas encore de système d'exploitation, procédez comme suit :

1. Dans l'arborescence de la console du dossier **Installation à distance**, sélectionnez le sous-dossier **Déploiement des images des appareils**.

   Assurez-vous que l'option **Afficher Gestion des vulnérabilités et des correctifs** est activée dans la **fenêtre** &Configuration de l'interface. Dans le cas contraire, le dossier **Installation à distance** ne s'affiche pas.

2. Cliquez sur le bouton **Actions supplémentaires** et sélectionnez **Administrer la liste des serveurs PXE sur le réseau** dans la liste déroulante.

   La fenêtre **Propriétés : Déploiement des images des appareils** s'ouvre dans la section **Serveurs PXE**.

3. Dans la section **Serveurs PXE**, cliquez sur le bouton **Ajouter** et, dans la fenêtre **Serveurs PXE** qui s'ouvre, sélectionnez l'appareil qui sera utilisé en tant que serveur PXE.

   L'appareil ajouté s'affichera dans la section Serveurs PXE. Les fichiers WinPE créés sont transférés du Serveur d'administration sur l'appareil. Le processus de transfert de fichier prend généralement 10 minutes. Une fois le transfert terminé, la valeur **État** affichée passe de **Guide de démarrage** à **Prêt**.

4. Dans la section **Serveurs PXE**, sélectionnez un serveur PXE et cliquez sur le bouton **Propriétés**.

5. Dans la fenêtre des propriétés du serveur PXE, dans l'onglet **Paramètres de connexion au serveur PXE**, configurez la connexion entre le Serveur d'administration et le serveur PXE.

6. Exécutez le démarrage de l'appareil client sur lequel vous voulez déployer le système d'exploitation.

7. Dans l'environnement BIOS de l'appareil client, sélectionnez l'option d'installation Network boot.

   L'appareil client se connecte au serveur PXE, puis apparaît dans l'espace de travail du dossier **Déploiement des images des appareils**.

8. Dans la section **Actions**, cliquez sur le lien **Désigner le paquet d'installation** pour sélectionner le paquet d'installation qui sera utilisé pour installer le système d'exploitation sur l'appareil sélectionné.

   Utilisez l'outil DiskPart sur l'appareil sélectionné pour vérifier les disques disponibles. À l'invite de commandes Windows PE, saisissez `diskpart` pour ouvrir l'outil DiskPart. Saisissez la `list disk` pour répertorier les disques.

   Après l'ajout de l'appareil et la désignation du paquet d'installation pour celui-ci, le déploiement du système d'exploitation sur cet appareil commence automatiquement.

9. Pour annuler le déploiement du système d'exploitation sur l'appareil client, cliquez sur le lien **Annuler l'installation des images du S.E** dans la section **Actions**.

Pour ajouter les appareils par l'adresse MAC,

- Dans le dossier **Déploiement des images des appareils**, cliquez sur **Ajouter l'adresse MAC de l'appareil ciblé** pour ouvrir la fenêtre **Nouvel appareil**, et indiquez l'adresse MAC de l'appareil que vous souhaitez ajouter.

- Dans le dossier **Déploiement des images des appareils**, cliquez sur **Importer les adresses MAC des appareils ciblés à partir d'un fichier** pour sélectionner le fichier contenant la liste des adresses MAC de tous les appareils sur lesquels vous voulez déployer un système d'exploitation.

Déploiement des systèmes d'exploitation sur les appareils clients

Pour exécuter le déploiement du système d'exploitation sur les appareils clients avec le système d'exploitation déjà installé, procédez comme suit :

1. Dans l'arborescence de la console, ouvrez le dossier **Installation à distance** et cliquez sur le lien **Déployer le paquet d'installation sur les appareils administrés (postes de travail)** pour exécuter l'Assistant de déploiement de la protection.

2. Dans la fenêtre **Sélection du paquet d'installation** de l'Assistant, définissez un paquet d'installation grâce à une image du système d'exploitation.

3. Suivez les instructions de l'assistant.

Suite au fonctionnement de l'Assistant, la tâche d'installation à distance du système d'exploitation sur les appareils clients est créée. Il est possible de lancer ou d'arrêter la tâche dans le dossier **Tâches**.

Création des paquets d'installation des applications

Afin de créer le paquet d'installation de l'application, procédez comme suit :

1. Dans l'arborescence de la console, dans le dossier **Installation à distance**, sélectionnez le sous-dossier **Paquets d'installation**.

2. Cliquez sur le bouton **Créer un paquet d'installation**, pour exécuter l'Assistant de création du paquet d'installation.

3. Dans la fenêtre de l'Assistant **Sélection du type de paquet d'installation**, cliquez sur l'un des boutons suivants :

- **Créer un paquet d'installation pour une application Kaspersky**. Sélectionnez cette option si vous voulez créer le paquet d'installation pour l'application de Kaspersky.

- **Créer un paquet d'installation pour le fichier exécutable indiqué**. Sélectionnez cette option si vous voulez créer un paquet d'installation pour une application tierce par un fichier exécutable. En règle générale, le fichier exécutable est un fichier d'installation de l'application.

  - Copier tout le dossi&er dans le paquet d'installation

    Sélectionnez cette option si le fichier exécutable est accompagné de fichiers supplémentaires requis pour l'installation de l'application. Avant d'activer cette option, assurez-vous que tous les fichiers requis sont stockés dans le même dossier. Si cette option est activée, l'application ajoute l'intégralité du contenu du dossier, y compris le fichier exécutable spécifié, au paquet d'installation.

  - Spécifier les paramètres d'installation

    Pour une installation à distance réussie, la plupart des applications nécessitent une installation en mode silencieux. Si c'est le cas, vous devez spécifier le paramètre pour une installation en mode silencieux.

    Configurez les paramètres d'installation :

    - **Ligne de commande du fichier exécutable**

      Si l'application nécessite des paramètres supplémentaires pour une installation en mode silencieux, spécifiez-les dans ce champ. Pour plus d'informations, voir la documentation du fournisseur.

      Vous pouvez aussi entrer d'autres paramètres.

    - **Convertissez les paramètres en valeurs recommandées pour les applications reconnues par Kaspersky Security Center**

      L'application sera installée avec les paramètres recommandés si la base de données de Kaspersky contient des informations sur l'application spécifiée.

      Si vous avez entré les paramètres dans le champ **Ligne de commande du fichier exécutable**, ils sont redéfinis avec les paramètres recommandés.

      Cette option est activée par défaut.

      La base de données de Kaspersky est créée et gérée par les analystes de Kaspersky. Les analystes de Kaspersky définissent les paramètres d'installation optimaux pour chaque application ajoutée à la base de données. Les paramètres sont définis pour garantir la réussite de l'installation à distance d'une application sur un appareil client. La base de données est automatiquement mise à jour sur le Serveur d'administration lorsque vous exécutez la tâche Télécharger les mises à jour sur le référentiel du Serveur d'administration.

- **Sélectionner l'application de la base de Kaspersky pour créer un paquet d'installation**. Choisissez cette option si vous voulez choisir dans la base de données de Kaspersky l'application pour laquelle le paquet d'installation doit être créé. La base de données est créée automatiquement lorsque vous exécutez automatiquement la tâche Télécharger les mises jour sur le référentiel du Serveur d'administration ; les applications sont affichées dans la liste.

- **Créer un paquet d'installation avec l'image du système d'exploitation**. Sélectionnez cette option si vous voulez créer le paquet d'installation avec l'image du système d'exploitation de l'appareil d'étalon.

Suite à l'exécution de l'Assistant, la tâche du Serveur d'administration est créée sous le nom **Création du paquet d'installation à partir de l'image du système d'exploitation** de l'appareil de référence. Suite à l'exécution de cette tâche, le paquet d'installation est créé. Ce paquet peut être utilisé pour déployer l'image du système d'exploitation à l'aide du serveur PXE ou à l'aide de la tâche d'installation à distance.

4. Suivez les instructions de l'assistant.

Suite au fonctionnement de l'Assistant, le paquet d'installation est créé. Ce paquet peut être utilisé pour installer l'application sur les appareils clients. Vous pouvez voir le paquet d'installation en sélectionnant **Paquets d'installation** dans l'arborescence de la console.

Établissement d'un certificat pour les paquets d'installation des applications

Afin de calculer un certificat pour un paquet d'installation d'application, procédez comme suit :

1. Dans l'arborescence de la console, dans le dossier **Installation à distance**, sélectionnez le sous-dossier **Paquets d'installation**.

   Le dossier **Installation à distance** est un sous-dossier par défaut du dossier **Avancé**.

2. Dans le menu contextuel du dossier **Paquets d'installation**, sélectionnez **Avancé**.

   Ainsi, la fenêtre des propriétés du dossier **Paquets d'installation** s'ouvre.

3. Dans la fenêtre des propriétés du dossier **Paquets d'installation**, sélectionnez la section **Signature des paquets autonomes**.

4. Dans la section **Signature des paquets autonomes**, cliquez sur le bouton **Définir**.

   La fenêtre **Certificat**.

5. Dans le champ **Type de certificat**, sélectionnez le type de certificat ouvert ou fermé :

   - Si la valeur **Conteneur PKCS#12** est sélectionnée, indiquez le fichier de certificat et le mot de passe.
   - Si la valeur **Certificat X.509** est sélectionnée :

     a. Indiquez un fichier clé privée (avec l'extension prk ou pem).

     b. Indiquez le mot de passe de la clé privée.

     c. Indiquez un fichier clé publique (avec l'extension cer).

6. Cliquez sur le bouton **OK**.

Suite à cette action, un certificat est établi pour le paquet d'installation de l'application.

Installation des applications sur les appareils clients

Pour installer l'application sur les appareils clients, procédez comme suit :

1. Dans l'arborescence de la console, ouvrez le dossier **Installation à distance** et cliquez sur **Déployer le paquet d'installation sur les appareils administrés (postes de travail)** pour exécuter l'Assistant de déploiement de la protection.

2. Dans la fenêtre **Sélection du paquet d'installation** de l'Assistant, indiquez le paquet d'installation de l'application que vous voulez installer.

3. Suivez les instructions de l'assistant.

Une fois l'Assistant terminé, la tâche d'installation à distance de l'application sur les appareils clients est créée. Il est possible de lancer ou d'arrêter la tâche dans le dossier **Tâches**.

Vous pouvez installer l'Agent d'administration sur les appareils clients fonctionnant sous les systèmes d'exploitation Windows, Linux et macOS à l'aide de l'Assistant de déploiement de la protection.

Pour administrer les applications de sécurité 64 bits à l'aide de Kaspersky Security Center sur les appareils qui tournent sous Linux, il faut utiliser un Agent d'administration 64 bits. Vous pouvez télécharger l'Agent d'administration depuis le site Internet du Support Technique.

Avant l'exécution de l'installation à distance de l'Agent d'administration sur l'appareil fonctionnant sous le système d'exploitation Linux, il est nécessaire de préparer l'appareil.

Utilisation des révisions des objets

Cette section contient les informations sur l'utilisation des révisions des objets. Kaspersky Security Center permet de suivre les modifications des objets. Chaque enregistrement de modification dans une objet entraîne la création d'une *révision*. Chaque révision possède un numéro.

Voici les objets de l'application compatibles avec les révisions :

- Propriétés du Serveur d'administration
- Stratégies
- Tâches
- Groupes d'administration
- Comptes utilisateurs
- Paquets d'installation

Vous pouvez réaliser les opérations suivantes avec les révisions d'objets :

- Comparer la révision sélectionnée à la révision actuelle
- Comparer les révisions sélectionnées
- Comparer un objet avec la révision sélectionnée d'un autre objet du même type
- Consulter la révision sélectionnée
- Annuler les modifications d'un objet jusqu'à la révision sélectionnée
- Enregistrer les révisions dans un fichier au format TXT

La section **Historique des révisions** de la fenêtre des propriétés des objets compatibles avec la gestion des révisions reprend une liste des révisions avec les informations suivantes :

- Le numéro de la révision de l'objet
- La date et l'heure de modification de l'objet
- Le nom de l'utilisateur ayant modifié l'objet
- L'action exécutée avec l'objet
- Description de la révision de modification des paramètres de l'objet

À propos des révisions des objets

Vous pouvez réaliser les opérations suivantes avec les révisions d'objets :

- Comparer la révision sélectionnée à la révision actuelle
- Comparer les révisions sélectionnées
- Comparer un objet avec la révision sélectionnée d'un autre objet du même type
- Consulter la révision sélectionnée
- Annuler les modifications d'un objet jusqu'à la révision sélectionnée
- Enregistrer les révisions dans un fichier au format TXT

La section **Historique des révisions** de la fenêtre des propriétés des objets compatibles avec la gestion des révisions reprend une liste des révisions avec les informations suivantes :

- Le numéro de la révision de l'objet
- La date et l'heure de modification de l'objet
- Le nom de l'utilisateur ayant modifié l'objet

- L'action exécutée avec l'objet
- Description de la révision de modification des paramètres de l'objet

Consultation de la Section Historique des révisions

Vous pouvez comparer les révisions d'un objet à la révision actuelle, comparer des révisions sélectionnées dans une liste ou comparer la révision d'un objet à la révision d'un autre objet du même type.

*Pour afficher la section **Historique des révisions** d'un objet, procédez comme suit :*

1. Dans l'arborescence de la console, choisissez un des objets :
   - Entrée **Serveur d'administration**
   - Dossier **Stratégies**
   - Dossier **Tâches**
   - Dossier du groupe d'administration
   - Dossier **Comptes utilisateurs**
   - Dossier **Objets supprimés**
   - Sous-dossier **Paquets d'installation**, imbriqué dans le dossier **Installation à distance**
2. En fonction de l'emplacement de l'objet pertinent, réalisez une des opérations suivantes :
   - Si l'objet se trouve dans l'entrée **Serveur d'administration** ou dans l'entrée d'un groupe d'administration, cliquez-droit sur l'entrée, puis dans le menu contextuel, sélectionnez **Propriétés**.
   - Si l'objet se trouve dans le dossier **Stratégies**, **Tâches**, **Comptes utilisateurs**, **Objets supprimés** ou **Paquets d'installation**, sélectionnez le dossier et, dans l'espace de travail correspondant, sélectionnez l'objet.

   La fenêtre de propriétés du Objet s'affiche.
3. Dans le volet de gauche **Sections**, sélectionnez **Historique des révisions**.

L'historique des révisions s'affiche dans l'espace de travail.

Comparaison des révisions des objets

Vous pouvez comparer les précédentes révisions d'un objet à la révision actuelle, comparer des révisions sélectionnées dans une liste ou comparer la révision d'un objet à la révision d'un autre objet du même type.

Pour comparer les révision de l'objet, procédez comme suit :

1. Sélectionner un objet et passez à la fenêtre des propriétés de celui-ci.
2. Dans la fenêtre des propriétés, passez à la section **Historique des révisions**.

3. Espace de travail ,Dans la liste des révisions de l'objet sélectionnez la révision à comparer.

   Pour sélectionner deux révisions et plus de l'objet, utilisez les touches **SHIFT** et **CTRL**.

4. Exécutez une des actions suivantes :

   - Cliquez sur le bouton **Comparer** et sélectionnez une des valeurs de la liste déroulante :

     - Comparer à la révision en cours

       Choisissez cette option pour comparer la révision sélectionnée à la révision en cours.

     - Comparer les révisions sélectionnées

       Sélectionnez cette option pour comparer deux révisions sélectionnées.

     - Comparer à une autre tâche

       Lors de l'utilisation des révisions des tâches, choisissez l'option **Comparer à une autre tâche** pour comparer la révision sélectionnée à la révision d'une autre tâche.

       Si vous travaillez avec des révisions des stratégies, sélectionnez **Comparer à une autre stratégie** pour comparer la révision sélectionnée à la révision d'une autre stratégie.

   - Double-cliquez sur le nom d'une révision, puis dans la fenêtre des propriétés de la révision qui s'ouvre, cliquez sur un des boutons suivants :

     - &Comparer à l'actuel

       Cliquez sur ce bouton pour comparer la révision sélectionnée à l'actuelle.

     - Comparer au précédent

       Cliquez sur ce bouton pour comparer la révision sélectionnée à la précédente.

   Un rapport au format HTML sur la comparaison des révisions s'affiche dans votre navigateur par défaut.

   Le rapport permet de réduire certaines sections des paramètres de révision. Pour réduire un groupe de paramètres de révision, cliquez sur l'icône flèche ( ) en regard du nom du groupe.

Pour les révisions du Serveur d'administration, nous retrouvons des informations sur les modifications, sauf les informations des sections suivantes :

- Section **Trafic**
- Section **Règles d'attribution des tags**
- Section **Notification**

- Section **Points de distribution**
- Section **Attaque de virus**

  Aucune information émanant de la section **Attaque de virus** sur la configuration de l'activation de stratégie qui se produit lorsqu'un événement d'attaque de virus n'est enregistrée.

Il est possible de comparer les révisions d'un objet supprimé à une révision d'un objet existant, mais pas l'inverse : il n'est pas possible de comparer les révisions d'un objet existant à la révision d'un objet supprimé.

Définition de la durée de stockage pour les révisions de l'objet et pour les informations sur l'objet supprimé

La durée stockage des révisions de l'objet et des informations relatives aux objets supprimés est identique. La valeur de stockage par défaut est de 90 jours. Ceci suffit pour l'audit régulier de l'application.

Seuls les utilisateurs dotés des permissions **Modifier** dans la zone **Objets supprimés** peuvent modifier la durée de conservation.

Pour modifier la durée de stockage des révisions de l'objet et des informations relatives aux objets supprimés :

1. Dans l'arborescence de la console, sélectionnez le Serveur d'administration pour lequel vous devez Modification les statistiques de KSN.
2. Cliquez-droit, puis sélectionnez **Propriétés** dans le menu contextuel.
3. Dans la fenêtre des propriétés du Serveur d'administration qui s'ouvre, dans la section **Stockage de l'historique des révisions**, saisissez la durée de stockage souhaitée (en jours).
4. Cliquez sur le bouton **OK**.

Les révision de l'objet et les informations relatives aux objets supprimés sont stockées pendant le nombre de jours que vous avez saisi.

Description de la révision de l'objet

Si vous souhaitez connaître les modifications apportées à un objet sur une période définie, vous pouvez consulter les révisions de l'objet.

Pour afficher les révisions de l'objet, procédez comme suit :

1. Passez à la section **Historique des révisions** de l'objet.
2. Dans la liste des révisions de l'objet, sélectionnez la révision pour laquelle vous devez consulter les paramètres.
3. Exécutez une des actions suivantes :
   - Cliquez sur le bouton **Consulter la révision**.
   - Ouvrez la fenêtre des propriétés de la révision en double cliquant sur le nom de la révision, puis en cliquant sur le bouton **Consulter la révision**.

Le rapport sur les paramètres de la révision de l'objet sélectionnée s'affiche au format HTML. Le rapport permet de réduire certains groupes de paramètres de révision de l'objet. Pour réduire un groupe de paramètres de révision, cliquez sur l'icône flèche ( ) en regard du nom du groupe.

Enregistrement de la révision de l'objet dans un fichier

Vous pouvez enregistrer la révision de l'objet dans un fichier texte, par exemple pour envoyer un fichier par email.

Pour enregistrer une révision d'un objet dans un fichier, procédez comme suit :

1. Passez à la section **Historique des révisions** de l'objet.
2. Dans la liste des révisions de l'objet, sélectionnez la révision dont vous souhaitez enregistrer les paramètres.
3. Cliquez sur le bouton **Avancé** et dans la liste déroulante, sélectionnez la valeur **Enregistrer dans un fichier**.

La révision est enregistrée dans un fichier au format TXT.

Restauration des modifications

En cas de besoin, vous pouvez restaurer les modifications de l'objet. Par exemple, il peut être nécessaire de rétablir les paramètres de la stratégie à leur état à la date définie.

Pour restaurer les modifications d'un objet, procédez comme suit :

1. Passez à la section **Historique des révisions** de l'objet.
2. Dans la liste des révisions de l'objet, sélectionnez le numéro de la révision pour laquelle il faut restaurer les modifications.
3. Cliquez sur le bouton **Avancé** et dans la liste déroulante, sélectionnez la valeur **Restaurer**.

La version sélectionnée est restaurée. La liste des révisions de l'objet reprend une entrée sur l'action exécutée. La description de la révision affiche les informations sur le numéro de révision rétablie pour l'objet.

Ajout d'une description de la révision

Vous pouvez ajouter une description de la révision afin de pouvoir la retrouver facilement dans la liste à l'avenir.

Pour ajouter une description de la révision, procédez comme suit :

1. Passez à la section **Historique des révisions** de l'objet.
2. Dans la liste des révisions de l'objet, sélectionnez la révision pour laquelle vous souhaitez ajouter une description.
3. Cliquez sur le bouton **Description**.
4. Dans la fenêtre **Description de la révision de l'objet**, saisissez un texte correspondant à la description de la révision.

   Par défaut, la description de la révision de l'objet n'est pas remplie.
5. Cliquez sur le bouton **OK**.

Suppression d'objets

Cette section fournit des informations sur la suppression d'objets.

Vous pouvez supprimer les objets suivants :

- Stratégies
- Tâches
- Paquets d'installation
- Serveurs d'administration virtuels
- Utilisateurs
- Groupes de sécurité
- Groupes d'administration

Pour supprimer un objet, procédez comme suit :

1. Ouvrez la section requise de Kaspersky Security Center Web Console, puis sélectionnez l'objet.
2. Dans la barre d'outils, cliquez sur le bouton **Supprimer**.
3. Dans la fenêtre qui s'ouvre, cliquez **OK** pour confirmer votre choix.

   L'objet sélectionné est supprimé.

Quand vous supprimez un objet, les informations à son sujet demeurent dans la base de données. La Durée de stockage des informations relatives aux objets supprimés est identique à la période de stockage des révisions de l'objet (la période recommandée est de 90 jours). Vous pouvez modifier la durée de conservation uniquement si vous possédez la permission **Modifier** dans la zone de privilèges **Objets supprimés**.

À propos de la suppression des appareils clients

Lorsque vous supprimez un appareil administré d'un groupe d'administration, l'application place l'appareil dans le groupe Appareils non définis. Après la suppression de l'appareil, les applications Kaspersky installées (Agent d'administration et toute application de sécurité, par exemple, Kaspersky Endpoint Security) restent sur l'appareil.

Kaspersky Security Center gère les appareils du groupe Appareils non définis selon les règles suivantes :

- Si vous avez configuré des règles de déplacement d'appareils et qu'un appareil répond aux critères d'une règle de déplacement, l'appareil est automatiquement déplacé vers un groupe d'administration conformément à la règle.

- L' appareil est stocké dans le groupe Appareils non définis et automatiquement supprimé du groupe conformément aux règles de conservation des appareils.

  Les règles de conservation des appareils n'affectent pas les appareils dont un ou plusieurs disques sont chiffrés à l'aide du chiffrement du disque. Ces appareils ne sont pas supprimés automatiquement. Vous ne pouvez les supprimer que manuellement. Si vous devez supprimer un appareil doté d'un disque chiffré, commencez par déchiffrer le disque, puis supprimez l'appareil.

  > Lorsque vous supprimez un appareil doté d'un disque chiffré, les données nécessaires au déchiffrement du disque sont également supprimées. Si vous cochez la case **Je comprends le risque et je souhaite supprimer les appareils sélectionnés** dans la fenêtre de confirmation qui s'ouvre lorsque vous supprimez de tels appareils (soit du groupe **Appareils non définis**, soit du groupe **Appareils administrés**), cela signifie que vous êtes au courant de la suppression des données ultérieure.

  Pour déchiffrer le disque, les conditions suivantes doivent être remplies :

  - L'appareil est reconnecté au Serveur d'administration pour restaurer les données nécessaires au déchiffrement du disque.

  - L'utilisateur de l'appareil se souvient du mot de passe de déchiffrement.

  - L'application de sécurité utilisée pour chiffrer le disque, par exemple, Kaspersky Endpoint Security for Windows, est toujours installée sur l'appareil.

  Si le disque a été chiffré à l'aide de la technologie Kaspersky Disk Encryption, vous pouvez également essayer de récupérer les données à l'aide de l'utilitaire de restauration FDERT.

> Dans VDI, si vous disposez d'un appareil avec des disques chiffrés, les informations contenues sur le disque chiffré sont supprimées après la suppression de l'appareil.

Lorsque vous supprimez manuellement un appareil du groupe Appareils non définis, l'application supprime l'appareil de la liste. Après la suppression de l'appareil, les applications Kaspersky installées (le cas échéant) restent sur l'appareil. Ensuite, si l'appareil est toujours visible pour le Serveur d'administration et que vous avez configuré le sondage du réseau régulier, Kaspersky Security Center découvre l'appareil lors du sondage du réseau et l'ajoute au groupe Appareils non définis. Par conséquent, il est raisonnable de supprimer un appareil manuellement uniquement si l'appareil est invisible pour le Serveur d'administration.

Suppression d'un objet

Vous pouvez supprimer des objets comme les stratégies, les tâches, les paquets d'installation, les utilisateurs internes et groupes de sécurité internes si vous possédez la permission Modifier, qui se trouve dans la catégorie de privilèges Fonctionnalité de base (consultez l'article Attribution des permissions aux utilisateurs et aux groupes pour en savoir plus).

Vous ne pouvez pas supprimer les paquets d'installation utilisés dans les tâches d'installation à distance. Vous devez d'abord arrêter les tâches correspondantes. Pour en savoir plus à propos des tâches d'installation automatique dans un groupe d'administration, consultez l'article Installation automatique des applications sur les appareils du groupe d'administration.

Pour supprimer un objet, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez un objet dans l'espace de travail du dossier requis.
2. Exécutez une des actions suivantes :
   - Faites un clic droit sur l'objet et sélectionnez **Supprimer**.
   - Cliquez sur la touche **DEL**.

L'objet est supprimé et les informations à son sujet sont conservées dans la base de données.

Consultation des informations relatives aux objets supprimés

Les informations relatives aux objets supprimés sont stockées dans le dossier Objets supprimés pendant la même durée que les révision de l'objet (la période recommandée est de 90 jours).

Seuls les utilisateurs avec des permissions de **Lire** dans la section **Objets supprimés** des autorisations peuvent voir la liste des objets supprimés (cf. Attribution des permissions aux utilisateurs et aux groupes pour en savoir plus).

Pour consulter la liste des Supprimer les objets reçues,

Dans l'arborescence de la console, sélectionnez **Objets supprimés** (par défaut, **Objets supprimés** est un sous-dossier du dossier **Avancé**).

Si vous ne disposez pas des permissions de lecture dans la section **Objets supprimés**, une liste vide apparaît dans le dossier **Objets supprimés**.

L'espace de travail du dossier **Objets supprimés** contient les informations suivantes au sujet des objets supprimés :

- **Nom**. Le nom de la Objet.
- **Type**. Le type d'objet comme stratégie, tâche ou paquet d'installation.

- **Heure**. L'heure de détection de l'objet.
- **Utilisateur**. Compte utilisateur le nom de l'utilisateur ayant Supprimé l'objet.

Pour voir les détails d'un objet :

1. Dans l'arborescence de la console, sélectionnez **Objets supprimés** (par défaut, **Objets supprimés** est un sous-dossier du dossier **Avancé**).
2. Dans l'espace de travail **Objets supprimés**, sélectionnez l'objet que vous souhaitez supprimer.

   La zone qui permet de manipuler l'objet sélectionné apparaît du côté droit de l'espace de travail.
3. Exécutez une des actions suivantes :
   - Cliquez sur le lien **Propriétés** dans la fenêtre.
   - Cliquez-droit sur l'objet sélectionné dans l'espace de travail, puis sélectionnez **Propriétés** dans le menu contextuel.

   La fenêtre des propriétés de la Objet s'ouvre. Cette fenêtre affiche les informations suivantes :
   - **Général**
   - **Historique des révisions**

Suppression permanente des objets dans la liste des objets supprimés

Seuls les utilisateurs dotés de permissions de **modification** dans la section **Objets supprimés** des permissions peuvent supprimer définitivement des objets dans la liste des objets supprimés (cf. Attribution des permissions aux utilisateurs et aux groupes pour les détails).

Pour supprimer un objet de la liste des objets supprimés :

1. Dans l'arborescence de la console, sélectionnez l'entrée du Serveur d'administration requis, puis sélectionnez le dossier **Objets supprimés**.
2. Dans la Espace de travail des tâches, sélectionnez la Objet() vous souhaitez supprimer.
3. Exécutez une des actions suivantes :
   - Cliquez sur la touche **DEL**.
   - Dans le menu contextuel du ou des objets que vous avez sélectionnés, choisissez l'option **Supprimer**.
4. Dans la boîte de dialogue de confirmation, cliquez sur **Oui**.

   L'objet est supprimé de manière définitive de la liste des objets supprimés. Toutes les informations relatives à cet objet (y compris toutes ses révisions) sont supprimées définitivement de la base de données. Il est impossible de rétablir ces informations.

Administration des appareils mobiles

L'administration de la protection des appareils mobiles via Kaspersky Security Center est confiée à la Fonction Administration des appareils mobiles qui requiert une licence dédiée. Si vous avez l'intention d'administrer les appareils mobiles qui appartiennent aux employés de votre organisation, vous devez activer l'Administration des appareils mobiles.

Cette section explique comment activer, configurer et désactiver l'Administration des appareils mobiles. Cette section décrit également l'administration des appareils mobiles connectés au Serveur d'administration.

Pour en savoir plus sur Kaspersky Security for Mobile, consultez l'*aide de Kaspersky Security for Mobile*.

Scénario : déploiement de l'administration des appareils mobiles

Cette section fournit un scénario pour configurer la fonctionnalité Administration des appareils mobiles dans Kaspersky Security Center.

Prérequis

Assurez-vous de disposer d'une licence qui donne accès à la fonction Administration des appareils mobiles.

Étapes

Le déploiement de la fonctionnalité d'administration des appareils mobiles se déroule par étapes :

1. **Préparation des ports**

   Assurez-vous que le port 13292 est disponible sur le Serveur d'administration. Ce port est requis pour la connexion d'appareils mobiles. De même, vous pouvez rendre le port 17100 disponible. Ce port n'est requis que pour le serveur proxy d'activation pour les appareils mobiles administrés ; si les appareils mobiles administrés ont un accès Internet, vous n'avez pas besoin de rendre ce port disponible.

2. **Activation de l'Administration des appareils mobiles**

   Vous pouvez activer l'administration des appareils mobiles lorsque vous exécutez l'Assistant de configuration initiale du Serveur d'administration ou plus tard.

3. **Indication de l'adresse externe du Serveur d'administration**

   Vous pouvez spécifier l'adresse externe lorsque vous exécutez l'Assistant de configuration initiale du Serveur d'administration ou ultérieurement. Si vous n'avez pas sélectionné Administration des appareils mobiles pour l'installation et n'avez pas spécifié l'adresse dans l'assistant d'installation, spécifiez l'adresse dans les propriétés du paquet d'installation.

4. **Ajout des appareils mobiles au groupe Appareils administrés**

   Ajout des appareils mobiles au groupe Appareils administrés pour pouvoir gérer ces appareils par les stratégies. Pour cela, vous pouvez créer une règle de déplacement pendant une des étapes de l'Assistant de configuration initiale du Serveur d'administration. Vous pouvez également créer cette règle ultérieurement. Si vous ne créez pas cette règle, vous pouvez ajouter manuellement des appareils mobiles au groupe Appareils administrés.

Vous pouvez ajouter directement des appareils mobiles au groupe Appareils administrés ou créer un ou plusieurs sous-groupes pour ces appareils.

Ultérieurement, vous pouvez à tout moment connecter tout nouvel appareil mobile au Serveur d'administration via l'Assistant de connexion d'un nouvel appareil mobile.

5. **Création d'une stratégie pour les appareils mobiles**

   Pour administrer des appareils mobiles, créez au moins une stratégie pour eux dans le groupe auquel ces appareils appartiennent. Vous pouvez modifier les paramètres de cette stratégie à tout moment ultérieurement.

Résultats

Après avoir terminé ce scénario, vous pouvez administrer des appareils mobiles Android et iOS avec Kaspersky Security Center. Vous pouvez traiter des certificats d'appareils mobiles et envoyer des commandes à des appareils mobiles.

À propos de la stratégie de groupe pour la gestion des appareils MDM iOS

Pour administrer les appareils MDM iOS, vous pouvez utiliser le plug-in d'administration Kaspersky Device Management for iOS inclus dans le kit de distribution de Kaspersky Security Center. Kaspersky Device Management for iOS permet de créer des stratégies de groupe pour la configuration des paramètres des appareils MDM iOS sans utiliser l'utilitaire de configuration de l'iPhone®.

Une stratégie de groupe pour l'administration des appareils MDM iOS offre les options suivantes à l'administrateur :

- Configurer les paramètres de sécurité de l'utilisation du mot de passe sur l'appareil.
- Configurer des restrictions pour l'utilisation des fonctions matérielles de l'appareil, ainsi que des restrictions relatives à l'installation et à la suppression d'apps mobiles.
- Configurer des restrictions pour l'utilisation des applications mobiles de série sur l'appareil. Par exemple, YouTube™, iTunes® Store ou Safari.
- Configurer des restrictions sur la consultation du contenu multimédia (par exemple, les films et les émissions télévisées) en fonction de la région où se trouve l'appareil.
- Configurer les paramètres de connexion à Internet via le serveur proxy (proxy HTTP mondial).
- Configurer les paramètres du compte utilisateur unique via lequel l'utilisateur accède aux applications et aux services d'entreprise (technologie d'authentification unique).
- Contrôler l'utilisation d'Internet (sites Internet consultés) sur les appareils mobiles.
- Configurer les paramètres des réseaux sans fil (Wi-Fi), des points d'accès (APN) et des réseaux privés virtuels (VPN) à l'aide de différents mécanismes d'authentification et protocoles réseau.
- Configurer les paramètres de connexion aux appareils AirPlay® pour la transmission de photographies, de musique et de vidéos sur le réseau.
- Configurer les paramètres de connexion aux imprimantes AirPrint™ pour l'impression sans fil de documents à partir de l'appareil.
- Configurer les paramètres de synchronisation avec le serveur Microsoft Exchange et les comptes utilisateurs pour la messagerie d'entreprise sur les appareils.

- Configurer les identifiants de l'utilisateur pour la synchronisation à partir du service des catalogues LDAP.
- Configurer les identifiants de l'utilisateur pour la connexion aux services CalDAV et CardDAV, ce qui permet à l'utilisateur d'exploiter les calendriers et listes de contacts de l'entreprise.
- Configurer les paramètres de l'interface iOS sur l'appareil de l'utilisateur, par exemple les polices et les icônes pour certains sites Internet.
- Ajouter de nouveaux certificats de sécurité à l'appareil.
- Configuration des paramètres du serveur Simple Certificate Enrollment Protocol SCEP pour que l'appareil récupère automatiquement les certificats à partir du Centre de certification.
- Ajouter des paramètres spécifiques pour le fonctionnement des apps mobiles.

La particularité de la stratégie d'administration des appareils MDM iOS repose dans son attribution à un groupe d'administration intégrant le Serveur MDM iOS (ci-après, le « serveur des appareils mobiles »). Tous les paramètres définis dans la stratégie sont d'abord diffusés sur le serveur des appareils mobiles, puis sur les appareils mobiles administrés via ces serveurs. En cas d'utilisation d'une structure hiérarchisée de groupes d'administration, les serveurs secondaires des appareils mobiles y étant rattachés reçoivent les paramètres de la stratégie en provenance des serveurs principaux des appareils mobiles, puis les diffusent sur les appareils mobiles.

Pour en savoir plus sur l'utilisation d'une stratégie de groupe pour l'administration des appareils MDM iOS dans la Console d'administration de Kaspersky Security Center, consultez la documentation *Kaspersky Security for Mobile*.

Activation de l'Administration des appareils mobiles

Pour administrer les appareils mobiles, il faut activer l'Administration des appareils mobiles. Si vous n'aviez pas activé cette fonction dans l'Assistant de configuration initiale de l'application, vous pouvez l'activer plus tard. L'administration des appareils mobiles requiert une licence.

L'activation de l'Administration des appareils mobiles est accessible uniquement sur le Serveur d'administration principal.

Pour activer l'Administration des appareils mobiles :

1. Dans l'arborescence de la console, sélectionnez le dossier **Administration des appareils mobiles**.
2. Dans l'espace de travail du dossier, cliquez sur le bouton **Activez l'Administration des appareils mobiles**. Ce bouton est disponible uniquement si vous n'avez pas encore activé **Administration des appareils mobiles**.

   La page **Modules complémentaires** de l'Assistant de configuration initiale du Serveur d'administration s'ouvre.
3. Sélectionnez **Activez l'Administration des appareils mobiles** afin d'administrer les appareils mobiles.
4. Sur la page **Sélection de la méthode d'activation de l'application**, activez l'application à l'aide d'un fichier clé ou d'un code d'activation.

   L'administration des appareils mobiles n'est pas possible tant que la fonction Administration des appareils mobiles n'a pas été activée.

5. Sur la page **Paramètres du serveur proxy pour accéder à Internet**, sélectionnez la case à cocher **Utiliser un serveur proxy** si vous voulez activer la possibilité de connexion à Internet via le serveur proxy. Si la case est cochée, les champs de saisie des paramètres sont accessibles. Configurez les paramètres de connexion au serveur proxy.

6. Sur la page **Recherche de mises à jour pour les plug-ins et les paquets d'installation**, sélectionnez l'une des options suivantes :

   - **Vérifier &que les plug-ins et les paquets d'installation sont à jour**

     Lancement de la vérification de l'actualité. Si la vérification détecte l'utilisation de versions obsolètes des plug-ins ou des paquets d'installation, l'Assistant propose de charger les versions actuelles au lieu des anciennes.

   - **&Ignorer l'analyse**

     Poursuite du travail sans vérifier que les plug-ins et les paquets d'installation sont à jour. Choisissez cette option, par exemple, si vous n'avez pas accès Internet ou si vous souhaitez, pour une raison quelconque, continuer à utiliser l'ancienne version de l'application.

     Si vous ignorez la vérification de l'actualité des plug-ins, l'application risque de ne pas fonctionner correctement.

7. Sur la page **Dernières versions disponibles des plug-ins**, chargez et installez les dernières versions des plug-ins dans la langue que la version de votre application exige. La mise à jour des plug-ins ne requiert pas de licence.

   Après l'installation des plug-ins et des paquets, l'application vérifie si tous les plug-ins indispensables au bon fonctionnement des appareils mobiles ont été installés. Si des versions dépassées de plug-ins sont détectées, l'Assistant propose de télécharger les versions actuelles au lieu des anciennes.

8. Sur la page **Paramètres de connexion des appareils mobiles**, configurez les ports du Serveur d'administration.

À la fin de l'Assistant, les modifications suivantes sont apportées :

- La stratégie Kaspersky Endpoint Security for Android est créée.
- Une stratégie Kaspersky Device Management for iOS est créée.
- Les ports sont ouverts pour le Sur le Serveur d'administration pour les appareils mobiles.

Modification des paramètres de l'Administration des appareils mobiles

Pour activer la prise en charge des appareils mobiles, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le dossier **Administration des appareils mobiles**.

2. Dans l'espace de travail du dossier, cliquez sur le lien **Ports de connexion pour appareils mobiles**.

   La section **Ports supplémentaires** de la fenêtre des propriétés du Serveur d'administration s'affiche.

3. Dans la section **Ports supplémentaires**, modifiez les paramètres nécessaires :

   - **Port SSL pour le serveur proxy d'activation**
   - **Ouvrir le port pour les appareils mobiles**

     Un port s'ouvre pour les appareils mobiles en vue de la connexion au serveur de licences. Vous pouvez définir le numéro du port et d'autres paramètres dans les champs plus bas.

     Cette option est activée par défaut.

   - **Port pour la synchronisation des appareils mobiles**

     Numéro du port utilisé pour la connexion des appareils mobiles au Serveur d'administration et l'échange d'informations avec ceux-ci. Le numéro de port par défaut est 13292.

     Vous pouvez désigner un autre port, si le port 13292 est utilisé à d'autres fins.

   - **Port pour l'activation des appareils mobiles**

     Port de connexion de Kaspersky Endpoint Security for Android aux serveurs d'activation de Kaspersky.

     Le numéro de port par défaut est 17100.

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

Désactivation de l'Administration des appareils mobiles

La désactivation de l'Administration des appareils mobiles est accessible uniquement sur le Serveur d'administration principal.

Pour désactiver l'Administration des appareils mobiles :

1. Dans l'arborescence de la console, sélectionnez le dossier **Administration des appareils mobiles**.
2. Dans l'espace de travail de ce dossier, cliquez sur le lien **Configurer les modules complémentaires**.

   La page **Modules complémentaires** de l'Assistant de configuration initiale du Serveur d'administration s'ouvre.
3. Sélectionnez **&Ne pas activer l'administration des appareils mobiles** si vous ne souhaitez plus administrer les appareils mobiles.
4. Cliquez sur le bouton **OK**.

Les appareils mobiles déjà connectés ne pourront plus se connecter au Serveur d'administration. Le port de connexion des appareils mobiles et le port d'activation des appareils mobiles seront fermés automatiquement.

Les stratégies Kaspersky Endpoint Security for Android et Kaspersky Device Management for iOS créées ne seront pas supprimées. Les règles d'émission des certificats ne sont pas modifiées. Les plug-ins installés ne sont pas supprimés. La règle de déplacement des appareils mobiles ne sera pas supprimée.

Après la nouvelle activation de l'Administration des appareils mobiles sur les appareils mobiles administrés, il peut être nécessaire de réinstaller les applications mobiles nécessaires à l'administration des appareils mobiles.

Utilisation des commandes pour les appareils mobiles

Cette section contient des informations sur les commandes d'administration des appareils mobiles prises en charge par Kaspersky Security Center. Elle comporte également des instructions relatives à l'envoi de commandes aux appareils mobiles et à la consultation de l'état de l'exécution de ces commandes dans le journal dédié.

Commandes d'administration des appareils mobiles

Kaspersky Security Center prend en charge les commandes d'administration des appareils mobiles.

Ces commandes sont utilisées pour assurer l'administration à distance des appareils mobiles. Par exemple, si l'appareil mobile a été perdu, une commande vous permet de supprimer les données d'entreprise qu'il contient.

Vous pouvez utiliser les commandes pour les types de appareils mobiles administrés suivants :

- Appareils MDM iOS
- Appareils KES

Chaque type d'appareil prend en charge son propre ensemble de commandes.

Particularités de certaines commandes

- Tous les appareils visés par la commande **Rétablir les paramètres par défaut** verront toutes leurs données supprimées et leurs paramètres réinitialisés en configuration de sortie d'usine.
- Les appareils MDM iOS visés par la commande **&Supprimer les données d'entreprise** verront tous leurs profils de configuration, provisioning, MDM iOS et toutes leurs applications supprimés si la case **Supprimer avec le profil MDM iOS** avait été cochée pour chacun d'entre eux.
- Les appareils KES visés par la commande **&Supprimer les données d'entreprise** verront leurs données d'entreprise, leurs entrées dans les Contacts, leur historique des SMS, leur journal des appels, leur calendrier, leurs paramètres de connexion à Internet et leurs comptes utilisateurs (sauf leur compte utilisateur Google™) supprimés. Les appareils KES verront également les données de leur carte mémoire supprimées.
- Avant d'envoyer la commande **Géolocaliser** à un appareil KES, il faut confirmer que vous utilisez cette commande pour la recherche autorisée d'un appareil égaré appartenant à votre société ou à un de vos employés. L'appareil mobile qui reçoit la commande **Géolocaliser** n'est pas verrouillé.

Liste des commandes pour les appareils mobiles

Le tableau ci-dessous reprend la liste des commandes pour les appareils MDM iOS.

Commandes prises en charge pour l'administration des appareils mobiles : appareils MDM iOS

Commandes	Résultat de la commande
Verrouiller	L'appareil mobile est bloqué.
Déverrouiller	Le verrouillage d'appareil mobile est activé par le code PIN. Le code PIN installé précédemment est réinitialisé.
Rétablir les paramètres par défaut	Toutes les données sont supprimées de l'appareil mobile, et les paramètres reprennent leur configuration d'usine.
&Supprimer les données d'entreprise	Suppression de tous les profils de configuration, de tous les profils provisioning, du profil MDM iOS et de toutes les applications dont la case **Supprimer avec le profil MDM iOS** avait été cochée.
Synchroniser l'appareil	Les données de l'appareil mobile sont synchronisées avec le Serveur d'administration.
Installer le profil	Le profil de configuration est installé sur l'appareil mobile.
Supprimer le profil	Le profil de configuration est supprimé de l'appareil mobile.
Installer le profil provisioning	Le profil provisioning est installé sur l'appareil mobile.
Supprimer le profil provisioning	Le profil provisioning est supprimé de l'appareil mobile.
Installer l'app	L'app est installée sur l'appareil mobile.
Supprimer l'app	L'app est supprimée de l'appareil mobile.
Saisir le code redemption	Saisit le code rédemption d'une app payante.
Configurer les paramètres d'itinérance	Active ou désactive l'itinérance des données et l'itinérance vocale.

Le tableau ci-dessous reprend la liste des commandes pour les appareils KES.

Commandes prises en charge pour l'administration des appareils mobiles : appareils KES

Commande	Résultat de la commande
Verrouiller	L'appareil mobile est bloqué.
Déverrouiller	Le verrouillage d'appareil mobile est activé par le code PIN. Le code PIN installé précédemment est réinitialisé.
Rétablir les paramètres par défaut	Toutes les données sont supprimées de l'appareil mobile, et les paramètres reprennent leur configuration d'usine.
&Supprimer les données d'entreprise	Suppression des données d'entreprise, des entrées dans les Contacts, de l'historique des SMS, du journal des appels, du calendrier, des paramètres de connexion à Internet et des comptes utilisateurs, sauf le compte utilisateur Google. Suppression des données de la carte mémoire.
Synchroniser l'appareil	Les données de l'appareil mobile sont synchronisées avec le Serveur d'administration.
&Géolocaliser l'appareil	L'appareil mobile est géolocalisé sur une carte Google Maps™. L'opérateur de téléphonie mobile facture l'envoi de SMS et l'utilisation d'Internet.
Photo furtive	L'appareil mobile est bloqué. Une photographie est prise avec l'appareil photo frontal de l'appareil et enregistrée sur le Serveur d'administration. Les photographies peuvent être consultées dans le journal des commandes. L'opérateur de téléphonie mobile facture l'envoi de SMS et l'utilisation d'Internet.
Alarme	L'appareil mobile émet une alarme.

Utilisation de Firebase Cloud Messaging

Pour une livraison opportune des commandes sur les appareils KES sous le système d'exploitation Android, le mécanisme des notifications push est utilisé dans Kaspersky Security Center. Les notifications push entre les appareils KES et le Serveur d'Administration sont échangées à l'aide de Firebase Cloud Messaging (ci-après dénommé FCM). La Console d'administration de Kaspersky Security Center permet d'indiquer les paramètres du service Firebase Cloud Messaging pour connecter les appareils KES à ce service.

Pour obtenir les paramètres de Firebase Cloud Messaging, vous devez avoir un compte utilisateur Google.

Pour activer FCM, procédez comme suit :

1. Dans la Console d'administration, sélectionnez l'entrée **Administration des appareils mobiles**, puis le dossier **Appareils mobiles**.
2. Dans le menu contextuel du dossier **Appareils mobiles**, sélectionnez l'option **Propriétés**.
3. Dans les propriétés du dossier, sélectionnez la section **Paramètres de Firebase Cloud Messaging**.
4. Dans le champ **Numéro de projet Firebase**, indiquez l'identificateur de l'expéditeur de FCM.
5. Dans le champ **Fichier clé privé (au format JSON)**, sélectionnez le fichier de clé privée.

   Lors de la synchronisation suivantes avec le Serveur d'administration, les appareils administrés KES sous le système d'exploitation Android seront connectés au service Firebase Cloud Messaging.

Vous pouvez modifier les paramètres de Firebase Cloud Messaging à l'aide du bouton **Abandonner les paramètres**.

Envoi d'une commande

Pour envoyer la commande à l'appareil mobile de l'utilisateur, procédez comme suit :

1. Dans le dossier **Administration des appareils mobiles** de l'arborescence de la console, sélectionnez le sous-dossier **Appareils mobiles**.

   La liste des appareils mobiles administrés s'affiche dans l'espace de travail du dossier.
2. Sélectionnez l'appareil mobile de l'utilisateur qui doit recevoir la commande.
3. Dans le menu contextuel de l'appareil mobile, sélectionnez l'option **Afficher le journal des commandes**.

4. Dans la fenêtre **Commandes pour l'administration des appareils mobiles**, passez à la section portant le nom de la commande qui doit être envoyée sur l'appareil mobile, puis cliquez sur le bouton **Envoyer la commande**.

   Selon la commande que vous avez sélectionnée, en cliquant sur le bouton **Envoyer la commande**, il est possible qu'une fenêtre de configuration des paramètres avancés de l'application s'ouvre. Par exemple, lors de l'envoi de la commande de suppression du profil provisioning sur l'appareil mobile, l'application propose de sélectionner le profil provisioning qui doit être supprimé. Dans la fenêtre, indiquez les paramètres avancés de la commande et confirmez votre choix. La commande sera ainsi envoyée à l'appareil mobile.

   Un clic sur le bouton **Renvoyer** permet de renvoyer la commande à l'appareil mobile de l'utilisateur.

   Le bouton **Mettre à jour de la file d'attente** permet d'annuler l'exécution de la commande envoyée si cette dernière n'a pas encore été exécutée.

   La section **Journal des commandes** affiche les commandes envoyées à l'appareil mobile et leurs états d'exécution respectifs. Cliquez sur le bouton **Actualiser** pour mettre à jour la liste des commandes.

5. Cliquez sur le bouton **OK** pour fermer la fenêtre **Commandes d'administration des appareils mobiles**.

Consultation de l'état des commandes dans le journal des commandes

L'application conserve les informations relatives à toutes les commandes envoyées aux appareils mobiles dans le journal des commandes. Le journal des commandes stocke des données telles que la date et l'heure d'envoi des commandes à l'appareil mobile, l'état des commandes, et certains détails concernant le résultat de leur exécution. Par exemple, en cas d'échec d'exécution d'une commande, la cause de l'erreur apparaît dans ce journal. Les enregistrements sont conservés pendant 30 jours dans le journal des commandes.

Les commandes envoyées aux appareils mobiles peuvent présenter les états suivants :

- *En cours d'exécution* : la commande est envoyée à l'appareil mobile.
- *Terminée* : l'exécution de la commande a réussi.
- *Terminée avec une erreur* : échec de l'exécution de la commande.
- *Suppression en cours* : la commande est supprimée de la file d'attente des commandes envoyées à l'appareil mobile.
- *Supprimée* : la commande a bien été supprimée de la file d'attente des commandes envoyées à l'appareil mobile.
- *Suppression terminée sur une erreur* : la commande n'a pas pu être supprimée de la file d'attente des commandes envoyées à l'appareil mobile.

L'application tient un journal des commandes pour chaque appareil mobile.

Pour consulter le journal des commandes envoyées sur l'appareil mobile, procédez comme suit :

1. Dans le dossier **Administration des appareils mobiles** de l'arborescence de la console, sélectionnez le sous-dossier **Appareils mobiles**.

   La liste des appareils mobiles administrés s'affiche dans l'espace de travail du dossier.

2. Dans la liste, sélectionnez l'appareil mobile dont vous souhaitez consulter le journal des commandes.

3. Dans le menu contextuel de l'appareil mobile, sélectionnez l'option **Afficher le journal des commandes**.

   La fenêtre **Commandes d'administration des appareils mobiles** s'ouvre. Les sections de la fenêtre **Commandes d'administration des appareils mobiles** comportent les commandes qu'il est possible d'envoyer à l'appareil mobile.

4. Sélectionnez les sections comportant les commandes dont vous avez besoin et consultez les informations relatives à leur envoi et à leur exécution dans la section **Journal des commandes**.

La section **Journal des commandes** permet de consulter la liste des commandes envoyées à l'appareil mobile et les informations les concernant. Le filtre **Afficher les commandes** vous permet d'afficher uniquement les commandes ayant le statut sélectionné dans la liste.

Utilisation des certificats d'appareils mobiles

Cette section contient les informations sur l'utilisation de certificats des appareils mobiles.

Le certificat racine pour appareils mobiles a une durée de validité fixe de 700 jours après sa création. Le certificat de réserve est généré 60 jours avant la date d'expiration. Vous pouvez modifier la période de formation du certificat de réserve à l'aide de la commande suivante :

```
klscflag.exe -fset -pv klserver -n KLSRV_AKLWNGT_MDM_CERT_CHANGE_TIMEOUT -t d -v <délai d'attente en secondes>
```

La période de formation du certificat de réserve doit être suffisamment longue pour que tous les appareils mobiles administrés puissent se synchroniser avec le Serveur d'administration et récupérer le certificat.

L'utilitaire klsclag se trouve dans le dossier dans lequel le Serveur d'administration est installé. Chemin d'installation par défaut est <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

Le renouvellement manuel du certificat racine pour les appareils mobiles n'est pas pris en charge.

Lancement de l'Assistant d'installation des certificats

Vous pouvez installer les types suivants de certificats sur l'appareil mobile d'un utilisateur :

- Certificats généraux pour l'identification de l'appareil mobile
- Certificats de messagerie pour la configuration de la messagerie corporative sur l'appareil mobile
- Certificat VPN pour la configuration de l'accès au réseau privé virtuel sur l'appareil mobile

Pour installer le certificat sur l'appareil mobile de l'utilisateur, procédez comme suit :

1. Dans l'arborescence de la console, développez le dossier **Administration des appareils mobiles** et sélectionnez le sous-dossier **Certificats**.

2. Dans l'espace de travail du dossier **Certificats**, cliquez sur le lien **Ajouter un certificat** pour exécuter l'Assistant d'installation des certificats.

Suivez les instructions de l'assistant.

A la fin de l'exécution de l'Assistant, le certificat sera créé et ajouté à la liste des certificats de l'utilisateur. De plus, l'utilisateur recevra une notification contenant un lien pour qu'il puisse télécharger et installer le certificat sur son appareil mobile. Vous pouvez consulter la liste de tous les certificats utilisateur et l'exporter dans un fichier. Il est également possible de supprimer et d'octroyer à nouveau les certificats, ainsi que de consulter leurs propriétés.

Étape 1. Sélection du type de certificat

Indiquez le type du certificat qu'il est nécessaire d'installer sur l'appareil mobile de l'utilisateur :

- **Certificat mobile** : pour l'identification de l'appareil mobile
- **Certificat de messagerie** : pour la configuration de la messagerie d'entreprise sur l'appareil mobile
- **Certificat VPN** : pour la configuration de l'accès au réseau privé virtuel sur l'appareil mobile

Étape 2. Séléction du type d'appareil

Cette fenêtre apparaît uniquement si vous avez sélectionné **Certificat de messagerie** ou **Certificat VPN** comme type de certificat.

Indiquez le type de système d'exploitation de l'appareil :

- **Appareil MDM iOS**. Choisissez cette option s'il est nécessaire d'installer le certificat sur l'appareil mobile qui se connecte au serveur MDM iOS selon le protocole MDM iOS.
- **Appareil KES administré par Kaspersky Security for Mobile**. Choisissez cette option s'il est nécessaire d'installer le certificat sur l'appareil KES. Dans ce cas, le certificat sera utilisé lors de la connexion au Serveur d'administration pour l'identification de l'utilisateur.
- **Appareil KES connecté au Serveur d'administration sans authentification par certificat utilisateur**. Choisissez cette option s'il est nécessaire d'installer le certificat sur l'appareil KES sans authentification selon le certificat. Dans ce cas, à l'étape finale de l'Assistant, dans la fenêtre **Mode de notification des utilisateurs**, l'administrateur doit choisir le type d'authentification utilisateur utilisé à chaque connexion au Serveur d'administration.

Étape 3. Sélection d'un utilisateur

Choisissez dans la liste les utilisateurs, les groupes de sécurité ou les groupes de sécurité Active Directory pour lesquelles vous voulez installer le certificat.

Dans la fenêtre **Choix de l'utilisateur**, vous pouvez exécuter la recherche des utilisateurs internes de Kaspersky Security Center. Vous pouvez cliquer sur **Ajouter** pour ajouter un utilisateur interne.

Étape 4. Sélection de la source du certificat

Dans la fenêtre, vous pouvez choisir la source du certificat à l'aide de laquelle le Serveur d'administration identifie l'appareil mobile. Vous pouvez définir le certificat de l'une des manières suivantes :

- Créer automatiquement un certificat à l'aide du Serveur d'administration et l'ajouter à l'appareil.
- Désignez le fichier d'un certificat créé au préalable. Cette méthode n'est pas accessible si plusieurs utilisateurs ont été choisi à l'étape précédente.

Cochez la case **Publier le certificat** s'il faut envoyer à l'utilisateur une notification sur la création d'un certificat pour son appareil mobile.

Si l'appareil mobile de l'utilisateur bénéficiait déjà d'une authentification par certificat, et qu'il est donc inutile d'indiquer le nom du compte utilisateur et le mot de passe pour obtenir un nouveau certificat, décochez la case **Publier le certificat**. Dans ce cas, la fenêtre **Mode de notification des utilisateurs** ne s'affiche pas.

Étape 5. Attribution d'un tag au certificat

La fenêtre **Tag de certificat** s'affiche, si dans la fenêtre **Type d'appareil**, vous avez choisi l'option **Appareil MDM iOS**.

La liste déroulante permet de désigner un tag pour le certificat de l'appareil MDM iOS de l'utilisateur. Le certificat qui a reçu le tag peut avoir des paramètres spéciaux définis pour ce tag dans les propriétés de la stratégie de Kaspersky Device Management for iOS.

La liste déroulante propose les tags suivants : *Modèle de certificat 1*, *Modèle de certificat 2* et *Modèle de certificat 3*. Les paramètres de ces tags peuvent être modifiés dans les sections suivantes :

- Si l'option **Certificat de messagerie** a été sélectionnée dans la fenêtre **Type de certificat**, les tags peuvent être définis dans les propriétés du compte Exchange ActiveSync pour les appareils mobiles (**Appareils administrés** →**Stratégies** → Propriétés de la stratégie Kaspersky Device Management for iOS > Section **Exchange ActiveSync** → **Ajouter** → **Avancé**).
- Si l'option **Certificat VPN** a été sélectionnée dans la fenêtre **Type de certificat**, les tags de ce dernier peuvent être définis dans les propriétés du réseau VPN pour les appareils mobiles (**Appareils administrés** → **Stratégies** → Propriétés de la stratégie Kaspersky Device Management for iOS → section **VPN** → **Ajouter** → **Avancé**). La configuration des tags utilisés pour les certificats VPN n'est pas accessible si le type de connexion sélectionné pour le réseau VPN est L2TP, PPTP ou IPSec (Cisco).

Étape 6. Définition des paramètres d'édition du certificat

Cette fenêtre permet de définir les paramètres d'édition de certificat suivants :

- **Ne pas signaler le nouveau certificat à l'utilisateur**

  Activer cette option si vous ne souhaitez pas envoyer à l'utilisateur une notification sur la création d'un certificat pour l'appareil mobile de l'utilisateur. Dans ce cas, la fenêtre **Mode de notification de l'utilisateur** ne s'affiche pas.

  > Cette option est uniquement applicable aux appareils dotés de Kaspersky Endpoint Security for Android.

  Pensez à activer cette option, par exemple, si l'appareil mobile de l'utilisateur a déjà été authentifié via un certificat, si bien qu'il n'est pas nécessaire de définir un nom de compte et un mot de passe pour obtenir un nouveau certificat.

- **Autoriser l'appareil à recevoir plusieurs fois un seul certificat (uniquement pour les appareils sur lesquels Kaspersky Endpoint Security for Android est installé)**

  Activez cette option si vous souhaitez que Kaspersky Security Center envoie à nouveau automatiquement le certificat chaque fois qu'il est sur le point d'expirer ou qu'il est introuvable sur l'appareil cible.

  Le certificat est automatiquement renvoyé plusieurs jours avant la date d'expiration du certificat. Vous pouvez configurer ce délai dans la fenêtre Règles d'émission des certificats.

  Il peut arriver que le certificat soit introuvable sur l'appareil. Cela peut se produire, par exemple, quand l'utilisateur installe à nouveau l'application de sécurité de Kaspersky sur l'appareil ou lors de la réinitialisation des paramètres de l'appareil et des données. Dans ce cas, Kaspersky Security Center vérifie l'Identificateur de l'appareil à la prochaine tentative de connexion de l'appareil au Serveur d'administration. Si l'appareil porte le même identificateur que lors de l'émission du certificat, l'application envoie à nouveau le certificat à l'appareil.

Étape 7. Sélection du mode de notification des utilisateurs

> Cette fenêtre ne s'affiche pas si vous avez sélectionné **Appareil MDM iOS** comme type d'appareil ou si vous avez sélectionné l'option **Ne pas signaler le nouveau certificat à l'utilisateur**.

La fenêtre **Mode de notification des utilisateurs** permet de configurer les notifications utilisateur concernant l'installation du certificat sur l'appareil mobile.

Indiquez le type d'authentification de l'utilisateur dans le champ **Méthode d'authentification** :

- **Identifiants (domaine ou alias)**

  Dans ce cas, l'utilisateur utilise le mot de passe de domaine ou le mot de passe de l'utilisateur interne de Kaspersky Security Center pour obtenir le nouveau certificat.

- **Mot de passe à usage unique**

  Dans ce cas, l'utilisateur obtient un mot de passe à usage unique qui est envoyé par email ou message SMS. Il conviendra de saisir ce mot de passe pour obtenir un nouveau certificat.

  Cette option devient **Mot de passe** si l'option **Autoriser l'appareil à recevoir plusieurs fois un seul certificat (uniquement pour les appareils dotés d'applications de sécurité pour appareils mobiles de Kaspersky)** a été activée dans la fenêtre **Paramètres d'édition de certificat**.

- **Mot de passe**

  Dans ce cas, le mot de passe est utilisé chaque fois que le certificat est envoyé à l'utilisateur.

  Cette option devient **Mot de passe à usage unique** lorsque l'option **Autoriser l'appareil à recevoir plusieurs fois un seul certificat (uniquement pour les appareils dotés d'applications de sécurité pour appareils mobiles de Kaspersky)** a été désactivée dans la fenêtre **Paramètres d'édition de certificat**.

Ce champ s'affiche si vous avez sélectionné **Certificat mobile** dans la fenêtre **Type de certificat** ou si vous avez sélectionné **Appareil KES connecté au Serveur d'administration sans authentification par certificat utilisateur** comme type d'appareil.

Sélectionnez l'option de notification de l'utilisateur :

- **Afficher le mot de passe d'authentification à la fin de l'Assistant**

  Si vous sélectionnez cette option, le nom d'utilisateur, le nom d'utilisateur dans SAM (Security Account Manager) et le mot de passe pour la récupération du certificat pour chacun des utilisateurs sélectionnés sera affiché à la dernière étape de l'Assistant d'installation des certificats. La configuration des paramètres de notification de l'utilisateur au sujet du certificat installé est inaccessible.

  Quand vous ajoutez des certificats pour plusieurs utilisateurs, vous pouvez enregistrer les identifiants fournis dans un fichier en cliquant sur le bouton **Exporter** à la dernière étape de l'Assistant d'installation des certificats.

  Cette option n'est pas disponible si vous avez choisi **Identifiants (domaine ou alias)** à l'étape **Mode de notification des utilisateurs** de l'Assistant d'installation des certificats.

- **Informer l'utilisateur à propos du nouveau certificat**

  Si vous choisissez cette option, vous pouvez Configurer les notifications de l'utilisateur au sujet du nouveau certificat.

  - **Par email**

    Le groupe de paramètres Par email permet de Configurer les notifications de l'utilisateur sur l'installation du certificat sur son appareil mobile via des messages électroniques. Ce mode de notification est disponible uniquement si un serveur SMTP a été configuré.

    Cliquez sur le lien **Modifier le message** pour voir et modifier le message si nécessaire.

  - **Par SMS**

    Ce groupe de paramètres permet de configurer la notification de l'utilisateur sur l'utilisation d'un SMS pour installer un certificat sur des appareils mobiles. Ce mode de notification est disponible uniquement si la notification par SMS a été configurée.

    Cliquez sur le lien **Modifier le message** pour voir et modifier le message si nécessaire.

Étape 8. Génération du certificat

À cette étape, le certificat est créé.

Vous pouvez cliquer sur **Terminer** pour quitter l'Assistant.

Le certificat est généré et affiché dans la liste de certificats de l'espace de travail du dossier **Certificats**.

Configurer les règles d'émission des certificats

Les certificats servent à authentifier les appareils sur le Serveur d'administration. Tous les appareils mobiles administrés doivent avoir des certificats. Vous pouvez configurer la façon dont les certificats sont émis.

Pour configurer les règles d'émission des certificats, procédez comme suit :

1. Dans l'arborescence de la console, développez le dossier **Administration des appareils mobiles** et sélectionnez le sous-dossier **Certificats**.

2. Dans l'espace de travail du dossier **Certificats**, cliquez sur le bouton **Configurer les règles d'émission des certificats** pour ouvrir la fenêtre **Règles d'émission des certificats**.

3. Affichez la section au nom du type du certificat :

   Émission des certificats de messagerie : pour configurer l'émission de certificats pour les appareils mobiles.

   Émission des certificats de messagerie : pour configurer l'émission de certificats de messagerie.

   Émission des certificats VPN : pour configurer l'émission de certificats VPN.

4. Dans le groupe **Paramètres d'émission**, configurez l'émission du certificat :

   - Indiquez la durée de validité du certificat en jours.

     Le nombre de certificats pour appareils mobiles est limité par la date d'expiration du certificat racine. Si vous définissez une durée de vie supérieure à la date d'expiration du certificat racine, la durée de vie du certificat est automatiquement ajustée lors de la création.

   - Sélectionnez une source de certificat (**Serveur d'administration** ou **Les certificats sont définis manuellement**).

     Le Serveur d'administration est sélectionné en tant que source de certificats par défaut.

   - Spécifiez un modèle de certificat (**Modèle par défaut**, **Autre modèle**).

     La configuration des modèles est accessible si, dans la section **Intégration avec PKI**, l'option Intégrer à l'infrastructure de clés ouvertes est activée.

5. Dans le groupe **Paramètres des mises à jour automatiques**, configurez la mise à jour automatique du certificat :

   - Dans le champ **Mettre à jour lorsqu'il reste le nombre de jours suivant avant la fin de la durée de validité du certificat (jours)**, indiquez le nombre de jours avant l'expiration auquel le certificat doit être renouvelé.

   - Pour activer les mises à jour automatiques des certificats, cochez la case **Réémettre automatiquement le certificat si possible**.

6. La section **Protection par mot de passe** permet d'activer et de configurer l'utilisation du mot de passe lors du déchiffrement des certificats.

   > La protection par mot de passe est uniquement disponible pour les certificats de messagerie.

   a. Cochez la case **Demander le mot de passe lors de l'installation du certificat**.

   b. Servez-vous du curseur pour configurer la quantité maximale de caractères dans le mot de passe de chiffrement.

7. Cliquez sur le bouton **OK**.

Intégration avec l'infrastructure à clé publique

Il est indispensable d'intégrer l'application à l'infrastructure à clé publique (Public Key Infrastructure, PKI) pour simplifier l'octroi des certificats aux utilisateurs de domaine. Suite à cette intégration, l'émission des certificats est automatique.

La version minimale prise en charge du serveur PKI est Windows Server 2008.

Il est indispensable de configurer un compte utilisateur pour l'intégration PKI. Ce compte utilisateur doit répondre aux conditions suivantes :

- Être utilisateur du domaine et administrateur de l'appareil hébergeant le Serveur d'administration.
- Disposer du privilège SeServiceLogonRight sur l'appareil hébergeant le Serveur d'administration.

Pour créer le profil permanent de l'utilisateur, il est nécessaire d'ouvrir au moins une fois une session du compte utilisateur configuré sur l'appareil hébergeant le Serveur d'administration. Installez le certificat de l'Agent d'enregistrement accordé par l'administrateur du domaine dans le stockage des certificats de cet utilisateur, sur l'appareil hébergeant le Serveur d'administration.

Pour configurer l'intégration avec l'infrastructure à clé publique, procédez comme suit :

1. Dans l'arborescence de la console, développez le dossier **Administration des appareils mobiles** et sélectionnez le sous-dossier **Certificats**.
2. Dans l'espace de travail, cliquez sur le bouton **Intégrer à l'infrastructure de clés ouvertes** pour ouvrir la section **Intégration avec PKI** de la fenêtre **Règles d'émission des certificats**.

   La section **Intégration avec PKI** de la fenêtre **Règles d'émission des certificats** s'ouvre.
3. Cochez la case **Intégrer la délivrance des certificats avec PKI**.
4. Dans le champ **Compte utilisateur**, indiquez le nom du compte utilisateur à utiliser pour l'intégration à l'infrastructure à clé publique.
5. Dans le champ **Mot de passe**, saisissez le mot de passe du domaine du compte utilisateur.
6. Dans la liste **Nom de modèle du certificat dans PKI**, sélectionnez le modèle de certificat qui servira de base à l'émission de certificats pour les utilisateurs du domaine.

   Un service dédié est exécuté dans Kaspersky Security Center sous le compte utilisateur défini. Ce service est responsable de l'émission des certificats de domaine des utilisateurs. Ce service est exécuté lors du téléchargement de la liste des modèles de certificats par un clic sur le bouton **Actualiser la liste** ou au moment de l'émission du certificat.
7. Cliquez sur le bouton **OK** afin d'enregistrer les paramètres.

Suite à cette intégration, l'émission des certificats est automatique.

Activation de la prise en charge de Kerberos Constrained Delegation

L'application prend en charge l'utilisation de Kerberos Constrained Delegation.

Pour activer la prise en charge de Kerberos Constrained Delegation, procédez comme suit :

1. Dans l'arborescence de la console ouvrez le dossier **Administration des appareils mobiles**.
2. Dans le dossier **Administration des appareils mobiles**, sélectionnez le sous-dossier **Serveurs des appareils mobiles**.
3. Dans l'espace de travail du dossier **Serveurs des appareils mobiles**, sélectionnez le Serveur MDM iOS.
4. Dans le menu contextuel du Serveur MDM iOS, sélectionnez l'option **Propriétés**.
5. Dans la fenêtre des propriétés du Serveur MDM iOS, sélectionnez la section **Paramètres**.
6. Dans la section **Paramètres**, cochez la case **Assurer la conformité avec Kerberos Constraint Delegation**.
7. Cliquez sur le bouton **OK**.

Ajout des appareils mobiles iOS à la liste des appareils administrés

Pour ajouter un appareil mobile iOS à la liste des appareils administrés, il faut ajouter et installer un certificat commun sur l'appareil. Les certificats communs sont utilisés par le Serveur d'administration pour identifier les appareils mobiles. Un certificat partagé pour un appareil mobile iOS est intégré au profil MDM iOS. Après l'ajout et l'installation d'un certificat partagé sur l'appareil mobile, celui-ci apparaît dans la liste des appareils administrés.

Kaspersky ne prend plus en charge Kaspersky Safe Browser.

Vous pouvez ajouter des appareils mobiles d'utilisateurs à la liste des appareils administrés à l'aide de l'Assistant de connexion d'un nouvel appareil mobile.

Pour connecter un appareil iOS au Serveur d'administration à l'aide d'un certificat partagé, procédez comme suit :

1. Démarrez l'Assistant de connexion d'un nouvel appareil mobile de l'une des manières suivantes :

   - Utilisez le menu contextuel dans le dossier **Comptes utilisateurs** :

     1. Dans l'arborescence de la console, ouvrez le dossier **Avancé** et sélectionnez le sous-dossier **Comptes utilisateurs**.

     2. Dans l'espace de travail du dossier **Comptes utilisateurs**, choisissez les utilisateurs, les groupes de sécurité ou les groupes de sécurité Active Directory auxquels vous souhaitez ajouter des appareils mobiles dans la liste des appareils administrés.

     3. Effectuez un clic droit et, dans le menu contextuel du compte utilisateur, sélectionnez **Ajouter un appareil mobile**.

        L'Assistant de connexion d'un nouvel appareil mobile démarre.

   - Dans l'espace de travail du dossier **Appareils mobiles**, cliquez sur le bouton **Ajouter un appareil mobile** :

     1. Dans l'arborescence de la console, développez le dossier **Administration des appareils mobiles** et sélectionnez le sous-dossier **Appareils mobiles**.

     2. Dans l'espace de travail du sous-dossier **Appareils mobiles**, cliquez sur le bouton **Ajouter un appareil mobile**.

        L'Assistant de connexion d'un nouvel appareil mobile démarre.

2. Dans la page **Système d'exploitation** de l'Assistant, sélectionnez **iOS** comme type de système d'exploitation de l'appareil mobile.

3. Sur la page **Sélection du Serveur MDM iOS**, sélectionnez le serveur MDM iOS.

4. Sur la page **Sélectionnez les utilisateurs dont vous souhaitez administrer les appareils mobiles**, sélectionnez les utilisateurs, les groupes de sécurité ou les groupes de sécurité Active Directory auxquels vous souhaitez ajouter des appareils mobiles dans la liste des appareils administrés.

   > Cette étape est ignorée si vous démarrez l'assistant en sélectionnant **Ajouter un appareil mobile** dans le menu contextuel du dossier **Comptes utilisateurs**.

   Si vous souhaitez ajouter un nouveau compte utilisateur à la liste, cliquez sur le bouton **Ajouter** et entrez les propriétés du compte utilisateur dans la fenêtre qui s'ouvre. Si vous souhaitez modifier ou consulter les propriétés du compte utilisateur, sélectionnez le compte utilisateur dans la liste et cliquez sur le bouton **Propriétés**.

5. Dans la page **Source du certificat** de l'Assistant, indiquez la méthode de création de certificat partagé que le Serveur d'administration va utiliser pour identifier l'appareil mobile. Il existe deux manières de fournir un certificat commun :

   - **Émettre le certificat via les outils du &Serveur d'administration**

     Sélectionnez cette option pour créer un nouveau certificat à l'aide des outils du Serveur d'administration si vous ne l'avez pas déjà créé.

     Si cette option est sélectionnée, le profil MDM iOS sera signé par le certificat généré automatiquement par le Serveur d'administration.

     Par défaut, cette option est sélectionnée.

   - **Indiquer le fichier du certificat**

     Sélectionnez cette option pour spécifier un fichier de certificat créé précédemment.

     Cette méthode n'est pas accessible si plusieurs utilisateurs ont été choisi à l'étape précédente.

6. Dans la page **Mode de notification des utilisateurs** de l'Assistant, configurez les paramètres de notification par message SMS ou email de l'utilisateur de l'appareil mobile de la création du certificat :

   - **Afficher le code QR dans l'assistant**

     En cas de sélection de cette option, le lien vers le paquet d'installation sera affiché à la dernière étape de l'Assistant de connexion d'un nouvel appareil mobile.

     Cette option est inaccessible si plusieurs utilisateurs ont été sélectionnés à l'étape précédente pour la connexion à l'appareil.

   - **Envoyer le code QR à l'utilisateur**

     Si vous choisissez cette option, vous pouvez configurer les notifications de l'utilisateur sur la connexion d'un nouvel appareil mobile.

     Il est possible de choisir le type d'adresse email, d'indiquer une adresse additionnelle et de modifier le texte du message. Il est également possible de choisir le type de téléphone de l'utilisateur pour l'envoi du message SMS, d'indiquer un numéro de téléphone supplémentaire et de modifier le texte du message SMS expédié.

     Si aucun serveur SMTP n'a été configuré, l'envoi de messages électroniques aux utilisateurs est impossible. Si la notification SMS n'est pas configurée, l'envoi de messages SMS aux utilisateurs est impossible.

7. Dans la page **Résultat** de l'Assistant, cliquez sur le bouton **Terminé** pour fermer l'Assistant.

Le profil MDM iOS est alors automatiquement publié sur le Serveur Web de Kaspersky Security Center. L'utilisateur de l'appareil mobile reçoit une notification avec un lien permettant de télécharger le profil MDM iOS sur le Serveur Web. L'utilisateur clique lui-même sur le lien reçu. Ensuite, le système d'exploitation de l'appareil mobile demande à l'utilisateur son accord pour l'installation du profil MDM iOS. Pour que le profil MDM iOS soit chargé sur l'appareil mobile, l'utilisateur doit accepter d'installer le profil MDM iOS. Après le téléchargement du profil MDM iOS et la synchronisation de l'appareil mobile avec le Serveur d'administration, l'appareil est affiché dans le sous-dossier **Appareils mobiles** du dossier **Administration des appareils mobiles** de l'arborescence de la console.

Pour que l'utilisateur puisse accéder au Serveur Web de Kaspersky Security Center via le lien reçu, l'appareil mobile doit pouvoir se connecter au Serveur d'administration sur le port 8061.

Ajout des appareils mobiles Android à la liste des appareils administrés

Pour ajouter un appareil mobile Android à la liste des appareils administrés, Kaspersky Endpoint Security for Android et un certificat partagé doivent être fournis et installés sur l'appareil mobile. Les certificats communs sont utilisés par le Serveur d'administration pour identifier les appareils mobiles. Après l'ajout et l'installation d'un certificat partagé sur l'appareil mobile, celui-ci apparaît dans la liste des appareils administrés.

Vous pouvez ajouter des appareils mobiles d'utilisateurs à la liste des appareils administrés à l'aide de l'Assistant de connexion d'un nouvel appareil mobile. L'Assistant propose deux options pour la livraison et l'installation d'un certificat partagé et de Kaspersky Endpoint Security for Android :

- Via un lien vers Google Play
- Via un lien à partir du Serveur Web de Kaspersky Security Center

  Le paquet d'installation de Kaspersky Endpoint Security for Android stocké pour distribution sur le Serveur d'administration est utilisé pour l'installation

Lancement de l'Assistant de connexion d'un nouvel appareil mobile

Pour lancer l'Assistant de connexion d'un nouvel appareil mobile, effectuez l'une des opérations suivantes :

- Utilisez le menu contextuel dans le dossier **Comptes utilisateurs** :

  1. Dans l'arborescence de la console, ouvrez le dossier **Avancé** et sélectionnez le sous-dossier **Comptes utilisateurs**.
  2. Dans l'espace de travail du dossier **Comptes utilisateurs**, choisissez les utilisateurs, les groupes de sécurité ou les groupes de sécurité Active Directory auxquels vous souhaitez ajouter des appareils mobiles dans la liste des appareils administrés.
  3. Effectuez un clic droit et, dans le menu contextuel du compte utilisateur, sélectionnez **Ajouter un appareil mobile**.

     L'Assistant de connexion d'un nouvel appareil mobile démarre.

- Dans l'espace de travail du dossier **Appareils mobiles**, cliquez sur le bouton **Ajouter un appareil mobile** :

  1. Dans l'arborescence de la console, développez le dossier **Administration des appareils mobiles** et sélectionnez le sous-dossier **Appareils mobiles**.
  2. Dans l'espace de travail du sous-dossier **Appareils mobiles**, cliquez sur le bouton **Ajouter un appareil mobile**.

     L'Assistant de connexion d'un nouvel appareil mobile démarre.

Ajout d'un appareil mobile Android à l'aide d'un lien Google Play

Pour installer Kaspersky Endpoint Security for Android et un certificat partagé sur un appareil mobile à l'aide d'un lien Google Play :

1. Lance l'Assistant de connexion d'un nouvel appareil mobile.
2. Dans la page **Système d'exploitation** de l'Assistant, sélectionnez **Android** comme type de système d'exploitation de l'appareil mobile.
3. Sur la page de l'Assistant **Méthode d'installation de Kaspersky Endpoint Security for Android sur les appareils**, sélectionnez **Télécharger l'application sur Google Play**.
4. Dans la page **Sélectionnez les utilisateurs dont vous souhaitez administrer les appareils mobiles**, choisissez les utilisateurs, les groupes de sécurité ou les groupes de sécurité Active Directory auxquels vous souhaitez ajouter des appareils mobiles dans la liste des appareils administrés.

   Cette étape est ignorée si l'assistant est démarré en sélectionnant **Ajouter un appareil mobile** dans le menu contextuel du dossier **Comptes utilisateurs**.

   Si vous souhaitez ajouter un nouveau compte utilisateur à la liste, cliquez sur le bouton **Ajouter** et entrez les propriétés du compte utilisateur dans la fenêtre qui s'ouvre. Si vous souhaitez modifier ou consulter les propriétés du compte utilisateur, sélectionnez le compte utilisateur dans la liste et cliquez sur le bouton **Propriétés**.
5. Dans la page **Source du certificat** de l'Assistant, indiquez la méthode de création de certificat partagé que le Serveur d'administration va utiliser pour identifier l'appareil mobile. Il existe deux manières de fournir un certificat commun :

   - **Émettre le certificat via les outils du &Serveur d'administration**

     Sélectionnez cette option pour créer un nouveau certificat à l'aide des outils du Serveur d'administration si vous ne l'avez pas déjà créé.

     Si cette option est sélectionnée, le certificat est automatiquement émis à l'aide des outils du Serveur d'administration.

     Par défaut, cette option est sélectionnée.

   - **Indiquer le fichier du certificat**

     Sélectionnez cette option pour spécifier un fichier de certificat créé précédemment.

     Cette méthode n'est pas accessible si plusieurs utilisateurs ont été choisi à l'étape précédente.

6. Dans la page **Mode de notification des utilisateurs** de l'Assistant, configurez les paramètres de notification par message SMS ou email de l'utilisateur de l'appareil mobile de la création du certificat :

   - **Afficher le code QR dans l'assistant**

     En cas de sélection de cette option, le lien vers le paquet d'installation sera affiché à la dernière étape de l'Assistant de connexion d'un nouvel appareil mobile.

     Cette option est inaccessible si plusieurs utilisateurs ont été sélectionnés à l'étape précédente pour la connexion à l'appareil.

   - **Envoyer le code QR à l'utilisateur**

     Si vous choisissez cette option, vous pouvez configurer les notifications de l'utilisateur sur la connexion d'un nouvel appareil mobile.

     Il est possible de choisir le type d'adresse email, d'indiquer une adresse additionnelle et de modifier le texte du message. Il est également possible de choisir le type de téléphone de l'utilisateur pour l'envoi du message SMS, d'indiquer un numéro de téléphone supplémentaire et de modifier le texte du message SMS expédié.

     Si aucun serveur SMTP n'a été configuré, l'envoi de messages électroniques aux utilisateurs est impossible. Si la notification SMS n'est pas configurée, l'envoi de messages SMS aux utilisateurs est impossible.

7. Dans la page **Résultat** de l'Assistant, cliquez sur le bouton **Terminé** pour fermer l'Assistant.

Suite au fonctionnement de l'assistant sur l'appareil mobile de l'utilisateur, un lien et un code QR seront envoyés pour le téléchargement de Kaspersky Endpoint Security for Android. L'utilisateur clique sur le lien et scanne le code QR. Ensuite, le système d'exploitation de l'appareil mobile demande à l'utilisateur son accord pour l'installation de Kaspersky Endpoint Security for Android. Après le téléchargement et l'installation de Kaspersky Endpoint Security for Android, l'appareil mobile se connecte au Serveur d'administration et télécharge le certificat commun. Après l'installation du certificat sur l'appareil mobile, celui-ci apparaît dans le dossier **Appareils mobiles**, lui-même sous-dossier du dossier **Administration des appareils mobiles** de l'arborescence de la console.

Ajout d'un appareil mobile Android à l'aide d'un lien depuis le Serveur Web de Kaspersky Security Center

Le paquet d'installation Kaspersky Endpoint Security for Android publié sur le Serveur d'administration est utilisé pour l'installation.

Pour installer Kaspersky Endpoint Security for Android et un certificat partagé sur un appareil mobile à l'aide d'un lien depuis un Serveur Web :

1. Lance l'Assistant de connexion d'un nouvel appareil mobile.

2. Dans la page **Système d'exploitation** de l'Assistant, sélectionnez **Android** comme type de système d'exploitation de l'appareil mobile.

3. Dans la fenêtre de l'Assistant **Méthode d'installation de Kaspersky Endpoint Security for Android sur les appareils**, sélectionnez **Télécharger le paquet d'installation de l'application à partir de Kaspersky Security Center**.

   Dans le champ qui apparaît ci-dessous, sélectionnez le paquet d'installation ou créez un nouveau paquet d'installation en cliquant sur **Nouvelle**.

4. Dans la page **Sélectionnez les utilisateurs dont vous souhaitez administrer les appareils mobiles**, choisissez les utilisateurs, les groupes de sécurité ou les groupes de sécurité Active Directory auxquels vous souhaitez ajouter des appareils mobiles dans la liste des appareils administrés.

   > Cette étape est ignorée si l'assistant est démarré en sélectionnant **Ajouter un appareil mobile** dans le menu contextuel du dossier **Comptes utilisateurs**.

   Si vous souhaitez ajouter un nouveau compte utilisateur à la liste, cliquez sur le bouton **Ajouter** et entrez les propriétés du compte utilisateur dans la fenêtre qui s'ouvre. Si vous souhaitez modifier ou consulter les propriétés du compte utilisateur, sélectionnez le compte utilisateur dans la liste et cliquez sur le bouton **Propriétés**.

5. Dans la page **Source du certificat** de l'Assistant, indiquez la méthode de création de certificat partagé que le Serveur d'administration va utiliser pour identifier l'appareil mobile. Il existe deux manières de fournir un certificat commun :

   - Émettre le certificat via les outils du &Serveur d'administration

     > Sélectionnez cette option pour créer un nouveau certificat à l'aide des outils du Serveur d'administration si vous ne l'avez pas déjà créé.
     >
     > Si cette option est sélectionnée, le certificat est automatiquement émis à l'aide des outils du Serveur d'administration.
     >
     > Par défaut, cette option est sélectionnée.

   - Indiquer le fichier du certificat

     > Sélectionnez cette option pour spécifier un fichier de certificat créé précédemment.
     >
     > Cette méthode n'est pas accessible si plusieurs utilisateurs ont été choisi à l'étape précédente.

6. Dans la page **Mode de notification des utilisateurs** de l'Assistant, configurez les paramètres de notification par message SMS ou email de l'utilisateur de l'appareil mobile de la création du certificat :

   - **Afficher le code QR dans l'assistant**

     En cas de sélection de cette option, le lien vers le paquet d'installation sera affiché à la dernière étape de l'Assistant de connexion d'un nouvel appareil mobile.

     Cette option est inaccessible si plusieurs utilisateurs ont été sélectionnés à l'étape précédente pour la connexion à l'appareil.

   - **Envoyer le code QR à l'utilisateur**

     Si vous choisissez cette option, vous pouvez configurer les notifications de l'utilisateur sur la connexion d'un nouvel appareil mobile.

     Il est possible de choisir le type d'adresse email, d'indiquer une adresse additionnelle et de modifier le texte du message. Il est également possible de choisir le type de téléphone de l'utilisateur pour l'envoi du message SMS, d'indiquer un numéro de téléphone supplémentaire et de modifier le texte du message SMS expédié.

     Si aucun serveur SMTP n'a été configuré, l'envoi de messages électroniques aux utilisateurs est impossible. Si la notification SMS n'est pas configurée, l'envoi de messages SMS aux utilisateurs est impossible.

7. Dans la page **Résultat** de l'Assistant, cliquez sur le bouton **Terminé** pour fermer l'Assistant.

Le paquet de l'application mobile Kaspersky Endpoint Security for Android est automatiquement publié sur le serveur Web de Kaspersky Security Center. Le paquet de l'application mobile contient l'app, les paramètres de connexion de l'appareil mobile au Serveur d'administration et le certificat. L'utilisateur de l'appareil mobile reçoit une notification contenant un lien pour télécharger le paquet sur le Serveur Web. L'utilisateur clique lui-même sur le lien reçu. Ensuite, le système d'exploitation de l'appareil invite l'utilisateur à accepter l'installation du paquet de l'application mobile. Si l'utilisateur est d'accord, le paquet est téléchargé sur l'appareil mobile. Après le téléchargement du paquet et la synchronisation avec le Serveur d'administration, l'appareil mobile est affiché dans le dossier **Appareils mobiles**, lui-même sous-dossier du dossier **Administration des appareils mobiles** de l'arborescence de la console.

Administration des appareils MDM iOS

Cette section décrit les options complémentaires d'administration des appareils MDM iOS à partir de Kaspersky Security Center. Pour administrer les appareils MDM iOS, l'application permet de :

- Configurer de manière centralisée les paramètres des appareils MDM iOS administrés et restreindre les fonctions de l'appareil à l'aide de profils de configuration. Vous pouvez ajouter et modifier les profils de configuration et installer des profils sur les appareils mobiles.
- Installer des apps sur les appareils mobiles, sans passer par l'App Store, à l'aide de profils provisioning. Les profils provisioning vous permettent par exemple d'installer sur les appareils mobiles des utilisateurs les apps d'entreprise conçues en interne. Le profil provisioning contient des informations sur l'app et sur l'appareil mobile.
- Installer une app sur l'appareil MDM iOS via l'App Store. L'app doit être ajoutée sur le Serveur MDM iOS avant son installation sur l'appareil MDM iOS.

Une notification PUSH est envoyée à tous les appareils MDM iOS connectés toutes les 24 heures pour synchroniser les données avec le Serveur MDM iOS.

Les informations relatives au profil de configuration, au profil provisioning et aux apps installées sur l'appareil MDM iOS, peuvent être consultées dans la fenêtre propriétés de l'appareil.

Signature d'un profil MDM iOS par un certificat

Vous pouvez signer un profil MDM iOS par un certificat. Vous pouvez utiliser un certificat que vous avez émis vous-même ou vous pouvez recevoir un certificat d'autorités de certification de confiance.

Les appareils iOS affichent un avertissement pour les profils non signés et invitent l'utilisateur à faire confiance au signataire lors de l'installation du profil.

Pour signer un profil MDM iOS par un certificat, procédez comme suit :

1. Dans le dossier **Administration des appareils mobiles** de l'arborescence de la console, sélectionnez le sous-dossier **Appareils mobiles**.
2. Dans le menu contextuel du dossier **Appareils mobiles**, sélectionnez l'option **Propriétés**.
3. Dans la fenêtre de propriétés du dossier, sélectionnez la section **Paramètres de connexion des appareils iOS**.
4. Cliquez sur le bouton **Parcourir** sous le champ **Sélectionner le fichier du certificat**.
   La fenêtre **Certificat**.
5. Dans le champ **Type de certificat**, sélectionnez le type de certificat ouvert ou fermé :
   - Si la valeur **Conteneur PKCS#12** est sélectionnée, indiquez le fichier de certificat et le mot de passe.
   - Si la valeur **Certificat X.509** est sélectionnée :
     a. Indiquez un fichier clé privée (avec l'extension prk ou pem).
     b. Indiquez le mot de passe de la clé privée.
     c. Indiquez un fichier clé publique (avec l'extension cer).
6. Cliquez sur le bouton **OK**.

Le profil MDM iOS est signé par un certificat.

Ajout du profil de configuration

Pour créer un profil de configuration, vous pouvez utiliser Apple Configurator 2, disponible sur le site Internet d'Apple Inc. Apple Configurator 2 fonctionne uniquement sur les appareils exécutant macOS ; si vous ne disposez pas de tels appareils, vous pouvez utiliser l'application iPhone Configuration Utility avec la Console d'administration à la place. Cependant, Apple Inc. ne prend plus en charge l'application iPhone Configuration Utility.

Pour créer le profil de configuration avec l'application iPhone Configuration Utility et l'ajouter sur le Serveur MDM iOS, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le dossier **Administration des appareils mobiles**.
2. Dans l'espace de travail du dossier **Administration des appareils mobiles**, sélectionnez le sous-dossier **Serveurs des appareils mobiles**.
3. Dans l'espace de travail du dossier **Serveurs des appareils mobiles**, sélectionnez le Serveur MDM iOS.
4. Dans le menu contextuel du Serveur MDM iOS, sélectionnez l'option **Propriétés**.

   La fenêtre des propriétés du Serveur des appareils mobiles s'ouvre.
5. Dans la fenêtre des propriétés du Serveur MDM iOS, sélectionnez l'option **Profils de configuration**.
6. Dans la section **Profils de configuration**, cliquez sur le bouton **Créer**.

   La fenêtre **Nouveau profil de configuration** s'ouvre.
7. Dans la fenêtre **Nouveau profil de configuration**, indiquez le nom et l'identificateur du profil.

   L'identificateur du profil de configuration doit être unique, la valeur de l'identificateur doit être définie au format Reverse-DNS, par exemple, *com.companyname.identifier*.
8. Cliquez sur le bouton **OK**.

   L'application iPhone Configuration Utility démarre alors si vous l'avez installée.
9. Exécutez la configuration des paramètres du profil dans l'application iPhone Configuration Utility.

   La description des paramètres du profil et les instructions de sa configuration sont décrites dans la documentation pour l'application iPhone Configuration Utility.

Après la configuration des paramètres du profil dans l'application iPhone Configuration Utility, un nouveau profil de configuration s'affiche dans la section **Profils de configuration** de la fenêtre des propriétés du Serveur MDM iOS.

Le bouton **Modifier** permet de modifier le profil de configuration.

Le bouton **Importer** permet de télécharger le profil de configuration dans l'application.

Le bouton **Exporter le filtre** permet d'enregistrer le profil de configuration dans un fichier.

Le profil que vous avez créé doit être installé sur les appareils MDM iOS.

Définition du profil de configuration sur l'appareil

Pour installer le profil de configuration sur l'appareil mobile, procédez comme suit :

1. Dans le dossier **Administration des appareils mobiles** de l'arborescence de la console, sélectionnez le sous-dossier **Appareils mobiles**.

   La liste des appareils mobiles administrés s'affiche dans l'espace de travail du dossier.
2. Dans l'espace de travail, filtrez les appareils MDM iOS par protocole d'administration *MDM iOS*.

3. Sélectionnez l'appareil mobile de l'utilisateur sur lequel vous devez installer le profil de configuration

   Vous pouvez sélectionner plusieurs appareils mobiles pour y installer le profil de façon simultanée.

4. Dans le menu contextuel de l'appareil mobile, sélectionnez l'option **Afficher le journal des commandes**.

5. Dans la fenêtre **Commandes d'administration des appareils mobiles**, ouvrez la section **Installer le profil** et cliquez sur le bouton **Envoyer la commande**.

   Vous pouvez également envoyer la commande à l'appareil mobile en sélectionnant l'option **Toutes les commandes** dans le menu contextuel de cet appareil mobile, puis **Installer le profil**.

   La fenêtre **Sélection des profils** s'ouvre, contenant une liste de profils. Dans la liste, sélectionnez le profil que vous devez installer sur l'appareil mobile. Vous pouvez sélectionner et installer simultanément plusieurs profils sur l'appareil mobile. Pour sélectionner une plage de profils, utilisez la touche **SHIFT**. Pour réunir des profils séparés dans un groupe, utilisez la touche **CTRL**.

6. Cliquez sur **OK** pour envoyer la commande à l'appareil mobile.

   Suite à l'exécution de cette commande, le profil de configuration sélectionné sera installé sur l'appareil mobile de l'utilisateur. Parallèlement, l'état de la commande du journal des commandes affichera la valeur *Progression*.

   Un clic sur le bouton **Renvoyer** permet de renvoyer la commande à l'appareil mobile de l'utilisateur.

   Le bouton **Mettre à jour de la file d'attente** permet d'annuler l'exécution de la commande envoyée si cette dernière n'a pas encore été exécutée.

   La section **Journal des commandes** affiche les commandes envoyées à l'appareil mobile et leurs états d'exécution respectifs. Cliquez sur le bouton **Actualiser** pour mettre à jour la liste des commandes.

7. Cliquez sur le bouton **OK** pour fermer la fenêtre **Commandes d'administration des appareils mobiles.**

Vous pouvez afficher le profil que vous avez installé et le retirer, si nécessaire.

Suppression du profil de configuration de l'appareil

Pour supprimer le profil de configuration de l'appareil mobile, procédez comme suit :

1. Dans le dossier **Administration des appareils mobiles** de l'arborescence de la console, sélectionnez le sous-dossier **Appareils mobiles**.

   La liste des appareils mobiles administrés s'affiche dans l'espace de travail du dossier.

2. Dans l'espace de travail, sélectionnez les appareils MDM iOS en cliquant sur le lien **MDM iOS**.

3. Sélectionnez l'appareil mobile de l'utilisateur duquel vous devez supprimer le profil de configuration.

   Vous pouvez sélectionner plusieurs appareils mobiles pour supprimer le profil de façon simultanée.

4. Dans le menu contextuel de l'appareil mobile, sélectionnez l'option **Afficher le journal des commandes**.

5. Dans la fenêtre **Commandes pour l'administration des appareils mobiles**, ouvrez la section **Supprimer le profil** et cliquez sur le bouton **Envoyer la commande**.

   Vous pouvez également envoyer la commande à l'appareil mobile en sélectionnant l'option **Toutes les commandes** dans le menu contextuel de cet appareil, puis **Supprimer le profil**.

   La fenêtre **Suppression des profils** s'ouvre, contenant une liste de profils.

6. Dans la liste, sélectionnez le profil que vous devez supprimer de l'appareil mobile. Vous pouvez sélectionner et supprimer simultanément plusieurs profils de l'appareil mobile. Pour sélectionner une plage de profils, utilisez la touche **SHIFT**. Pour réunir des profils séparés dans un groupe, utilisez la touche **CTRL**.

7. Cliquez sur **OK** pour envoyer la commande à l'appareil mobile.

   Suite à l'exécution de cette commande, le profil de configuration sélectionné sera supprimé de l'appareil mobile de l'utilisateur. Parallèlement, l'état de la commande affichera la valeur *Terminée*.

   Un clic sur le bouton **Renvoyer** permet de renvoyer la commande à l'appareil mobile de l'utilisateur.

   Le bouton **Mettre à jour de la file d'attente** permet d'annuler l'exécution de la commande envoyée si cette dernière n'a pas encore été exécutée.

   La section **Journal des commandes** affiche les commandes envoyées à l'appareil mobile et leurs états d'exécution respectifs. Cliquez sur le bouton **Actualiser** pour mettre à jour la liste des commandes.

8. Cliquez sur le bouton **OK** pour fermer la fenêtre **Commandes d'administration des appareils mobiles**.

Ajout d'un nouvel appareil à l'aide de la publication d'un lien vers le profil

L'administrateur crée un profil MDM iOS dans la Console d'administration à l'aide de l'Assistant d'installation des certificats. Suite à l'exécution de l'Assistant, les actions suivantes sont réalisées :

- Le profil MDM iOS est automatiquement publié sur le Serveur Web.
- L'utilisateur reçoit par message SMS ou par email un lien vers le profil MDM iOS. Après avoir reçu le lien, l'utilisateur installe le profil MDM iOS sur l'appareil mobile.
- L'appareil mobile est connecté au serveur MDM iOS.

Vu l'adoption par la société Apple d'une stratégie de sécurité plus stricte, il faut configurer les protocoles des versions TLS 1.1 et TLS 1.2 pour connecter un appareil mobile tournant sous iOS 11 au Serveur d'administration sur lequel l'intégration à Public Key Infrastructure (PKI) est configurée.

Ajout d'un nouvel appareil via l'installation d'un profil par l'administrateur

Pour connecter l'appareil mobile au serveur MDM iOS via l'installation du profil MDM iOS sur l'appareil mobile, l'administrateur doit réaliser les opérations suivantes :

1. Dans la Console d'administration, ouvrez l'Assistant d'installation des certificats.
2. Créez un nouveau profil MDM iOS en cochant la case **Afficher le certificat à la fin de l'Assistant** dans la fenêtre de l'Assistant.
3. Enregistrer le profil MDM iOS.
4. Installer le profil MDM iOS sur l'appareil mobile de l'utilisateur à l'aide de l'utilitaire Apple Configurator.

L'appareil mobile est connecté au serveur MDM iOS.

Vu l'adoption par la société Apple d'une stratégie de sécurité plus stricte, il faut configurer les protocoles des versions TLS 1.1 et TLS 1.2 pour connecter un appareil mobile tournant sous iOS 11 au Serveur d'administration sur lequel l'intégration à Public Key Infrastructure (PKI) est configurée.

Ajout d'un profil provisioning

Pour ajouter le profil provisioning sur le Serveur MDM iOS, procédez comme suit :

1. Dans l'arborescence de la console ouvrez le dossier **Administration des appareils mobiles**.
2. Dans le dossier **Administration des appareils mobiles**, sélectionnez le sous-dossier **Serveurs des appareils mobiles**.
3. Dans l'espace de travail du dossier **Serveurs des appareils mobiles**, sélectionnez le Serveur MDM iOS.
4. Dans le menu contextuel du Serveur MDM iOS, sélectionnez l'option **Propriétés**.

   La fenêtre des propriétés du Serveur des appareils mobiles s'ouvre.
5. Dans la fenêtre des propriétés du **Serveur MDM iOS**, sélectionnez l'option **Profils provisioning**.
6. Dans la section **Profils provisioning**, cliquez sur le bouton **Importer** et indiquez le chemin d'accès au fichier du profil provisioning.

Le profil sera ajouté dans les paramètres du Serveur MDM iOS.

Le bouton **Exporter le profil** permet d'enregistrer le profil provisioning dans un fichier.

Vous pouvez installer le profil provisioning que vous avez importé sur les appareils MDM iOS.

Définition du profil provisioning sur l'appareil

Pour installer le profil provisioning sur l'appareil mobile, procédez comme suit :

1. Dans le dossier **Administration des appareils mobiles** de l'arborescence de la console, sélectionnez le sous-dossier **Appareils mobiles**.

   La liste des appareils mobiles administrés s'affiche dans l'espace de travail du dossier.
2. Dans l'espace de travail, filtrez les appareils MDM iOS par protocole d'administration *MDM iOS*.
3. Sélectionnez l'appareil mobile de l'utilisateur sur lequel vous devez installer le profil provisioning.

   Vous pouvez sélectionner plusieurs appareils mobiles pour y installer le profil provisioning de façon simultanée.
4. Dans le menu contextuel de l'appareil mobile, sélectionnez l'option **Afficher le journal des commandes**.
5. Dans la fenêtre **Commandes pour l'administration des appareils mobiles**, ouvrez la section **Installer le profil provisioning** et cliquez sur le bouton **Envoyer la commande**.

   Vous pouvez également envoyer la commande à l'appareil mobile en sélectionnant l'option **Toutes les commandes** dans le menu contextuel de cet appareil mobile, puis **Installer le profil provisioning**.

   La fenêtre **Sélection des profils provisioning** s'ouvre, contenant la liste des profils provisioning. Dans la liste, sélectionnez le profil provisioning que vous devez installer sur l'appareil mobile. Vous pouvez sélectionner et installer plusieurs profils provisioning simultanément sur l'appareil mobile. Afin de sélectionner une plage de profils provisioning, utilisez la touche **SHIFT**. Afin de réunir des profils provisioning séparés dans un groupe, utilisez la touche **CTRL**.

6. Cliquez sur **OK** pour envoyer la commande à l'appareil mobile.

   Suite à l'exécution de cette commande, le profil provisioning sélectionné sera installé sur l'appareil mobile de l'utilisateur. Parallèlement, l'état de la commande du journal des commandes affiche la valeur *Terminée*.

   Un clic sur le bouton **Renvoyer** permet de renvoyer la commande à l'appareil mobile de l'utilisateur.

   Le bouton **Mettre à jour de la file d'attente** permet d'annuler l'exécution de la commande envoyée si cette dernière n'a pas encore été exécutée.

   La section **Journal des commandes** affiche les commandes envoyées à l'appareil mobile et leurs états d'exécution respectifs. Cliquez sur le bouton **Actualiser** pour mettre à jour la liste des commandes.

7. Cliquez sur le bouton **OK** pour fermer la fenêtre **Commandes d'administration des appareils mobiles.**

Vous pouvez afficher le profil que vous avez installé et le retirer, si nécessaire.

Suppression du profil provisioning de l'appareil

Pour supprimer un profil provisioning de l'appareil mobile, procédez comme suit :

1. Dans le dossier **Administration des appareils mobiles** de l'arborescence de la console, sélectionnez le sous-dossier **Appareils mobiles**.

   La liste des appareils mobiles administrés s'affiche dans l'espace de travail du dossier.

2. Dans l'espace de travail, filtrez les appareils MDM iOS par protocole d'administration *MDM iOS*.

3. Sélectionnez l'appareil mobile de l'utilisateur duquel vous devez supprimer le profil provisioning.

   Vous pouvez sélectionner plusieurs appareils mobiles pour supprimer le profil provisioning de façon simultanée.

4. Dans le menu contextuel de l'appareil mobile, sélectionnez l'option **Afficher le journal des commandes**.

5. Dans la fenêtre **Commandes pour l'administration des appareils mobiles**, ouvrez la section **Supprimer le profil provisioning** et cliquez sur le bouton **Envoyer la commande**.

   Vous pouvez également envoyer la commande à l'appareil mobile en sélectionnant l'option **Toutes les commandes** dans le menu contextuel de cet appareil, puis **Supprimer le profil provisioning**.

   La fenêtre **Suppression des profils provisioning** contient la liste des profils.

6. Dans la liste, sélectionnez le profil provisioning que vous devez supprimer de l'appareil mobile. Vous pouvez sélectionner et supprimer plusieurs profils provisioning simultanément de l'appareil mobile. Afin de sélectionner une plage de profils provisioning, utilisez la touche **SHIFT**. Afin de réunir des profils provisioning séparés dans un groupe, utilisez la touche **CTRL**.

7. Cliquez sur **OK** pour envoyer la commande à l'appareil mobile.

   Suite à l'exécution de cette commande, le profil provisioning sélectionné sera supprimé de l'appareil mobile de l'utilisateur. Les apps liées au profil provisioning supprimé ne fonctionneront plus. Parallèlement, l'état de la commande affichera la valeur *Terminée*.

   Un clic sur le bouton **Renvoyer** permet de renvoyer la commande à l'appareil mobile de l'utilisateur.

   Le bouton **Mettre à jour de la file d'attente** permet d'annuler l'exécution de la commande envoyée si cette dernière n'a pas encore été exécutée.

   La section **Journal des commandes** affiche les commandes envoyées à l'appareil mobile et leurs états d'exécution respectifs. Cliquez sur le bouton **Actualiser** pour mettre à jour la liste des commandes.

8. Cliquez sur le bouton **OK** pour fermer la fenêtre **Commandes d'administration des appareils mobiles**.

Ajout d'une app administrée

L'app doit être ajoutée sur le Serveur MDM iOS avant son installation sur l'appareil MDM iOS. L'app est administrée si elle a été installée sur l'appareil à l'aide de Kaspersky Security Center. Il est possible de gérer à distance les apps administrées à l'aide de Kaspersky Security Center.

Pour ajouter l'app administrée sur le Serveur MDM iOS, procédez comme suit :

1. Dans l'arborescence de la console ouvrez le dossier **Administration des appareils mobiles**.
2. Dans le dossier **Administration des appareils mobiles**, sélectionnez le sous-dossier **Serveurs des appareils mobiles**.
3. Dans l'espace de travail du dossier **Serveurs des appareils mobiles**, sélectionnez le Serveur MDM iOS.
4. Dans le menu contextuel du Serveur MDM iOS, sélectionnez l'option **Propriétés**.

   La fenêtre des propriétés du Serveur MDM iOS s'ouvre.
5. Dans la fenêtre des propriétés du Serveur MDM iOS, sélectionnez la section **Applications administrées**.
6. Cliquez sur le bouton **Ajouter** de la section **Applications administrées**.

   La fenêtre **Ajout de l'app** s'ouvre.
7. Dans la fenêtre **Ajout de l'app**, dans le champ **Nom de l'application**, indiquez le nom de l'application à ajouter.
8. Dans le champ **Apple ID ou le lien vers le fichier manifeste**, indiquez l'identifiant Apple de l'application à ajouter, ou le lien vers le fichier manifeste permettant de télécharger l'application.
9. Si vous souhaitez que l'application administrée soit supprimée de l'appareil mobile de l'utilisateur en même temps que le profil MDM iOS, cochez la case **Supprimer avec le profil MDM iOS**.
10. Si vous souhaitez interdire la sauvegarde des données de l'application via iTunes, cochez la case **Interdire la création des copies de sauvegarde des données**.
11. Cliquez sur le bouton **OK**.

L'application ajoutée s'affiche dans la section **Applications administrées** de la fenêtre des propriétés du Serveur MDM iOS.

Installation de l'app sur l'appareil mobile

Pour installer l'app sur l'appareil mobile MDM iOS, procédez comme suit :

1. Dans le dossier **Administration des appareils mobiles** de l'arborescence de la console, sélectionnez le sous-dossier **Appareils mobiles**.

   La liste des appareils mobiles administrés s'affiche dans l'espace de travail du dossier.
2. Sélectionnez l'appareil MDM iOS sur lequel vous devez installer l'app.

   Vous pouvez sélectionner plusieurs appareils mobiles pour y installer l'app en même temps.
3. Dans le menu contextuel de l'appareil mobile, sélectionnez l'option **Afficher le journal des commandes**.

4. Dans la fenêtre **Commandes pour l'administration des appareils mobiles**, ouvrez la section **Installer l'application** et cliquez sur le bouton **Envoyer la commande**.

   Vous pouvez également envoyer la commande à l'appareil mobile en sélectionnant **Toutes les commandes** dans le menu contextuel de cet appareil mobile, puis en sélectionnant **Installer l'application**.

   Cette opération ouvre la fenêtre **Sélection des applications** contenant la liste de profils. Dans la liste, sélectionnez l'app que vous devez installer sur l'appareil mobile. Vous pouvez sélectionner et installer plusieurs apps en même temps sur l'appareil mobile. Pour sélectionner une plage d'apps, utilisez la touche **SHIFT**. Pour regrouper plusieurs apps, utilisez la touche **CTRL**.

5. Cliquez sur le bouton **OK** pour envoyer la commande à l'appareil mobile.

   Suite à l'exécution de cette commande, l'app sélectionnée sera installée sur l'appareil mobile de l'utilisateur. Parallèlement, l'état de la commande du journal des commandes affiche la valeur *Terminée*.

   Un clic sur le bouton **Renvoyer** permet de renvoyer la commande à l'appareil mobile de l'utilisateur. Le bouton **Mettre à jour de la file d'attente** permet d'annuler l'exécution de la commande envoyée si cette dernière n'a pas encore été exécutée.

   La section **Journal des commandes** affiche les commandes envoyées à l'appareil mobile et leurs états d'exécution respectifs. Cliquez sur le bouton **Actualiser** pour mettre à jour la liste des commandes.

6. Cliquez sur le bouton **OK** pour fermer la fenêtre **Commandes d'administration des appareils mobiles.**

Les informations concernant les apps installées s'affichent dans les paramètres de l'appareil mobile MDM iOS. Vous pouvez supprimer une app à partir de l'appareil mobile à l'aide du journal des commandes ou à partir du menu contextuel de l'appareil mobile.

Suppression de l'app de l'appareil

Pour supprimer l'app de l'appareil mobile, procédez comme suit :

1. Dans le dossier **Administration des appareils mobiles** de l'arborescence de la console, sélectionnez le sous-dossier **Appareils mobiles**.

   La liste des appareils mobiles administrés s'affiche dans l'espace de travail du dossier.

2. Dans l'espace de travail, filtrez les appareils MDM iOS par protocole d'administration *MDM iOS*.

3. Sélectionnez l'appareil mobile de l'utilisateur contenant l'app à supprimer.

   Vous pouvez sélectionner plusieurs appareils mobiles pour supprimer l'app en même temps.

4. Dans le menu contextuel de l'appareil mobile, sélectionnez l'option **Afficher le journal des commandes**.

5. Dans la fenêtre **Commandes pour l'administration des appareils mobiles**, ouvrez la section **Supprimer l'application** et cliquez sur le bouton **Envoyer la commande**.

   Vous pouvez également envoyer la commande à l'appareil mobile en sélectionnant **Toutes les commandes** dans le menu contextuel de cet appareil mobile, puis en sélectionnant **Supprimer l'app**.

   Cette opération ouvre la fenêtre **Suppression des applications** contenant la liste des applications.

6. Dans la liste, sélectionnez l'app que vous devez supprimer de l'appareil mobile. Vous pouvez sélectionner et supprimer plusieurs apps en même temps sur l'appareil. Pour sélectionner une plage d'apps, utilisez la touche **SHIFT**. Pour regrouper plusieurs apps, utilisez la touche **CTRL**.

7. Cliquez sur **OK** pour envoyer la commande à l'appareil mobile.

   Suite à l'exécution de cette commande, l'app sélectionnée sera supprimée de l'appareil mobile de l'utilisateur. Parallèlement, l'état de la commande affichera la valeur *Terminée*.

   Un clic sur le bouton **Renvoyer** permet de renvoyer la commande à l'appareil mobile de l'utilisateur.

   Le bouton **Mettre à jour de la file d'attente** permet d'annuler l'exécution de la commande envoyée si cette dernière n'a pas encore été exécutée.

   La section **Journal des commandes** affiche les commandes envoyées à l'appareil mobile et leurs états d'exécution respectifs. Cliquez sur le bouton **Actualiser** pour mettre à jour la liste des commandes.

8. Cliquez sur le bouton **OK** pour fermer la fenêtre **Commandes d'administration des appareils mobiles**.

Configuration des paramètres d'itinérance sur un appareil mobile MDM iOS

Pour configurer les paramètres d'itinérance, procédez comme suit :

1. Dans l'arborescence de la console ouvrez le dossier **Administration des appareils mobiles**.

2. Dans le dossier **Administration des appareils mobiles**, sélectionnez le sous-dossier **Appareils mobiles**.

   La liste des appareils mobiles administrés s'affiche dans l'espace de travail du dossier.

3. Sélectionnez l'appareil MDM iOS de l'utilisateur dont vous souhaitez configurer les paramètres d'itinérance.

   Vous pouvez sélectionner plusieurs appareils mobiles pour en configurer les paramètres d'itinérance simultanément.

4. Dans le menu contextuel de l'appareil mobile, sélectionnez l'option **Afficher le journal des commandes**.

5. Dans la fenêtre **Commandes pour l'administration des appareils mobiles**, ouvrez la section **Configurer les paramètres d'itinérance** et cliquez sur le bouton **Envoyer la commande**.

   Vous pouvez également envoyer la commande à l'appareil mobile en sélectionnant l'option **Toutes les commandes → Configurer les paramètres d'itinérance** dans le menu contextuel de cet appareil.

6. Dans la fenêtre **Paramètres d'itinérance**, indiquez les paramètres pertinents :

   - Activer l'itinérance des données

     Si cette option est activée, l'itinérance vocale est activée sur l'appareil mobile MDM iOS. L'utilisateur de l'appareil MDM iOS peut utiliser Internet dans l'itinérance.

     Cette option est Inactif par défaut.

Les paramètres d'itinérance sont configurés pour les appareils sélectionnés.

Affichage des informations sur l'appareil MDM iOS

Pour consulter les informations relatives à l'appareil MDM iOS, procédez comme suit :

1. Dans le dossier **Administration des appareils mobiles** de l'arborescence de la console, sélectionnez le sous-dossier **Appareils mobiles**.

   La liste des appareils mobiles administrés s'affiche dans l'espace de travail du dossier.

2. Dans l'espace de travail, sélectionnez les appareils MDM iOS en cliquant sur le lien **MDM iOS**.

3. Sélectionnez l'appareil mobile dont vous souhaitez afficher les informations.

4. Dans le menu contextuel de l'appareil mobile, sélectionnez l'option **Propriétés**.

   Cela ouvre la fenêtre des propriétés de l'appareil MDM iOS.

La fenêtre des propriétés de l'appareil mobile affiche des informations sur l'appareil MDM iOS connecté.

Désactivation de l'administration de l'appareil MDM iOS

Pour désactiver l'appareil MDM iOS du Serveur MDM iOS, procédez comme suit :

1. Dans le dossier **Administration des appareils mobiles** de l'arborescence de la console, sélectionnez le sous-dossier **Appareils mobiles**.

   La liste des appareils mobiles administrés s'affiche dans l'espace de travail du dossier.

2. Dans l'espace de travail, sélectionnez les appareils MDM iOS en cliquant sur le lien **MDM iOS**.

3. Sélectionnez l'appareil mobile désiré.

4. Dans le menu contextuel de l'appareil mobile, sélectionnez l'option **Supprimer**.

   L'appareil MDM iOS est marqué pour suppression. L'appareil mobile sera automatiquement supprimé de la liste des appareils administrés après sa suppression de la base de données du Serveur MDM iOS. La suppression de l'appareil mobile sur la base de données du Serveur MDM iOS s'effectue en une minute.

Après la désactivation de l'appareil MDM iOS de l'administration, tous les profils de configuration installés seront supprimés de l'appareil mobile, ainsi que le profil MDM iOS et toutes les applications pour lesquelles l'option **Supprimer avec le profil MDM iOS** avait été activée.

Envoi de commandes sur un appareil

Pour envoyer une commande à un appareil MDM iOS, procédez comme suit :

1. Dans la Console d'administration, ouvrez l'entrée **Administration des appareils mobiles**.

2. Choisir le dossier **Appareils mobiles**.

3. Dans le dossier **Appareils mobiles**, sélectionnez l'appareil mobile auquel il faut envoyer les commandes.

4. Dans le menu contextuel de l'appareil mobile, sélectionnez l'option **Afficher le journal des commandes**.
5. puis choisir dans la liste déroulante la commande à envoyer à l'appareil mobile.

Contrôle de l'état d'exécution des commandes envoyées

Pour vérifier l'état d'exécution d'une commande qui a été envoyée à un appareil mobile, procédez comme suit :

1. Dans la Console d'administration, ouvrez l'entrée **Administration des appareils mobiles**.
2. Choisir le dossier **Appareils mobiles**.
3. Dans le dossier **Appareils mobiles**, sélectionnez l'appareil mobile sur lequel il faut vérifier l'état d'exécution des commandes envoyées.
4. Dans le menu contextuel de l'appareil mobile, sélectionnez l'option **Afficher le journal des commandes**.

Administration des appareils KES

Dans Kaspersky Security Center, vous pouvez administrer les appareils mobiles KES des façons suivantes :

- Administrer les appareils KES de façon centralisée à l'aide de commandes.
- Consulter les informations sur les paramètres d'administration des appareils KES.
- Installer les applications à l'aide de paquets des applications mobiles.
- Désactivation d'un appareil KES de l'administration.

Création du paquet des applications mobiles pour les appareils KES

Une licence Kaspersky Endpoint Security for Android est indispensable pour la création d'un paquet des applications mobiles destiné aux appareils KES.

Pour créer un paquet des applications mobiles, procédez comme suit :

1. Dans l'arborescence de la console, dans le dossier **Installation à distance**, sélectionnez le sous-dossier **Paquets d'installation**.

   Le dossier **Installation à distance** est un sous-dossier par défaut du dossier **Avancé**.
2. Cliquez sur le bouton **Actions supplémentaires** et, dans la liste déroulante, sélectionnez l'option **Administrer les paquets des applications mobiles**.
3. Dans la fenêtre **Administration des paquets des applications mobiles**, cliquez sur le bouton **Nouvelle**.
4. L'Assistant de création du paquet d'installation se lance. Suivez les instructions de l'assistant.

Le paquet des applications mobiles créé s'affiche dans la fenêtre **Administration des paquets des applications mobiles**.

Activation de l'authentification basée sur certificat des appareils KES

Pour activer l'authentification basée sur certificat d'un appareil KES, procédez comme suit :

1. Ouvrez le registre système de l'appareil client sur lequel le Serveur d'administration est installé, par exemple, à l'aide de la commande regedit dans le menu **Démarrer** → **Exécuter**.
2. Rendez-vous dans la section :
   - Pour les systèmes 32 bits :

     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\.core\.independent\KLLIM
   - Pour les systèmes 64 bits :

     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\.core\.independent\
3. Créez une clé appelée LP_MobileMustUseTwoWayAuthOnPort13292.
4. Définissez le type de clé REG_DWORD.
5. Indiquez la valeur 1 pour la clé.
6. Relancez le service du Serveur d'administration.

Une authentification obligatoire basée sur un certificat de l'appareil KES avec utilisation d'un certificat commun sera activée après le lancement du service du Serveur d'administration.

Lors de la première connexion d'un appareil KES au Serveur d'administration, la présence d'un certificat n'est pas obligatoire.

Par défaut, l'authentification basée sur certificat des appareils KES est désactivée.

Affichage des informations sur l'appareil KES

Pour consulter les informations relatives à un appareil KES, procédez comme suit :

1. Dans le dossier **Administration des appareils mobiles** de l'arborescence de la console, sélectionnez le sous-dossier **Appareils mobiles**.

   La liste des appareils mobiles administrés s'affiche dans l'espace de travail du dossier.
2. Dans l'espace de travail, filtrez les appareils KES selon le protocole d'administration *KES*.
3. Sélectionnez l'appareil mobile dont vous souhaitez afficher les informations.
4. Dans le menu contextuel de l'appareil mobile, sélectionnez l'option **Propriétés**.

Cette action entraîne l'ouverture de la fenêtre des propriétés de l'appareil KES.

La fenêtre des propriétés de l'appareil mobile affiche des informations sur l'appareil KES connecté.

Désactivation d'un appareil KES de l'administration

Pour désactiver un appareil KES de l'administration, l'utilisateur doit supprimer l'Agent d'administration de l'appareil mobile concerné. Suite à la suppression de l'Agent d'administration par l'utilisateur, les informations relatives à l'appareil mobile sont supprimées de la base de données du Serveur d'administration. De même, l'administrateur peut supprimer l'appareil mobile de la liste des appareils administrés.

Pour supprimer l'appareil KES de la liste des appareils administrés, procédez comme suit :

1. Dans le dossier **Administration des appareils mobiles** de l'arborescence de la console, sélectionnez le sous-dossier **Appareils mobiles**.

   La liste des appareils mobiles administrés s'affiche dans l'espace de travail du dossier.

2. Dans l'espace de travail, filtrez les appareils KES selon le protocole d'administration *KES*.

3. Sélectionnez l'appareil mobile dont il faut désactiver l'administration.

4. Dans le menu contextuel de l'appareil mobile, sélectionnez l'option **Supprimer**.

   Ainsi, l'appareil mobile sera supprimé de la liste des appareils administrés.

   Si Kaspersky Endpoint Security for Android n'est pas supprimé de l'appareil mobile, la prochaine synchronisation avec le Serveur d'administration entraînera la réapparition de cet appareil mobile dans la liste des appareils administrés.

Chiffrement et protection des données

Le chiffrement des données diminue les risques de fuite d'informations en cas de vol ou de perte d'un appareil portable, d'un disque amovible ou d'un disque dur, ou en cas d'accès aux données par des utilisateurs et des applications non autorisés.

La fonction de chiffrement est assurée par l'application Kaspersky Endpoint Security for Windows. Kaspersky Endpoint Security for Windows permet de chiffrer les fichiers enregistrés dur les disques locaux de l'appareil et sur les supports amovibles, ainsi que les disques amovibles et les disques durs entièrement.

La configuration des règles de chiffrement est exécutée à l'aide de Kaspersky Security Center via la définition de stratégies. Le chiffrement et le déchiffrement selon les règles définies sont exécutés lors de l'application de la stratégie.

L'accessibilité de la fonctionnalité d'administration de chiffrement est déterminée à l'aide des paramètres de l'interface de l'utilisateur.

L'administrateur peut exécuter les actions suivantes :

- Configurer et exécuter le chiffrement ou le déchiffrement des fichiers sur les disques locaux de l'appareil.
- Configurer et exécuter le chiffrement des fichiers sur les disques amovibles.

- Former les règles d'accès des applications aux fichiers chiffrés.
- Créer et transmettre à l'utilisateur le fichier clé d'accès aux fichiers chiffrés si l'appareil de l'utilisateur a des restrictions de la fonctionnalité de chiffrement des fichiers.
- Configurer et exécuter le chiffrement des disques durs.
- Administrer l'accès des utilisateurs aux disques durs chiffrés et aux disques amovibles (administrer les comptes de l'agent d'authentification, former et transmettre aux utilisateurs les groupes de réponse sur la demande de restauration du nom et du mot de passe du compte utilisateur et les clés d'accès aux appareils chiffrés).
- Consulter les états de chiffrement et les rapports sur le chiffrement des fichiers.

Ces opérations sont exécutées à l'aide des outils de l'application Kaspersky Endpoint Security for Windows. Les instructions détaillées sur l'exécution des opérations et la description des particularités de fonctionnalité de chiffrement sont décrites dans l'Aide en ligne de Kaspersky Endpoint Security for Windows.

Kaspersky Security Center prend en charge la fonctionnalité d'administration du chiffrement pour les appareils dotés de systèmes d'exploitation macOS. La configuration du chiffrement s'opère à l'aide des outils de l'application Kaspersky Endpoint Security for Mac pour les versions qui prennent en charge la fonction de chiffrement. Les instructions détaillées sur l'exécution des opérations et la description des particularités de fonctionnalité de chiffrement sont décrites dans le *Manuel de l'administrateur de Kaspersky Endpoint Security for Mac*.

Consultation de la liste des appareils chiffrés

Pour consulter la liste des appareils dont les informations ont été chiffrées, procédez comme suit :

1. Dans l'arborescence de la console du Serveur d'administration, sélectionnez le dossier **Chiffrement et protection des données**.
2. Passez à la liste des appareils chiffrés à l'aide d'un des moyens suivants :
   - En cliquant sur le lien **Accéder à la liste des disques chiffrés** dans la section **Administrer les disques chiffrés**.
   - En sélectionnant le dossier **Disques chiffrés** dans l'arborescence de la console.

Finalement, l'espace de travail reprend les informations sur les appareils présents dans le réseau sur lesquels il y a des fichiers chiffrés et les informations sur les appareils chiffrés au niveau des disques. Après le déchiffrement des informations sur l'appareil, celui-ci sera automatiquement supprimé de la liste.

Vous pouvez trier les informations dans la liste des appareils en ordre croissant ou décroissant à partir de n'importe quel paramètre.

La présence ou l'absence du dossier **Chiffrement et protection des données** dans l'arborescence de la console est définie par les paramètres de l'interface utilisateur.

Consultation de la liste des événements du chiffrement

Pendant l'exécution des tâches de chiffrement ou de déchiffrement des données sur les appareils, Kaspersky Endpoint Security for Windows envoie dans Kaspersky Security Center les informations sur les événements survenus des types suivants :

- Il est impossible de chiffrer ou déchiffrer le fichier ou de créer l'archive chiffrée en raison d'un espace sur le disque insuffisant.
- Il est impossible de chiffrer ou déchiffrer le fichier ou créer l'archive chiffrée à cause de problèmes avec la licence.
- Il est impossible de chiffrer ou déchiffrer le fichier ou créer une archive chiffrée en raison de l'absence de privilèges d'accès.
- L'accès au fichier chiffré est interdit à l'application.
- Les erreurs inconnues.

Pour consulter la liste des événements survenus lors du chiffrement des données sur les appareils, procédez comme suit :

1. Dans l'arborescence de la console du Serveur d'administration, sélectionnez le dossier **Chiffrement et protection des données**.
2. Passez à la liste des événements survenus lors du chiffrement à l'aide d'un des moyens suivants :
   - A l'aide du lien **Accéder à la liste des erreurs** dans le groupe d'administration **Erreurs de chiffrement des données**.
   - Dans l'arborescence de la console, sélectionnez le dossier **Disques chiffrés**.

L'espace de travail reprend enfin les informations sur les problèmes survenus lors du chiffrement des données sur les appareils clients.

Vous pouvez exécuter les actions suivantes avec la liste des événements du chiffrement :

- Trier les enregistrements dans l'ordre croissant ou décroissant des données dans n'importe quelle colonne.
- Exécuter la recherche rapide selon les enregistrements (selon la coïncidence de texte avec la sous-ligne dans n'importe quel champ de la liste).
- Exporter la liste formée des événements dans le fichier texte.

La présence ou l'absence du dossier **Chiffrement et protection des données** dans l'arborescence de la console est définie par les paramètres de l'interface utilisateur.

Exportation de la liste des événements du chiffrement dans le fichier texte

Pour exporter la liste des événements du chiffrement dans un fichier texte, procédez comme suit :

1. Formez la liste des événements du chiffrement.
2. Dans le menu contextuel de la liste des événements, sélectionnez l'option **Exporter la liste**.

   La fenêtre **Exporter la liste** s'ouvre.
3. Dans la fenêtre **Exporter la liste**, indiquez le nom du fichier texte avec la liste des événements, sélectionnez le dossier dans lequel la liste sera enregistrée et cliquez sur le bouton **Enregistrer**.

   La liste des événements du chiffrement sera enregistrée dans le fichier indiqué.

Formation et consultation des rapports sur le chiffrement

Vous pouvez créer les rapports suivants :

- Rapport de l'état de chiffrement des appareils administrés. Ce rapport fournit des détails sur le chiffrement des données de divers appareils administrés. Par exemple, le rapport indique le nombre d'appareils auxquels s'applique la stratégie avec les règles de chiffrement configurées. Vous pouvez également savoir, par exemple, combien d'appareils doivent être redémarrés. Le rapport contient également des informations sur la technologie et l'algorithme de chiffrement pour chaque appareil.
- Rapport de l'état de chiffrement des appareils de stockage. Ce rapport contient des informations similaires à celles du rapport sur l'état de chiffrement des appareils administrés, mais il ne fournit des données que pour les appareils de stockage de masse et les disques amovibles.
- Rapport sur les privilèges d'accès aux disques chiffrés. Ce rapport indique quels comptes utilisateurs ont accès aux disques chiffrés.
- Rapport sur les erreurs de chiffrement des fichiers. Ce rapport contient les erreurs survenues lors de l'exécution des tâches de chiffrement ou de déchiffrement des données sur les appareils.
- Rapport sur le blocage de l'accès aux fichiers chiffrés. Ce rapport contient les informations sur le blocage de l'accès de l'application aux fichiers chiffrés. Ce rapport est utile si un utilisateur ou une application non autorisé tente d'accéder à des fichiers ou des lecteurs chiffrés.

Pour générer le rapport sur le chiffrement des appareils :

1. Sélectionnez le dossier **Chiffrement et protection des données** dans l'arborescence de la console.
2. Exécutez une des actions suivantes :

   - Pour générer le rapport sur l'état de chiffrement des appareils administrés, cliquez sur le lien **Consulter le rapport sur l'état de chiffrement des appareils de stockage de masse**.

     Si vous n'avez pas encore configuré ce rapport, l'assistant de création du modèle du rapport démarre. Suivez les étapes de l'Assistant.
   - Pour générer le rapport sur l'état de chiffrement des appareils de stockage de masse, dans l'arborescence de la console, sélectionnez le sous-dossier **Disques chiffrés**, puis cliquez sur le bouton **Consulter le rapport sur l'état de chiffrement des appareils de stockage de masse**.

La création du rapport démarre. Le rapport apparaît sous l'onglet **Rapports** de l'entrée **Serveur d'administration**.

Pour créer un rapport sur les privilèges d'accès aux appareils chiffrés :

1. Sélectionnez le dossier **Chiffrement et protection des données** dans l'arborescence de la console.
2. Exécutez une des actions suivantes :
   - Cliquez sur le lien **Rapport sur les privilèges d'accès aux disques chiffrés** dans la section **Administrer les disques chiffrés** pour démarrer l'Assistant de création du modèle du rapport.
   - Sélectionnez le sous-dossier **Disques chiffrés**, puis cliquez sur le bouton **Rapport sur les privilèges d'accès aux disques chiffrés** pour démarrer l'Assistant de création du modèle du rapport.
3. Suivez les étapes de l'Assistant de création du modèle du rapport.

La création du rapport démarre. Le rapport apparaît sous l'onglet **Rapports** de l'entrée **Serveur d'administration**.

Pour générer le rapport sur les erreurs de chiffrement des fichiers :

1. Sélectionnez le dossier **Chiffrement et protection des données** dans l'arborescence de la console.
2. Exécutez une des actions suivantes :
   - Cliquez sur le lien **Consulter le rapport sur les erreurs de chiffrement des fichiers** dans la section **Erreurs de chiffrement des données** pour lancer l'Assistant de création du modèle du rapport.
   - Sélectionnez le sous-dossier **Événements du chiffrement**, puis à l'aide du lien **Rapport sur les erreurs de chiffrement des fichiers**, lancez l'Assistant de création du modèle du rapport.
3. Suivez les étapes de l'Assistant de création du modèle du rapport.

La création du rapport démarre. Le rapport apparaît sous l'onglet **Rapports** de l'entrée **Serveur d'administration**.

Pour créer le rapport sur l'état de chiffrement des appareils administrés :

1. Dans l'arborescence de la console, sélectionnez l'entrée portant le nom du Serveur d'administration requis.
2. Dans l'espace de travail de l'entrée, sélectionnez l'onglet **Rapports**.
3. Cliquez sur le bouton **New report template** pour lancer l'Assistant de création du modèle du rapport.
4. Suivez les indices de l'Assistant de création du modèle du rapport. dans la fenêtre **Sélection du type de modèle de rapport**, dans la section **Autres**, sélectionnez **Rapport de l'état de chiffrement des appareils administrés**.

   À la fin de l'Assistant de création du modèle du rapport, un nouveau modèle de rapport apparaît dans l'entrée Serveur d'administration, sous l'onglet **Rapports**.
5. Dans l'entrée du Serveur d'administration concerné, sous l'onglet **Rapports**, choisissez le modèle de rapport créé lors des étapes antérieures.

La création du rapport démarre. Le rapport apparaît sous l'onglet **Rapports** de l'entrée **Serveur d'administration**.

Les informations sur la conformité des états de chiffrement des appareils et des disques amovibles à la stratégie de chiffrement sont aussi consultables dans les panneaux d'informations sous l'onglet **Statistiques** du nœud Serveur d'administration.

Pour créer un rapport sur le blocage de l'accès aux fichiers chiffrés :

1. Dans l'arborescence de la console, sélectionnez l'entrée portant le nom du Serveur d'administration requis.
2. Dans l'espace de travail de l'entrée, sélectionnez l'onglet **Rapports**.
3. Cliquez sur le bouton **Nouveau modèle de rapport** pour lancer l'Assistant de création du modèle du rapport.
4. Suivez les indices de l'Assistant de création du modèle du rapport. Dans la fenêtre **Sélection du type de modèle de rapport**, dans la section **Autres**, sélectionnez **Rapport sur le blocage de l'accès aux fichiers chiffrés**.

   À la fin de l'Assistant de création du modèle du rapport, un nouveau modèle de rapport apparaît dans l'entrée **Serveur d'administration**, sous l'onglet **Rapports**.
5. Dans l'entrée **Serveur d'administration**, sous l'onglet **Rapports**, choisissez le modèle du rapport créé lors des étapes antérieures.

La création du rapport démarre. Le rapport apparaît sous l'onglet **Rapports** de l'entrée **Serveur d'administration**.

Transmission des clés de chiffrement entre les Serveurs d'administration

Si la fonctionnalité de chiffrement des données est activée sur un appareil administré, la clé de chiffrement est stockée sur le Serveur d'administration. La clé de chiffrement est utilisée pour accéder aux données chiffrées et pour administrer la stratégie de chiffrement.

La clé de chiffrement doit être transmise à un autre Serveur d'administration dans les cas suivants :

- Vous reconfigurez l'Agent d'administration sur un appareil administré pour affecter l'appareil à un autre Serveur d'administration. Si cet appareil contient des données chiffrées, la clé de chiffrement doit être transmise au Serveur d'administration cible. Sinon, les données ne peuvent pas être déchiffrées.
- Vous chiffrez un disque amovible connecté à un appareil D1 administré par le Serveur d'administration S1, puis vous connectez ce disque amovible à un appareil D2 administré par le Serveur d'administration S2. Pour accéder aux données sur le disque amovible, la clé de chiffrement doit être transmise du Serveur d'administration S1 au Serveur d'administration S2.
- Vous chiffrez un fichier sur un appareil D1 administré par le Serveur d'administration S1, puis vous essayez d'accéder au fichier sur un appareil D2 administré par le Serveur d'administration S2. Pour accéder au fichier, la clé de chiffrement doit être transmise du Serveur d'administration S1 au Serveur d'administration S2.

Vous pouvez transmettre des clés de chiffrement des manières suivantes :

- Automatiquement, en activant l'option **&Utiliser la hiérarchie des Serveurs d'administration pour obtenir des clés de chiffrement** dans les propriétés de deux Serveurs d'administration entre lesquels une clé de chiffrement doit être transmise. Si cette option est désactivée pour l'un des Serveurs d'administration, la transmission automatique des clés de chiffrement n'est pas possible.

  Lorsque vous activez l'option **&Utiliser la hiérarchie des Serveurs d'administration pour obtenir des clés de chiffrement** dans un Serveurs d'administration, le Serveur d'administration envoie toutes les clés de chiffrement stockées dans son stockage au Serveur d'administration principal (le cas échéant) d'un niveau supérieur dans la hiérarchie.

  Lorsque vous essayez d'accéder à des données chiffrées, le Serveur d'administration recherche d'abord la clé de chiffrement dans son propre stockage. Si l'option **&Utiliser la hiérarchie des Serveurs d'administration pour obtenir des clés de chiffrement** est activée et que la clé de chiffrement requise n'a pas été trouvée dans le stockage, le Serveur d'administration envoie également une demande aux Serveurs d'administration principaux (le cas échéant) de lui fournir la clé de chiffrement requise. La demande sera envoyée à tous les Serveurs d'administration principaux jusqu'au serveur situé au niveau le plus élevé de la hiérarchie.

L'option **&Utiliser la hiérarchie des Serveurs d'administration pour obtenir des clés de chiffrement** n'est actuellement pas disponible dans l'interface de Web Console. Si vous n'avez pas accès à la Console d'administration basée sur MMC, utilisez le Serveur d'administration principal pour administrer les appareils chiffrés.

- Manuellement d'un Serveur d'administration à un autre en exportant et en important le fichier contenant les clés de chiffrement.

  L'exportation et l'importation des clés de chiffrement sont des actions incluses dans la fonctionnalité Gestion des clés de chiffrement. Pour exécuter ces actions, configurez les privilèges d'accès à la fonctionnalité pour les utilisateurs de Kaspersky Security Center comme suit :

  - Accordez le privilège d'accès **Lire** à la fonction de gestion des clés de chiffrement à l'utilisateur qui exporte les clés de chiffrement depuis le Serveur d'administration secondaire.
  - Accordez le privilège d'accès **Écrire** à la fonction de gestion des clés de chiffrement à l'utilisateur qui importe les clés de chiffrement sur le Serveur d'administration cible.

Pour activer la transmission automatique des clés de chiffrement entre les Serveurs d'administration au sein de la hiérarchie, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le Serveur d'administration pour lequel vous souhaitez activer la transmission automatique des clés de chiffrement.
2. Dans le menu contextuel Serveur d'administration, sélectionnez l'option **Propriétés**.
3. Dans la fenêtre des propriétés, sélectionnez la section **Algorithme de chiffrement**.
4. Activez l'option **&Utiliser la hiérarchie des Serveurs d'administration pour obtenir des clés de chiffrement**.
5. Cliquez sur le bouton **OK** pour appliquer les modifications.

Les clés de chiffrement seront transmises aux Serveurs d'administration principaux (le cas échéant) lors de la prochaine synchronisation (le battement de cœur). Ce Serveur d'administration fournira également, sur demande, une clé de chiffrement de son stockage à un Serveur d'administration secondaire.

Pour transmettre manuellement les clés de chiffrement entre les Serveur d'administration :

1. Dans l'arborescence de la console du Serveur d'administration, sélectionnez le Serveur d'administration secondaire à partir duquel vous souhaitez transmettre les clés de chiffrement.
2. Dans le menu contextuel Serveur d'administration, sélectionnez l'option **Propriétés**.
3. Dans la fenêtre des propriétés, sélectionnez la section **Algorithme de chiffrement**.
4. Cliquez sur **&Exporter des clés de chiffrement à partir du Serveur d'administration**.

   Assurez-vous que l'utilisateur qui exporte les clés de chiffrement depuis le Serveur dispose du privilège d'accès **Lire** pour la fonction de gestion des clés de chiffrement.
5. Dans la fenêtre **Exporter des clés de chiffrement** :
   - Cliquez sur le bouton **Parcourir**, puis spécifiez où vous souhaitez enregistrer le fichier.
   - Spécifiez un mot de passe pour protéger le fichier contre tout accès non autorisé.

     N'oubliez pas le mot de passe. Un mot de passe oublié ne peut pas être récupéré. Si le mot de passe est perdu, vous devez répéter la procédure d'exportation. Par conséquent, prenez note du mot de passe et conservez-le à portée de main.
6. Transmettez le fichier à un autre Serveur d'administration, par exemple, via un dossier partagé ou un lecteur amovible.
7. Sur le Serveur d'administration cible, assurez-vous que la Console d'administration de Kaspersky Security Center est en cours d'exécution.
8. Dans l'arborescence de la console du Serveur d'administration, sélectionnez le Serveur d'administration cible sur lequel vous souhaitez transmettre les clés de chiffrement.
9. Dans le menu contextuel Serveur d'administration, sélectionnez l'option **Propriétés**.
10. Dans la fenêtre des propriétés, sélectionnez la section **Algorithme de chiffrement**.
11. Cliquez sur **&Importer des clés de chiffrement sur le Serveur d'administration**.

    Assurez-vous que l'utilisateur qui importe les clés de chiffrement depuis le Serveur dispose du privilège d'accès **Écrire** pour la fonction de gestion des clés de chiffrement.
12. Dans la fenêtre **Importer des clés de chiffrement** :
    - Cliquez sur le bouton **Parcourir**, puis sélectionnez le fichier contenant les clés de chiffrement.
    - Indiquez le mot de passe.
13. Cliquez sur le bouton **OK**.

Les clés de chiffrement sont transmises au Serveur d'administration cible.

Stockages des données

Cette section contient les informations sur les données enregistrées sur le Serveur d'administration et utilisées pour suivre les états des appareils clients et pour leur service.

Les données du dossier **Stockages** de l'arborescence de la console affichent les données utilisées pour assurer le suivi des appareils client.

Le dossier **Stockages** contient les objets suivants :

- Les mises à jour reçues par le Serveur d'administration et diffusées vers les appareils clients
- La liste de l'inventaire détecté dans le réseau
- Les clés de licence détectées sur les appareils clients
- Fichiers placés par les applications de sécurité dans les dossiers de quarantaine sur les appareils
- Fichiers placés dans la Sauvegarde des appareils clients
- Fichiers pour lesquels les applications de sécurité ont décidé d'une analyse ultérieure

Exportation de la liste des objets dans le stockage dans le fichier texte

Vous pouvez exporter de la liste des objets dans le stockage dans le fichier texte.

Pour exporter de la liste des objets du stockage dans le fichier texte, procédez comme suit :

1. Dans l'arborescence de la console **Stockages**, sélectionnez le sous-dossier du stockage concerné.
2. Dans le sous-dossier du stockage, sélectionnez **Exporter la liste** dans le menu contextuel.

   Finalement, la fenêtre **Exporter la liste** s'ouvre. Cette fenêtre permet d'indiquer le nom du fichier texte et l'adresse du dossier dans lequel il sera placé.

Paquets d'installation

Kaspersky Security Center place dans les stockages de données les paquets d'installation des applications de Kaspersky et des applications des éditeurs tiers.

Le *Paquet d'installation* représente l'ensemble de fichiers nécessaires pour installer l'application. Le paquet d'installation contient les paramètres du processus d'installation et de la configuration initiale de l'application installée.

Si vous voulez installer n'importe quelle application sur l'appareil client, il faut créer un paquet d'installation pour cette application ou utiliser le paquet d'installation déjà créé. La liste des paquets d'installation créés se trouve dans le dossier **Installation à distance** de l'arborescence de la console, dans le sous-dossier **Paquets d'installation**.

Principaux états des fichiers dans le stockage

Les applications de sécurité analysent la présence de virus connus et d'autres applications présentant une menace les fichiers sur les appareils, attribuent des états aux fichiers et placent certains fichiers dans le stockage.

Par exemple, les applications de sécurité peuvent :

- Enregistrer dans le stockage une copie du fichier avant sa suppression
- Isoler dans le stockage les fichiers probablement infectés

Les principaux états des fichiers figurent dans le tableau ci-après. Vous pouvez recevoir des informations plus détaillées sur les actions applicables aux fichiers dans les aides des applications de sécurité.

États des fichiers dans le stockage

Nom de l'état	Description de l'état
Infecté	Le fichier contient une partie de code d'un virus connu ou d'une autre application présentant une menace dont les informations se trouvent dans les bases antivirus de Kaspersky.
Non infecté	Aucun virus connus ou autres applications présentant une menace n'a été détecté dans le fichier.
Avertissement	Le fichier contient une partie de code correspondant partiellement à la partie de code de contrôle d'une menace connue.
Probablement infecté	Le fichier contient soit le code modifié d'un virus connu ou un code rappelant un virus inconnu de Kaspersky.
Placé dans le dossier par l'utilisateur	L'utilisateur a placé lui-même le fichier dans le stockage parce que, par exemple, le comportement du fichier laisse penser qu'il présente des menaces. L'utilisateur peut analyser le fichier pour voir s'il contient des menaces à l'aide des bases mises à jour.
Faux positif	L'application Kaspersky a attribué l'état infecté au fichier désinfecté étant donné que son code rappelle le code d'un virus. Après analyse à l'aide des bases mises à jour, le fichier est défini comme non infecté.
Désinfecté	Le fichier a pu être désinfecté.
Supprimé	Le fichier est supprimé suite à la désinfection.
Protégé par un mot de passe	Le fichier ne peut pas être traité car il est protégé par un mot de passe.

Déclenchement des règles en mode Apprentissage intelligent

Cette section fournit des informations relatives aux détections réalisées par les règles du contrôle évolutif des anomalies dans Kaspersky Endpoint Security for Windows sur les appareils clients.

Les règles détectent le comportement anormal sur les appareils clients et peuvent le bloquer. Si les règles fonctionnent en mode Apprentissage intelligent, elles détectent tout comportement anormal et envoient des rapports sur chaque cas au Serveur d'administration de Kaspersky Security Center. Ces informations sont stockées sous forme de liste dans le sous-dossier **Déclenchements de règles dans l'état Apprentissage intelligent** du dossier **Stockages**. Vous pouvez confirmer les détections comme étant correctes ou les ajouter en tant qu'exclusions afin que ce type de comportement ne soit plus considéré comme une anomalie.

Les informations relatives aux détections sont stockées dans le journal des événements sur le Serveur d'administration (avec les autres événements) et dans le rapport Contrôle évolutif des anomalies.

Pour en savoir plus sur le Contrôle évolutif des anomalies, les règles, leur mode et les états, consultez l'aide de Kaspersky Endpoint Security for Windows.

Consultation de la liste des détections réalisées à l'aide des règles du contrôle évolutif des anomalies

Pour consulter la liste des détections réalisées à l'aide des règles du contrôle évolutif des anomalies, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez l'entrée correspondant au Serveur d'administration de laquelle il faut se déconnecter.

2. Sélectionnez le sous-dossier **Déclenchements de règles dans l'état Apprentissage intelligent** (par défaut, il s'agit d'un sous-dossier de **Avancé** → **Stockages**).

   La liste affiche les informations suivantes relatives aux détections réalisées à l'aide des règles du contrôle évolutif des anomalies :

   - **Groupe d'administration**

     Le nom du groupe d'administration dont l'appareil fait partie.

   - **Nom de l'appareil**

     Le nom de l'appareil client sur lequel la règle a été appliquée.

   - **Nom**

     Le nom de la règle qui a été appliquée.

   - **État**

     Exclusion en cours : si l'Administrateur a traité cet élément et l'a ajouté en tant qu'exclusion aux règles. Cet état se maintient jusqu'à la synchronisation suivante de l'appareil client avec le Serveur d'administration après la synchronisation, l'appareil disparaît de la liste.

     Confirmation en cours : si l'administrateur a traité cet élément et l'a confirmé. Cet état se maintient jusqu'à la synchronisation suivante de l'appareil client avec le Serveur d'administration après la synchronisation, l'appareil disparaît de la liste.

     Vide : si l'administrateur n'a pas traité cet élément.

   - **Nombre de fois où les règles ont été déclenchées**

     Le nombre de détections au sein d'une règle heuristique, un processus et un appareil client. Cette quantité est calculée par Kaspersky Endpoint Security.

   - **Nom d'utilisateur**

     Le nom de l'utilisateur de l'appareil client qui exécute le processus qui a généré la détection.

   - **Chemin du processus source**

Chemin d'accès au processus source, à savoir au processus qui réalise l'action (pour en savoir plus, consultez l'aide de Kaspersky Endpoint Security).

- **Hash du processus source**

  Hash SHA256 du fichier du processus source (pour en savoir plus, consultez l'aide de Kaspersky Endpoint Security).

- **Chemin d'accès à l'objet source**

  Chemin d'accès à l'objet qui a lancé le processus (pour en savoir plus, consultez l'aide de Kaspersky Endpoint Security).

- **Hash de l'objet source**

  Hash SHA256 du fichier de base (pour en savoir plus, consultez l'aide de Kaspersky Endpoint Security).

- **Chemin du processus cible**

  Chemin d'accès au processus cible (pour en savoir plus, consultez l'aide de Kaspersky Endpoint Security).

- **Hash du processus cible**

  Hash SHA256 du fichier cible (pour en savoir plus, consultez l'aide de Kaspersky Endpoint Security).

- **Chemin d'accès à l'objet cible**

  Chemin d'accès à l'objet cible (pour en savoir plus, consultez l'aide de Kaspersky Endpoint Security).

- **Hash de l'objet cible**

  Hash SHA256 du fichier cible (pour en savoir plus, consultez l'aide de Kaspersky Endpoint Security).

- **Traité**

  Date de détection de l'anomalie.

Pour voir les propriétés de chaque élément d'information, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez l'entrée correspondant au Serveur d'administration de laquelle il faut se déconnecter.
2. Sélectionnez le sous-dossier **Déclenchements de règles dans l'état Apprentissage intelligent** (par défaut, il s'agit d'un sous-dossier de **Avancé** → **Stockages**).

3. Dans l'espace de travail **Déclenchements de règles dans l'état Apprentissage intelligent**, sélectionnez l'objet souhaité.

4. Exécutez une des actions suivantes :

   - Cliquez sur le lien **Propriétés** dans la zone d'informations qui apparaît à droite de la fenêtre.
   - Cliquez-droit, puis sélectionnez **Propriétés** dans le menu contextuel.

   La fenêtre des propriétés de l'objet s'ouvre et présente les informations relatives à l'élément sélectionné :

Vous pouvez confirmer ou ajouter aux exclusions n'importe quel élément de la liste des détections des règles du contrôle évolutif des anomalies.

Pour confirmer un élément,

Sélectionnez un (ou plusieurs éléments) dans la liste des détections, puis cliquez sur le bouton **Confirmer**.

L'état du ou des éléments devient **Confirmation en cours**.

Votre confirmation contribue aux statistiques utilisées par les règles (pour en savoir plus, consultez l'aide de Kaspersky Endpoint Security 11 for Windows).

Pour ajouter un élément en tant qu'exclusion,

Cliquez-droit sur un ou plusieurs éléments de la liste des détections, puis sélectionnez l'option **Ajouter aux exclusions** dans le menu contextuel.

L'Assistant d'ajout d'une exclusion démarre. Suivez les instructions de l'Assistant.

Si vous rejetez ou confirmez un élément, celui-ci est exclu de la liste des Détections après la prochaine synchronisation de l'appareil client avec le Serveur d'administration et il n'apparaît plus dans la liste.

Ajout d'exclusions au départ des règles du contrôle évolutif des anomalies

L'Assistant d'ajout d'une exclusion permet d'ajouter des exclusions au départ des règles du contrôle évolutif des anomalies pour Kaspersky Endpoint Security.

Vous pouvez lancer l'Assistant via une des trois procédures ci-dessous.

Pour lancer l'Assistant d'ajout d'une exclusion via l'entrée Contrôle évolutif des anomalies :

1. Dans l'arborescence de la console, sélectionnez l'entrée du Serveur d'administration requis.

2. Sélectionnez **Déclenchements de règles dans l'état Apprentissage intelligent** (par défaut, il s'agit d'un sous-dossier de **Avancé** → **Stockages**).

3. Dans l'espace de travail, cliquez-droit sur une ou plusieurs options de la liste des détections, puis sélectionnez l'option **Ajouter aux exclusions**.

   Vous pouvez ajouter un maximum de 1 000 exclusions en une fois. Si vous sélectionnez plus d'éléments et que vous tentez de les ajouter aux exclusions, un message d'erreur s'affiche.

L'Assistant d'ajout d'une exclusion démarre.

Vous pouvez lancer l'Assistant d'ajout d'une exclusion depuis d'autres entrées de l'arborescence de la console :

- L'onglet **Événements** de la fenêtre principale du Serveur d'administration (option **Requêtes des utilisateurs** ou option **Derniers événements**).

- **Rapport sur l'état des règles du Contrôle évolutif des anomalies**, colonne **Quantité de détections**.

Étape 1. Sélection d'une application

> Vous pouvez ignorer cette étape si vous n'avez qu'une instance de Kaspersky Endpoint Security for Windows et aucune autre application qui prend en charge les règles du Contrôle évolutif des anomalies.

L'Assistant d'ajout d'une exclusion affiche la liste des applications de Kaspersky dont les plug-ins d'administration permettent d'ajouter des exclusions aux stratégies pour ces applications. Sélectionnez une application dans cette liste, puis cliquez sur **Suivant** pour passer à la sélection de la stratégie à laquelle l'exclusion va être ajoutée.

Étape 2. Sélection de la ou des stratégies

L'Assistant affiche la liste des stratégies (avec les profils de stratégie) pour Kaspersky Endpoint Security.

Sélectionnez toutes les stratégies et les profils que vous souhaitez ajouter aux exclusions, puis cliquez sur **Suivant**.

Étape 3. Traitement de la ou des stratégies

L'Assistant affiche une barre d'état pour le traitement des stratégies. Pour interrompre le traitement des stratégies, cliquez sur **Annuler**.

Il est impossible de mettre à jour les stratégies héritées. Si vous ne possédez pas les privilèges de modification d'une stratégie, celle-ci ne sera pas mise à jour.

Une fois que toutes les stratégies ont été traitées (ou si vous interrompez le traitement), un rapport apparaît. Il montre les stratégies qui ont été traitées (icône verte) et celles qui n'ont pas été mises à jour (icône rouge).

Ceci est la dernière étape de l'Assistant. Cliquez sur **Terminer** pour quitter l'Assistant.

Quarantaine et sauvegarde

Les applications antivirus de Kaspersky installées sur les appareils clients peuvent placer les fichiers en quarantaine ou dans le dossier de sauvegarde lors de l'analyse des appareils.

La *Quarantaine* est un stockage spécial qui contient les fichiers probablement infectés par les virus ou irréparables lors de la découverte.

La *Sauvegarde* est conçue pour enregistrer les copies de sauvegarde des fichiers qui ont été supprimés ou modifiés lors de la désinfection.

Kaspersky Security Center forme une liste générale des fichiers placés en quarantaine ou dans le dossier de sauvegarde par les applications de Kaspersky sur les appareils clients. Les Agents d'administration des appareils clients transmettent les informations sur les fichiers en quarantaine et dans les dossiers de sauvegarde sur le Serveur d'administration. Via la Console d'administration vous pouvez consulter les propriétés des fichiers qui se trouvent dans les stockages sur les appareils, lancer l'analyse des logiciels malveillants de ces stockages et en supprimer les fichiers. Les icônes des états des fichiers sont décrites dans l'application.

Les opérations de quarantaine et de sauvegarde sont prises en charge pour Kaspersky Endpoint Security.

Kaspersky Security Center ne copie pas les fichiers depuis les stockages sur le Serveur d'administration. Tous les fichiers sont placés dans les stockages des appareils. La restauration des fichiers s'exécute sur l'appareil où est installée l'application antivirus ayant placé le fichier dans le stockage.

Activation de l'administration à distance des fichiers dans les stockages

L'administration à distance des fichiers dans les stockages sur les appareils clients est désactivée par défaut.

Pour activer l'administration à distance des fichiers dans les stockages sur les appareils clients, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le groupe d'administration pour lequel il faut activer la gestion à distance des fichiers dans les stockages.
2. Dans l'espace de travail du groupe, ouvrez l'onglet **Stratégies**.
3. Sous l'onglet **Stratégies**, sélectionnez la stratégie de l'application de sécurité qui place les fichiers dans les stockages sur les appareils clients.
4. Dans la fenêtre des paramètres de la stratégie dans le groupe **Transfert de données vers le Serveur d'administration**, cochez les cases qui correspondent aux stockages pour lesquels vous voulez activer l'administration à distance.

   L'emplacement du groupe de paramètres **Transfert de données vers le Serveur d'administration** dans la fenêtre des propriétés de la stratégie et les noms des cases dépendent de l'application de sécurité utilisée.

Consultation des propriétés du fichier placé dans le stockage

Pour consulter les propriétés du fichier placé en quarantaine ou dans le dossier de sauvegarde, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le dossier **Stockages**, **Quarantaine** ou le sous-dossier **Sauvegarde**.
2. Dans l'espace de travail du dossier **Quarantaine** (**Sauvegarde**), sélectionnez un fichier dont vous voulez afficher les propriétés.
3. Dans le menu contextuel du fichier, sélectionnez l'option **Propriétés**.

Suppression des fichiers depuis les stockages

Pour supprimer le fichier placé en quarantaine ou dans le dossier de sauvegarde, procédez comme suit :

1. Dans l'arborescence de la console, dans le dossier **Stockages**, sélectionnez le sous-dossier **Quarantaine** ou **Sauvegarde**.
2. Dans l'espace de travail du dossier **Quarantaine** (ou **Sauvegarde**), sélectionnez les fichiers que vous souhaitez supprimer à l'aide des touches **Shift** et **Ctrl**.
3. Supprimez les fichiers à l'aide d'un des moyens suivants :
   - Sélectionnez l'option **Supprimer** dans le menu contextuel des fichiers.
   - En cliquant sur lien **Supprimer** (**Supprimer**) si vous souhaitez supprimer un fichier) dans la zone d'informations correspondant aux fichiers sélectionnés.

Ainsi, les applications de sécurité qui ont placé les fichiers sélectionnés dans les stockages sur les appareils clients suppriment les fichiers de ces stockages.

Restauration des fichiers depuis les stockages

Pour restaurer le fichier depuis la quarantaine ou le dossier de sauvegarde, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le dossier **Stockages**, **Quarantaine** ou le sous-dossier **Sauvegarde**.
2. Dans l'espace de travail du dossier **Quarantaine** (**Sauvegarde**), sélectionnez les fichiers à restaurer à l'aide des touches **Shift** et **Ctrl**.
3. Lancez le processus de restauration des fichiers à l'aide d'un des moyens suivants :
   - Sélectionnez l'option **Restaurer** dans le menu contextuel des fichiers.
   - À l'aide du lien **Restaurer** dans la zone d'informations correspondant aux fichiers sélectionnés.

Ainsi, les applications de sécurité, qui ont placé les fichiers dans les stockages sur les appareils clients, restaurent les fichiers dans les dossiers d'origine.

Enregistrement du fichier depuis les stockages sur le disque

Kaspersky Security Center permet d'enregistrer sur le disque les copies des fichiers placés par l'application de sécurité en quarantaine ou dans le dossier de sauvegarde sur l'appareil client. Les fichiers sont copiés dans le dossier indiqué sur l'appareil avec Kaspersky Security Center installé.

Pour enregistrer une copie du fichier de la quarantaine ou du dossier de sauvegarde sur le disque dur, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le dossier **Stockages**, **Quarantaine** ou le sous-dossier **Sauvegarde**.
2. Dans l'espace de travail du dossier **Quarantaine** (**Sauvegarde**), sélectionnez un fichier à copier sur le disque dur.
3. Lancez le processus de copie du fichier à l'aide d'un des modes suivants :
   - Dans le menu contextuel du fichier, sélectionnez l'option **Enregistrer sur le disque**.
   - À l'aide du lien **Enregistrer sur le disque** dans la zone d'informations correspondant aux fichiers sélectionnés.

L'application de sécurité qui avait placé ce fichier en quarantaine sur l'appareil client sauvegardera la copie du fichier dans le dossier indiqué.

Analyse des fichiers en quarantaine

Pour analyser les fichiers en quarantaine, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le dossier **Stockages**, sous-dossier **Quarantaine**.
2. Dans l'espace de travail du dossier **Quarantaine**, sélectionnez les fichiers à analyser à l'aide des touches **SHIFT** et **CTRL**.
3. Lancez le processus d'analyse des fichiers à l'aide d'un des modes suivants :
   - Dans le menu contextuel du fichier, sélectionnez l'option **Analyse**.
   - À l'aide du lien **Analyser** dans la zone d'informations correspondant aux fichiers sélectionnés.

Ainsi, pour les applications de sécurité qui ont placé les fichiers en quarantaine, la tâche d'analyse à la demande sera lancée sur les appareils clients sur lesquels les fichiers sélectionnés se trouvent en quarantaine.

Menaces actives

Les informations sur les fichiers non traités détectés sur les appareils clients se trouvent dans le dossier **Stockages**, dans le sous-dossier **Menaces actives**.

Le traitement différé et la désinfection des fichiers de l'application de sécurité sont effectués à la demande ou après la survenue d'un événement déterminé. Vous pouvez configurer les paramètres de désinfection différée des fichiers.

Désinfection d'un fichier non traité

Pour lancer la désinfection d'un fichier non traité, procédez comme suit :

1. Dans l'arborescence de la console, dans le dossier **Stockages**, sélectionnez le sous-dossier **Menaces actives**.
2. Dans l'espace de travail du dossier **Menaces actives**, sélectionnez le fichier à désinfecter.
3. Lancez le processus de désinfection du fichier à l'aide d'un des modes suivants :
   - Dans le menu contextuel du fichier, sélectionnez l'option **Réparer**.
   - À l'aide du lien **Réparer** dans la zone d'informations correspondant aux fichiers sélectionnés.

   Cela entraîne la tentative de désinfection du fichier.

Si le fichier est réparé, l'application de sécurité installée sur l'appareil client le restaure dans le dossier d'origine. L'enregistrement sur le fichier est supprimé de la liste du dossier **Menaces actives**. Si la désinfection du fichier est impossible, l'application de sécurité installée sur l'appareil supprime le fichier de l'appareil. L'enregistrement sur le fichier est supprimé de la liste du dossier **Menaces actives**.

La capacité de désinfection et de suppression des fichiers peut varier en fonction de l'application de sécurité installée, de la version et des paramètres de l'application.

Enregistrement d'un fichier non traité sur le disque

Kaspersky Security Center permet d'enregistrer les copies des fichiers non traités sur les appareils clients sur le disque. Les fichiers sont copiés dans le dossier indiqué sur l'appareil avec Kaspersky Security Center installé.

Vous pouvez enregistrer des copies de fichiers dans les cas suivants :

- Les fichiers ont été supprimés ou modifiés lors de la désinfection, et leurs copies sont stockées dans le stockage de Kaspersky Endpoint Security for Windows sur l'appareil administré.
- L'option **Consigner uniquement** est sélectionnée pour le paramètre **Action en cas de détection d'une menace** (**Protection essentielle contre les menaces → Protection contre les fichiers malicieux**) dans la stratégie de Kaspersky Endpoint Security.

Pour enregistrer une copie d'un fichier non traité sur le disque, procédez comme suit :

1. Dans l'arborescence de la console, dans le dossier **Stockages**, sélectionnez le sous-dossier **Menaces actives**.
2. Dans l'espace de travail du dossier **Menaces actives**, sélectionnez les fichiers à copier sur le disque.
3. Lancez le processus de copie du fichier à l'aide d'un des modes suivants :
   - Dans le menu contextuel du fichier, sélectionnez l'option **Enregistrer sur le disque**.
   - À l'aide du lien **Enregistrer sur le disque** dans la zone d'informations correspondant aux fichiers sélectionnés.

Ainsi, l'application de sécurité de l'appareil client sur lequel le fichier non traité a été détecté, enregistre une copie du fichier dans le dossier indiqué.

Suppression des fichiers du dossier « Menaces actives »

*Pour supprimer un fichier du dossier **Menaces actives** :*

1. Dans l'arborescence de la console, dans le dossier **Stockages**, sélectionnez le sous-dossier **Menaces actives**.
2. Dans l'espace de travail du dossier **Menaces actives**, sélectionnez les fichiers à supprimer à l'aide des touches **SHIFT** et **CTRL**.
3. Supprimez les fichiers à l'aide d'un des moyens suivants :
   - Sélectionnez l'option **Supprimer** dans le menu contextuel des fichiers.
   - Cliquez sur le lien **Supprimer** (**Supprimer** si vous souhaitez supprimer un fichier) dans la zone d'informations correspondant aux fichiers sélectionnés.

Ainsi, les applications de sécurité qui ont placé les fichiers sélectionnés dans les stockages sur les appareils clients suppriment les fichiers de ces stockages. Les enregistrements des fichiers sont supprimés de la liste dans le dossier **Menaces actives**.

Kaspersky Security Network (KSN)

Cette section explique l'utilisation de l'infrastructure de services en ligne Kaspersky Security Network (KSN). Elle comporte des informations relatives à KSN, ainsi que des instructions pour l'activation de KSN, la configuration de l'accès à KSN et la consultation des statistiques d'utilisation du serveur proxy KSN.

La fonctionnalité de mises à jour (y compris la fourniture de mises à jour des signatures antivirus et des bases de code), ainsi que la fonctionnalité KSN peuvent ne pas être disponibles dans le logiciel aux États-Unis.

À propos de KSN

Kaspersky Security Network (KSN) est une infrastructure de services en ligne qui donne accès à la base opérationnelle des connaissances de Kaspersky concernant la réputation des fichiers, des ressources Internet et des logiciels. L'utilisation des données de Kaspersky Security Network assure une vitesse de réaction plus élevée des applications de Kaspersky sur les menaces, augmente l'efficacité de fonctionnement de certains modules de protection, ainsi que diminue la possibilité des faux positifs. KSN vous permet de recevoir des informations sur les applications installées sur les appareils administrés. Ces informations se trouvent dans les bases de réputation de Kaspersky.

Kaspersky Security Center est compatible avec les solutions d'infrastructure suivantes :

- *KSN* est une solution qui permet d'échanger des informations avec Kaspersky Security Network. Si vous participez à KSN, vous acceptez de transmettre automatiquement à Kaspersky les informations relatives au fonctionnement des applications de Kaspersky installées sur les appareils clients administrés par le Kaspersky Security Center. Le transfert des informations s'exécute conformément aux paramètres d'accès à KSN configurés. Les analystes de Kaspersky analysent également les informations reçues et les incluent dans les bases de données statistiques et de réputation de Kaspersky Security Network. Kaspersky Security Center utilise cette solution par défaut.

- *Kaspersky Private Security Network (KPSN)* est une solution qui permet aux utilisateurs d'appareils dotés d'applications Kaspersky d'accéder aux bases de données de réputation de Kaspersky Security Network et à d'autres données statistiques sans envoyer de données de leurs propres appareils à KSN global. KPSN est conçu pour les entreprises qui ne peuvent pas participer à Kaspersky Security Network pour l'une des raisons suivantes :

  - Les appareils de l'utilisateur ne sont pas connectés à Internet.

  - La transmission de données à l'extérieur du pays ou à l'extérieur du réseau local de l'entreprise est interdite par la loi ou restreinte par les stratégies de sécurité de l'entreprise.

  Vous pouvez configurer les paramètres d'accès de Kaspersky Private Security NetworK dans la section **Paramètres du proxy KSN** de la fenêtre des propriétés du Serveur d'administration.

L'application vous invite à vous connecter à KSN lors de l'exécution de l'Assistant de configuration initiale de l'application. Vous pouvez commencer à utiliser KSN ou refuser le service KSN à tout moment du fonctionnement de l'application.

Vous utilisez KSN conformément à la Déclaration KSN que vous lisez et acceptez en activant KSN. Si la Déclaration KSN est mise à jour, elle s'affiche lorsque vous mettez à niveau une version du Serveur d'administration. Vous pouvez accepter la Déclaration KSN mise à jour ou la refuser. Si vous le refusez, vous continuez à utiliser KSN conformément à la version précédente de la Déclaration KSN que vous avez acceptée auparavant.

Lorsque KSN est activé, Kaspersky Security Center vérifie si les serveurs KSN sont accessibles. Si l'accès aux serveurs via le DNS système n'est pas possible, l'application utilise les serveurs DNS publics. Cela est nécessaire pour garantir le maintien du niveau de sécurité des appareils administrés.

Les appareils clients administrés par le Serveur d'administration interagissent avec KSN à l'aide du serveur proxy KSN. Le serveur proxy KSN fournit les possibilités suivantes :

- Les appareils clients peuvent exécuter les demandes à KSN, obtenir des informations de KSN et transmettre dans KSN les informations même s'ils n'ont pas d'accès Internet direct.

- Le serveur proxy KSN met en cache les données traitées en diminuant la charge sur le canal du réseau externe et en accélérant l'obtention des informations demandées par l'appareil client.

Vous pouvez configurer le serveur proxy KSN dans la section **Paramètres du proxy KSN** de la fenêtre des propriétés du Serveur d'administration.

Configuration de l'accès à Kaspersky Security Network

Vous pouvez configurer l'accès à Kaspersky Security Network (KSN) sur le Serveur d'administration et sur un point de distribution.

Pour configurer l'accès du Serveur d'administration à Kaspersky Security Network (KSN) :

1. Dans l'arborescence de la console, sélectionnez le Serveur d'administration pour lequel vous devez configurer l'accès à KSN.

2. Dans le menu contextuel Serveur d'administration, sélectionnez l'option **Propriétés**.

3. Dans la fenêtre des propriétés du Serveur d'administration, sélectionnez **Proxy KSN → Paramètres du proxy KSN** dans le volet **Sections**.

4. Dans l'espace de travail, activez l'option **Utiliser le Serveur d'administration comme serveur proxy** pour utiliser le service KSN proxy.

   La transmission des informations depuis les appareils clients vers KSN est régie par la stratégie Kaspersky Endpoint Security active sur ces appareils. Si la case est décochée, la transmission des données depuis le Serveur d'administration ou les appareils clients vers KSN via le Kaspersky Security Center ne s'exécute pas. Toutefois, selon leur configuration, les appareils clients peuvent transmettre directement les données à KSN (et non via le Kaspersky Security Center). La stratégie de Kaspersky Endpoint Security for Windows appliquée sur les appareils clients définit quelles données de ces appareils sont envoyées directement à KSN (et non via le Kaspersky Security Center).

5. Activez l'option **&J'accepte les termes du Kaspersky Security Network**.

   Si cette option est activée, les appareils clients transmettent les résultats de l'installation des correctifs à Kaspersky. Une fois que vous avez activé cette option, vous devez lire et accepter la Déclaration KSN.

   Si vous utilisez Kaspersky Private Security Network, activez l'option **Configurer KPSN** et cliquez sur le bouton **Choix du fichier de paramètres de proxy KSN** pour télécharger les paramètres de KPSN (fichiers avec les extensions .pkcs7 et .pem). Suite au téléchargement des paramètres, l'interface affiche le nom du fournisseur, ses coordonnées et la date de création du fichier avec les paramètres de KPSN.

   > Lorsque vous activez KPSN, faites attention aux points de distribution configurés pour envoyer les requêtes KSN directement au Cloud KSN. Les points de distribution sur lesquels l'Agent d'administration version 11 (ou antérieure) est installé continueront d'envoyer des requêtes KSN au Cloud KSN. Pour reconfigurer les points de distribution pour envoyer des requêtes KSN à KPSN, activez l'option **&Transférer les demandes KSN au Serveur d'administration** pour chaque point de distribution. Vous pouvez activer cette option dans les propriétés du point de distribution ou dans la stratégie d'Agent d'administration.

   Lorsque vous cochez la case **Configurer KPSN**, un message vous indique les détails relatifs à KPSN.

   Si vous activez l'option **Configurer KPSN** dans Kaspersky Security Center, ces applications reçoivent des informations au sujet de KPSN. Dans la fenêtre de paramètres de l'application, dans la sous-section **Kaspersky Security Network** de la section **Protection avancée**, les informations sur le fournisseur KSN sélectionné s'affichent : KSN ou KPSN.

   > Si vous utilisez KPSN via des versions de l'application antérieures à Kaspersky Security for Virtualization 3.0 Agentless Service Pack 2 ou à Kaspersky Security for Virtualization 3.0 Service Pack 1 Light Agent, il est recommandé d'utiliser les Serveurs d'administration secondaires pour lesquels l'utilisation de KPSN n'a pas été configurée.

   > Kaspersky Security Center n'envoie pas de données statistiques à Kaspersky Security Network si KPSN est configuré dans la section **Proxy KSN** → **Paramètres du proxy KSN** de la fenêtre des propriétés du Serveur d'administration.

   Si vous avez configuré les paramètres du serveur proxy dans les propriétés du Serveur d'administration mais votre architecture réseau nécessite d'utiliser directement KPSN, activez l'option **Ignorer les paramètres du serveur proxy lors de la connexion à KPSN**. Dans le cas contraire, les requêtes des applications administrées ne peuvent pas atteindre le KPSN.

6. Configurez les paramètres de connexion du Serveur d'administration au service KSN proxy :

   - Sous **Paramètres de connexion**, pour **Port TCP**, indiquez le numéro du port TCP via lequel la connexion au serveur proxy KSN sera établie. Par défaut, la connexion au serveur proxy KSN est exécutée via le port 13111.
   - Pour que le Serveur d'administration se connecte au serveur proxy KSN via un port UDP, activez l'option **Utiliser un port UDP** et indiquez le numéro du port dans le champ **Port UDP**. Cette option est désactivée et le port TCP est utilisé par défaut. Si cette option est activée, la connexion au serveur proxy KSN est exécutée par défaut via le port UDP 15111.
   - Si vous souhaitez que le Serveur d'administration se connecte au serveur proxy KSN via un port HTTPS, activez l'option **Utiliser le protocole HTTPS par le port**, et spécifiez un numéro de port. Cette option est désactivée et le port TCP est utilisé par défaut. Si cette option est activée, la connexion au serveur proxy KSN est exécutée par défaut via le port HTTPS 17111.

7. Activez l'option **Connecter les Serveurs d'administration secondaires à KSN via le Serveur d'administration &principal**.

   Si cette option est activée, les Serveurs d'administration secondaires, quel que soit leur niveau hiérarchique, utilisent le Serveur d'administration principal comme serveur proxy KSN. Si cette option est désactivée, les Serveurs d'administration secondaires se connectent au KSN indépendamment. Dans ce cas, les appareils administrés utilisent les Serveurs d'administration secondaires comme serveurs proxy KSN.

   > Les Serveurs d'administration secondaires utilisent le Serveur d'administration principal comme serveur proxy si dans le volet droit de la section **Paramètres du proxy KSN**, dans les propriétés des Serveurs d'administration secondaires, la case **&Utiliser le Serveur d'administration comme serveur proxy** est cochée.

8. Cliquez sur le bouton **OK**.

Cela enregistre les paramètres d'accès à KSN.

Vous pouvez également configurer un accès de point de distribution à KSN, par exemple si vous souhaitez réduire la charge sur le Serveur d'administration. Le point de distribution dont le rôle du serveur proxy KSN envoie directement les requêtes KSN des appareils administrés à Kaspersky, sans utiliser le serveur d'administration.

Pour configurer l'accès du point de distribution à Kaspersky Security Network (KSN) :

1. Vérifiez que le point de distribution est assigné manuellement.
2. Dans l'arborescence de la console, sélectionnez l'entrée **Serveur d'administration**.
3. Dans le menu contextuel Serveur d'administration, sélectionnez l'option **Propriétés**.
4. Ouvrir à nouveau la fenêtre des propriétés du Serveur d'administration, sélectionnez la section **Points de distribution**.
5. Sélectionnez le point de distribution dans la liste et, cliquez sur le bouton **Propriétés** pour ouvrir la fenêtre de ses propriétés.
6. Dans la fenêtre des propriétés du point de distribution, dans la section **Proxy KSN**, sélectionnez **Accéder à KSN Cloud/KPSN directement via Internet**.
7. Cliquez sur le bouton **OK**.

Le point de distribution agit comme un serveur proxy KSN.

Activation et désactivation de KSN

Pour activer KSN, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le Serveur d'administration pour lequel vous devez activer KSN.
2. Dans le menu contextuel Serveur d'administration, sélectionnez l'option **Propriétés**.
3. Dans la fenêtre des propriétés du Serveur d'administration, dans la section **Proxy KSN**, sélectionnez la sous-section **Paramètres du proxy KSN**.

4. Sélectionnez **&Utiliser le Serveur d'administration comme serveur proxy**.

   Suite à cette action, le service du serveur proxy KSN est activé.

5. Cochez la case **&J'accepte les termes du Kaspersky Security Network**.

   KSN est ainsi activé.

   Si la case est cochée, les appareils clients transmettent les résultats de l'installation des correctifs à Kaspersky. Une fois que vous avez coché la case, vous devez lire et accepter les Conditions de la Déclaration KSN.

6. Cliquez sur le bouton **OK**.

Pour désactiver KSN, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le Serveur d'administration pour lequel vous devez activer KSN.
2. Dans le menu contextuel Serveur d'administration, sélectionnez l'option **Propriétés**.
3. Dans la fenêtre des propriétés du Serveur d'administration, dans la section **Proxy KSN**, sélectionnez la sous-section **Paramètres du proxy KSN**.
4. Décochez la case **Utiliser le Serveur d'administration comme serveur proxy** pour désactiver le service KSN proxy ou décochez la case **&J'accepte les termes du Kaspersky Security Network**.

   Si la case est décochée, les appareils clients ne transmettent pas les résultats de l'installation des correctifs à Kaspersky.

   Si vous utilisez KPSN, décochez la case **Configurer KPSN**.

   KSN est ainsi désactivé.

5. Cliquez sur le bouton **OK**.

Affichage de la Déclaration KSN acceptée

Lorsque vous activez Kaspersky Security Network (KSN), vous devez lire et accepter la Déclaration KSN. Vous pouvez consulter à tout moment la déclaration KSN.

Pour afficher la Déclaration KSN acceptée, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le Serveur d'administration pour lequel vous avez activé KSN.
2. Dans le menu contextuel Serveur d'administration, sélectionnez l'option **Propriétés**.
3. Dans la fenêtre des propriétés du Serveur d'administration, dans la section **Proxy KSN**, sélectionnez la sous-section **Paramètres du proxy KSN**.
4. Cliquez sur le lien **Afficher la Déclaration KSN acceptée**.

Dans la fenêtre qui s'ouvre, vous pouvez voir le texte de la Déclaration KSN acceptée.

Consulter les statistiques du serveur proxy KSN

Le *serveur proxy KSN* est un service qui assure l'interaction entre l'infrastructure de Kaspersky Security Network et les appareils clients qui sont administrés par le Serveur d'administration.

L'utilisation du serveur proxy KSN fournit les possibilités suivantes :

- Les appareils clients peuvent exécuter les demandes à KSN et transmettre dans KSN les informations même s'ils n'ont pas d'accès Internet direct.
- Le serveur proxy KSN met en cache les données traitées en diminuant la charge sur le canal du réseau externe et en accélérant l'obtention des informations demandées par l'appareil client.

Dans la fenêtre de propriétés du Serveur d'administration, vous pouvez configurer les paramètres du serveur proxy KSN et consulter des statistiques sur son utilisation.

Pour consulter les statistiques du serveur proxy KSN, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le Serveur d'administration pour lequel vous devez afficher les statistiques de KSN.
2. Dans le menu contextuel Serveur d'administration, sélectionnez l'option **Propriétés**.
3. Dans la fenêtre des propriétés du Serveur d'administration, sélectionnez la sous-section **Statistiques du proxy KSN** dans la section **Proxy KSN**.

   Cette section affiche les statistiques réelles de fonctionnement du serveur proxy KSN (le nombre d'enregistrements dans le cache, de paquets traités dans le cache et de paquets reçus). De plus, si le Serveur d'administration est connecté à KSN, le message d'information correspondant s'affiche.

   Si nécessaire, procédez comme suit :

   - Cliquez sur **Actualiser** pour mettre à jour les statistiques sur l'utilisation du serveur proxy KSN.
   - Cliquez sur le bouton **Exporter dans un fichier** pour exporter les statistiques dans un fichier au format CSV.
   - Cliquez sur le bouton **Vérifier la connexion à KSN** pour vérifier si le Serveur d'administration est actuellement connecté à KSN.
4. Cliquez sur **OK** pour fermer la fenêtre des propriétés du Serveur d'administration.

Accepter une Déclaration KSN mise à jour

Vous utilisez KSN conformément à la Déclaration KSN que vous lisez et acceptez en activant KSN. Si la Déclaration KSN est mise à jour, elle s'affiche lorsque vous mettez à jour ou mettez à niveau le Serveur d'administration. Vous pouvez accepter la Déclaration KSN mise à jour ou la refuser. Si vous la refusez, vous continuez à utiliser KSN conformément à la version précédente de la Déclaration KSN que vous avez acceptée auparavant.

Après la mise à jour ou la mise à niveau du Serveur d'administration, la Déclaration KSN mise à jour s'affiche automatiquement. Si vous refusez la Déclaration KSN mise à jour, vous pouvez toujours la consulter et l'accepter ultérieurement.

Pour afficher, puis accepter ou refuser une Déclaration KSN mise à jour, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez l'entrée **Serveur d'administration**.

2. Sous l'onglet **Surveillance**, dans la section **Surveillance**, cliquez sur le lien **La Déclaration de Kaspersky Security Network acceptée est obsolète**.

   La fenêtre **Déclaration KSN** s'ouvre.

3. Lisez attentivement la Déclaration KSN, puis faites votre choix. Si vous acceptez la Déclaration KSN mise à jour, cliquez sur le bouton **J'&accepte les termes du Contrat de licence**. Si vous refusez la Déclaration KSN mise à jour, cliquez sur le bouton **Annuler**.

En fonction de votre choix, KSN continue de fonctionner conformément aux conditions de la Déclaration KSN actuelle ou de celle qui est mise à jour. Vous pouvez consulter le texte de la Déclaration KSN acceptée dans les propriétés du Serveur d'administration à tout moment.

Protection complémentaire avec l'utilisation de Kaspersky Security Network

Kaspersky offre un niveau complémentaire de protection avec l'utilisation de Kaspersky Security Network. Ce mode de protection permet une lutte efficace contre les menaces dangereuses et les menaces du type zero-day (jour zéro). Les technologies Cloud unies avec Kaspersky Endpoint Security et les connaissances d'experts des experts de virus de Kaspersky assurent une protection puissante contre les menaces les plus difficiles.

Pour plus d'informations sur la protection complémentaire dans Kaspersky Endpoint Security, visitez le site Internet de Kaspersky.

Vérifier si le point de distribution fonctionne en tant que serveur proxy KSN

Sur un appareil administré qui fonctionne comme un point de distribution, vous pouvez activer le serveur proxy KSN. Un appareil administré fonctionne comme un serveur proxy KSN lorsque le service ksnproxy est exécuté sur l'appareil. Vous pouvez vérifier, activer ou désactiver ce service sur l'appareil localement.

Vous pouvez désigner un appareil Windows ou Linux comme point de distribution. La méthode de vérification du point de distribution dépend du système d'exploitation de ce point de distribution.

Pour vérifier si le point de distribution basé sur Windows fonctionne comme serveur proxy KSN, procédez comme suit :

1. Sur l'appareil du point de distribution, sous Windows, ouvrez **Services** (**Tous les programmes** → **Outils d'administration** → **Services**).

2. Dans la liste des services, vérifiez si le service ksnproxy est en cours d'exécution.

   Si le service ksnproxy est en cours d'exécution, l'Agent d'administration de l'appareil participe à Kaspersky Security Network et fonctionne comme serveur proxy KSN pour les appareils administrés inclus dans la zone d'action du point de distribution.

Si vous le souhaitez, vous pouvez désactiver le service ksnproxy. Dans ce cas, l'Agent d'administration sur le point de distribution cesse de participer à Kaspersky Security Network. Cela requiert des autorisations d'administrateur local.

Pour vérifier si le point de distribution basé sur Linux fonctionne comme serveur proxy KSN, procédez comme suit :

1. Sur l'appareil du point de distribution, affichez la liste des processus en cours d'exécution.

2. Dans la liste des processus en cours d'exécution, vérifiez si le processus `/opt/kaspersky/ksc64/sbin/ksnproxy` est en cours d'exécution.

Si le processus `/opt/kaspersky/ksc64/sbin/ksnproxy` est en cours d'exécution, l'Agent d'administration de l'appareil participe à Kaspersky Security Network et fonctionne comme serveur proxy KSN pour les appareils administrés inclus dans la zone d'action du point de distribution.

Basculer entre l'aide en ligne et l'aide hors ligne

Si vous n'avez pas accès à Internet, vous pouvez utiliser l'aide hors ligne.

Pour basculer entre l'aide en ligne et l'aide hors ligne, procédez comme suit :

1. Dans la fenêtre principale de Kaspersky Security Center, sélectionnez **Kaspersky Security Center 15.1** dans l'arborescence de la console.

2. Cliquez sur le lien **Paramètres d'interface globaux**.

   La fenêtre des paramètres s'ouvre.

3. Dans la fenêtre des paramètres, cliquez sur **Utiliser l'aide hors ligne**.

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

   Les paramètres sont appliqués et enregistrés. Si vous le souhaitez, vous pouvez à tout moment modifier les paramètres et commencer à utiliser l'aide en ligne.

Exportation des événements dans les systèmes SIEM

Cette section décrit la procédure d'exportation des événements enregistrés dans Kaspersky Security Center vers des systèmes d'administration des événements de sécurité de l'information externes (systèmes SIEM, Security Information and Event Management).

Configuration de l'export d'événements vers des systèmes SIEM

Kaspersky Security Center permet la configuration par l'une des méthodes suivantes : exportation vers n'importe quel système SIEM utilisant le format Syslog, exportation vers les systèmes QRadar, Splunk, ArcSight SIEM utilisant les formats LEEF et CEF ou exportation d'événements vers les systèmes SIEM directement depuis la base de données Kaspersky Security Center. Une fois ce scénario terminé, le Serveur d'administration envoie automatiquement les événements au système SIEM.

Prérequis

Avant de lancer l'exportation de la configuration des événements vers Kaspersky Security Center :

- En savoir plus sur les méthodes d'export d'événements.
- Assurez-vous de disposer des valeurs des paramètres système.

> Vous pouvez exécuter les étapes de ce scénario dans n'importe quel ordre.

Le processus d'exportation des événements vers le système SIEM comprend les étapes suivantes :

- **Configuration du système SIEM pour recevoir les événements de Kaspersky Security Center**

  Procédure : Configuration de l'exportation d'événements dans un système SIEM

- **Sélection des événements que vous souhaitez exporter vers le système SIEM :**

  Instructions pour :

  - Console d'administration : Marquage des événements d'une application Kaspersky pour l'exportation au format Syslog, Marquage des événements généraux pour l'exportation au format Syslog
  - Kaspersky Security Center Web Console : Marquage des événements d'une application Kaspersky pour l'exportation au format Syslog, Marquage d'événements généraux pour l'exportation au format Syslog

- **Configuration de l'exportation des événements dans le système SIEM en utilisant l'une des méthodes suivantes :**

  - Avec les protocoles TCP/IP, UDP ou TLS par TCP.

    Instructions pour :

    - Console d'administration : Configuration de l'exportation des événements vers les systèmes SIEM
    - Kaspersky Security Center Web Console : configuration de l'exportation des événements vers les systèmes SIEM

  - En utilisant l'exportation d'événements directement depuis la base de données Kaspersky Security Center (Un ensemble de représentations publiques se trouve dans la base de données de Kaspersky Security Center ; la description de ces représentations publiques figurent dans le document klakdb.chm).

Résultats

Une fois l'exportation des événements vers le système SIEM configurée, si vous avez sélectionné des événements que vous souhaitez exporte, vous pouvez afficher résultats de l'exportation.

Conditions préalables

Dans le cadre de la configuration de l'exportation des événements automatique dans Kaspersky Security Center, il faut définir certains paramètres du système SIEM. Il est recommandé de préciser ces paramètres au préalable afin de se préparer pour la configuration de Kaspersky Security Center.

Pour configurer l'exportation des événements automatique vers le système SIEM, il faut connaître la valeur des paramètres suivants :

- **Adresse du serveur du système SIEM**

  Adresse du serveur hébergeant le système SIEM à utiliser. Cette valeur doit être définie dans les paramètres du système SIEM.

- **Port du serveur du système SIEM**

  Le numéro de port pour une connexion entre Kaspersky Security Center et le serveur du système SIEM. Il faut définir cette valeur dans les paramètres de Kaspersky Security Center et les paramètres du récepteur du système SIEM.

- **Protocole**

  Le protocole utilisé pour la transmission des messages depuis Kaspersky Security Center vers le système SIEM. Il faut définir cette valeur dans les paramètres de Kaspersky Security Center et les paramètres du récepteur du système SIEM.

À propos des événements de Kaspersky Security Center

Kaspersky Security Center vous permet d'obtenir des informations sur les événements survenus pendant le fonctionnement du Serveur d'administration et des applications Kaspersky installées sur les appareils administrés. Les informations relatives aux événements sont conservées dans la base de données du Serveur d'administration. Vous pouvez exporter ces informations dans des systèmes SIEM externes. L'exportation des informations relatives aux événements vers des systèmes SIEM externes permet à l'administrateur des systèmes SIEM de réagir efficacement aux événements du système de sécurité survenus sur les appareils administrés ou dans les groupes d'administration.

Types d'événement

Dans Kaspersky Security Center, il existe les types d'événements suivants :

- Événements généraux. Ces événements se produisent dans toutes les applications Kaspersky administrées. Voici un exemple d'événement général : Attaque de virus. Les événements généraux ont une syntaxe et une sémantique strictement définies. Les événements généraux sont utilisés, par exemple, dans les rapports et les tableaux de bord.

- Événements spécifiques aux applications Kaspersky administrées. Chaque application de Kaspersky administrée possède son propre ensemble d'événements.

Sources de l'événement

Les événements peuvent être générés par les applications suivantes :

- Modules de Kaspersky Security Center :
  - Serveur d'administration
  - Agent d'administration
  - Serveur MDM iOS
- Applications Kaspersky administrées

  Pour en savoir plus sur les événements générés par les applications administrées par Kaspersky, veuillez consulter la documentation de l'application correspondante.

Vous pouvez consulter la liste complète des événements qui peuvent être générés par une application sous l'onglet **Configuration des événements** dans la stratégie de l'application. Pour le Serveur d'administration, vous pouvez également consulter la liste des événements dans les propriétés du Serveur d'administration.

Niveau d'importance des événements

Chaque événement possède le niveau d'importance personnel. En fonction des conditions dans lesquelles l'événement s'est produit, il peut recevoir un niveau d'importance différent. Il existe quatre niveaux d'importance pour les événements :

- *Événement critique* : événement qui indique l'apparition d'un problème critique qui peut entraîner une perte de données, un échec ou une erreur critique.
- *Erreur de fonctionnement* : événement qui indique l'apparition d'un problème sérieux, d'une erreur ou d'un échec survenu pendant le fonctionnement de l'application ou l'exécution de la procédure.
- *Avertissement* événement qui n'est pas forcément sérieux, mais qui pourrait entraîner des problèmes à l'avenir. Le plus souvent les événements appartiennent à la catégorie Avertissement, si vous pouvez rétablir le fonctionnement de l'application par la suite, sans perte de données ou de fonctions.
- *Information* : événement qui vise à informer sur la réussite d'une opération, le fonction adéquat de l'application ou la fin d'une procédure.

On définit pour chaque événement la durée de conservation pendant laquelle l'événement peut être consulté ou modifié dans Kaspersky Security Center. Certains événements ne sont pas conservés par défaut dans la base de données du Serveur d'administration car la durée de conservation définie pour ceux-ci est égale à zéro. L'exportation vers des systèmes externes est uniquement possible pour les événements conservés dans la base de données du Serveur d'administration depuis moins d'un jour.

À propos de l'exportation des événements

L'exportation des événements peut être utilisée dans les systèmes centralisés qui traitent des questions de sécurité au niveau organisationnel et technique, qui surveillent les systèmes de sécurité et consolident les données issues de différentes solutions. Parmi ces système, il y a les systèmes SIEM qui garantissent l'analyse des alertes des systèmes de sécurité et des événements de la configuration matérielle réseau et des applications en temps réel, sans oublier les centres d'administration de la sécurité (Security Operation Center, SOC).

Les systèmes SIEM récoltent des données auprès de différentes sources, dont des réseaux des systèmes de sécurité, des serveurs, des bases de données et des applications. Ils assurent aussi la fonction de regroupement des données traitées, ce qui ne vous permet pas d'ignorer les événements critiques. De plus, ces systèmes exécutent l'analyse automatique des événements associés et des signaux d'alerte pour prévenir les administrateurs des problèmes du système de sécurité qui requièrent une solution immédiate. Les notifications peuvent s'afficher sur les barres des indicateurs ou être envoyées par des canaux tiers, par exemple, par email.

La procédure d'exportation des événements de Kaspersky Security Center vers les systèmes SIEM fait intervenir deux parties : l'expéditeur des événements (Kaspersky Security Center), et le destinataire de ceux-ci (le système SIEM). Pour que l'exportation des événements réussisse, il faut réaliser une configuration dans le système SIEM utilisé et dans Kaspersky Security Center. L'ordre des configurations n'a pas d'importance : Vous pouvez commencer par configurer l'envoi des événements à Kaspersky Security Center, puis passer à la configuration de la réception de ceux-ci du côté du système SIEM ou inversement.

Modes d'envoi des événements de Kaspersky Security Center

Il existe trois modes d'envoi des événements depuis Kaspersky Security Center vers les systèmes externes :

- Envoi des événements via le protocole Syslog à n'importe quel système SIEM.

  Le protocole Syslog permet de transmettre n'importe quel événement survenu sur le Serveur d'administration de Kaspersky Security Center et dans les applications de Kaspersky installées sur les appareils administrés. Le protocole Syslog est un protocole standard d'enregistrement de messages. Vous pouvez l'utiliser pour exporter des événements vers n'importe quel système SIEM.

  Pour cela, vous devez marquer les événements que vous souhaitez relayer au système SIEM. Vous pouvez marquer les événements dans la Console d'administration ou dans Kaspersky Security Center Web Console). Seuls les événements marqués seront relayés au système SIEM. Si vous n'avez rien coché, aucun événement ne sera relayé.

- Envoi des événements via les protocoles CEF et LEEF vers les systèmes QRadar, Splunk et ArcSight.

  Vous pouvez utiliser les protocoles CEF et LEEF pour exporter des événements généraux. Dans le cadre de l'exportation des événements via les protocoles CEF et LEEF, vous ne pouvez pas sélectionner les événements à exporter. Tous les événements généraux sont exportés. Pour convertir les événements de Kaspersky Security Center en événements au format CEF et LEEF, vous devez utiliser le fichier siem_conversion_rules.xml. Ce fichier contient la liste des attributs d'événements de Kaspersky Security Center et les attributs correspondants des événements au format CEF et LEEF. De plus, le fichier siem_conversion_rules.xml contient les règles de génération de messages correspondant aux événements. Ce fichier figure dans le kit de distribution de Kaspersky Security Center.

  A la différence du protocole Syslog, les protocoles CEF et LEEF ne sont pas universels. CEF et LEEF sont destinés aux systèmes SIEM correspondants (QRadar, Splunk et ArcSight). Par conséquent, quand vous décidez d'exporter des événements via un de ces protocoles, vous devez utiliser l'analyseur requis dans le système SIEM.

- Directement depuis la base de données de Kaspersky Security Center vers n'importe quel système SIEM.

  Ce mode d'exportation des événements peut être utilisé pour obtenir des événements directement depuis les représentations publiques de la base de données avec l'l'aide des de requêtes SQL. Les résultats de l'exécution de la requête sont enregistrés dans le fichier .xml qui peut être utilisé pour les données d'entrée du système externe. L'exportation directe depuis la base de données concerne uniquement les événements accessibles dans les représentations publiques.

Réception des événements par le système SIEM

Le système SIEM doit accepter et analyser correctement les événements en provenance de Kaspersky Security Center. Il faut pour cela configurer le système SIEM. La configuration dépend du système SIEM utilisé en particulier. Toutefois, il existe une série d'étapes communes à l'ensemble des systèmes SIEM : la configuration du récepteur et de l'analyseur.

À propos de la configuration de l'exportation d'événements dans le système SIEM

La procédure d'exportation des événements de Kaspersky Security Center vers les systèmes SIEM fait intervenir deux parties : l'expéditeur des événements (Kaspersky Security Center), et le destinataire de ceux-ci (le système SIEM). Vous devez configurer l'exportation dans votre système SIEM et dans Kaspersky Security Center.

Les configurations réalisées du système SIEM dépendent du système que vous utilisez. Quoi qu'il en soit, il faut configurer le récepteur des messages pour tous les systèmes SIEM et, le cas échéant, l'analyseur des messages afin de pouvoir décomposer les messages reçus en champs.

Configuration du récepteur des messages

Pour le système SIEM, il faut configurer le récepteur des événements envoyés par Kaspersky Security Center. En général, il faut définir les paramètres suivants dans le système SIEM :

- **Protocole de l'exportation ou type de données entrantes**

  Le protocole de transmission des messages peut être TCP/IP ou UDP. Il est nécessaire d'indiquer le même protocole que celui qui a été choisi dans Kaspersky Security Center pour envoyer les événements.

- **Port**

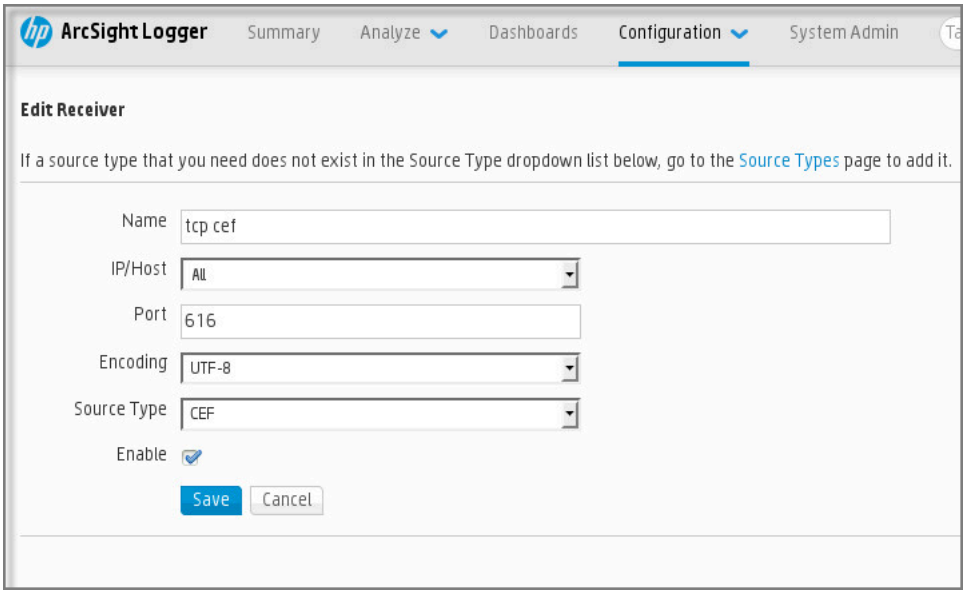
  Le numéro de port pour se connecter à Kaspersky Security Center. Il est nécessaire d'indiquer le même numéro de port que celui qui a été choisi dans Kaspersky Security Center pour envoyer les événements.

- **Protocole de transfert de messages ou type de données sortantes**

  Le protocole utilisé pour l'exportation des événements vers le système SIEM. Il peut s'agir d'un des protocoles standard : Syslog, CEF ou LEEF. Le système SIEM choisit l'analyseur d'événements qui correspond au protocole indiqué.

En fonction du système SIEM utilisé, vous devrez peut-être définir des paramètres avancés pour le récepteur de messages.

La figure ci-dessous représente la configuration d'un récepteur dans ArcSight.



Configuration du récepteur dans ArcSight

Analyseur des messages

Les événements exportés sont transmis au systèmes SIEM sous la forme de messages. Ces messages sont ensuite soumis à l'analyseur afin que les informations relatives aux événements soient transmises correctement au système SIEM. L'analyseur des messages est inséré au système SIEM il permet de décomposer le message en ses champs comme l'identifiant du message, le niveau d'importance, la description et d'autres paramètres. Le système SIEM peut ainsi traiter les événements envoyés par Kaspersky Security Center afin qu'ils soient enregistrés dans la base de données du système SIEM.

Marquage des événements pour l'export vers les systèmes SIEM au format Syslog

Une fois que l'exportation automatique des événements a été activée, il faut sélectionner les événements à exporter dans le système SIEM externe.

Vous pouvez configurer l'exportation des événements au format Syslog dans le système externe selon une des conditions suivantes :

- Marquage d'événements généraux. Si vous marquez des événements à exporter dans une stratégie, dans les paramètres d'un événement ou dans les paramètres du Serveur d'administration, le système SIEM recevra les événements marqués qui se sont produits dans toutes les applications administrées par la stratégie spécifique. Si des événements à exporter ont été choisis dans la stratégie, vous ne serez pas en mesure de les redéfinir pour une application distincte administrée par cette stratégie.

- Marquage des événements pour une application administrée. Si vous marquez les événements à exporter pour une application administrée installée sur un appareil administré, le système SIEM reçoit uniquement les événements survenus dans cette application.

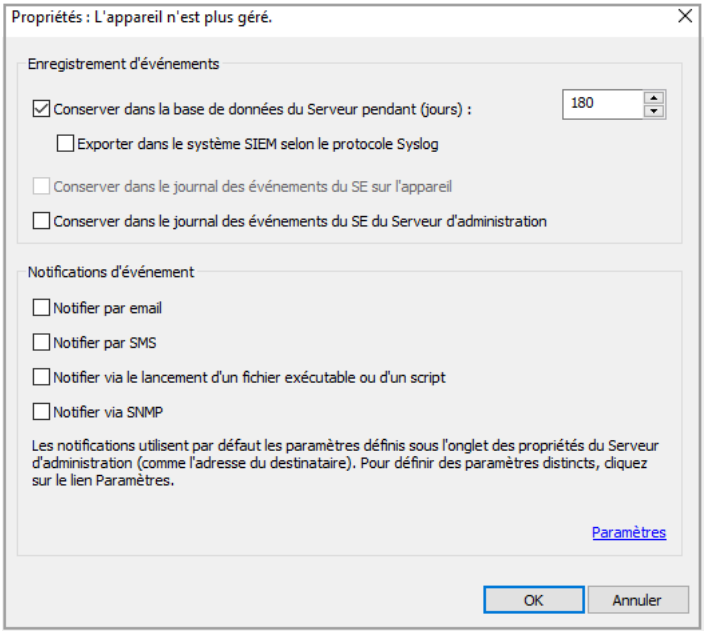
Marquage des événements d'une application Kaspersky pour l'exportation au format Syslog

Si vous souhaitez exporter des événements survenus dans une application administrée en particulier installée sur un appareil administré, marquez les événements à exporter pour celle-ci. Si des événements déjà exportés ont été marqués dans la stratégie, vous ne serez pas en mesure de redéfinir les événements marqués pour une application distincte administrée par cette stratégie.

Pour marquer les événements à exporter pour une application administrée en particulier, procédez comme suit :

1. Dans l'arborescence de la console de Kaspersky Security Center, sélectionnez l'entrée **Appareils administrés**, puis accédez à l'onglet **Appareils**.
2. Ouvrez le menu contextuel de l'appareil requis d'un clic droit, puis sélectionnez l'option **Propriétés**.
3. Dans la fenêtre des propriétés de l'appareil qui s'ouvre, sélectionnez la section **Applications**.
4. Dans la liste des applications qui s'affiche, choisissez l'application dont vous voulez exporter les événements, puis cliquez sur le bouton **Propriétés**.
5. Dans la fenêtre des propriétés des applications, sélectionnez la section **Configuration de l'événement**.
6. Dans la liste des événements qui s'affiche, choisissez un ou plusieurs événements à exporter dans le système SIEM, puis cliquez sur le bouton **Propriétés**.
7. Dans la fenêtre des propriétés de l'événement qui s'affiche, cochez la case **Exporter dans le système SIEM selon le protocole Syslog** pour marquer les événements sélectionnés pour l'exportation au format Syslog. Décochez la case **Exporter dans le système SIEM selon le protocole Syslog** pour supprimer la marque des événements sélectionnés pour l'exportation au format Syslog.

> Si les propriétés d'événement sont définies dans la stratégie, les champs de cette fenêtre ne peuvent pas être modifiés.



Fenêtre des propriétés des événements

8. Cliquez sur le bouton **OK** afin d'enregistrer les modifications.

9. Cliquez sur le bouton **OK** dans la fenêtre des propriétés de l'application et dans la fenêtre des propriétés de l'appareil.

Les événements marqués seront envoyés au système SIEM via le format Syslog. Les événements dont vous avez désélectionné la case à cocher **Exporter dans le système SIEM selon le protocole Syslog** ne seront pas exportés vers un système SIEM. L'exportation débute directement après l'activation de l'exportation automatique et sélectionne les événements à exporter. Réalisez la configuration du système SIEM afin de garantir la réception des événements de Kaspersky Security Center.

Marquage d'événements généraux pour l'exportation au format Syslog

Si vous souhaitez exporter des événements survenus dans toutes les applications administrées par une stratégie définie, choisissez les événements à exporter dans la stratégie. Dans ce cas, il est impossible de choisir des événements pour une application administrée particulière.

Pour marquer des événements généraux à exporter vers un système SIEM, procédez comme suit :

1. Dans l'arborescence de la console de Kaspersky Security Center, sélectionnez l'entrée **Stratégies**.

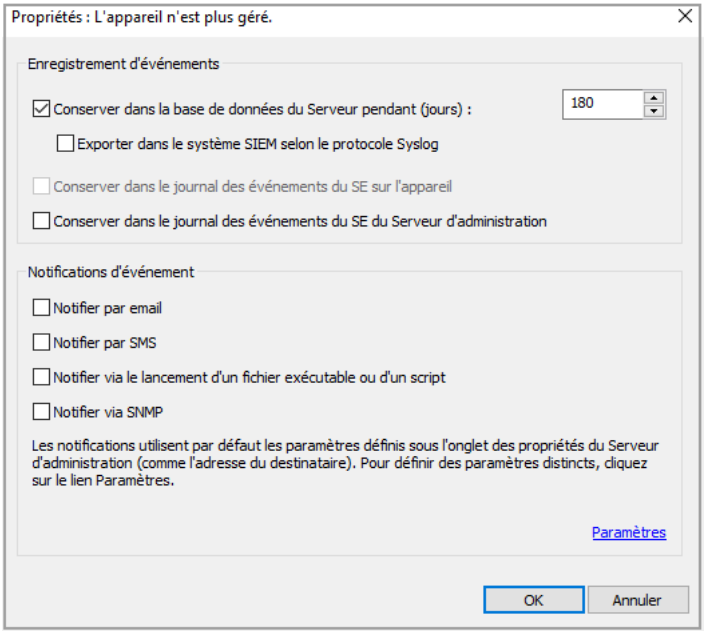
2. Ouvrez le menu contextuel de la stratégie concernée d'un clic droit, puis sélectionnez l'option **Propriétés**.

3. Dans la fenêtre des propriétés de la stratégie qui s'ouvre, sélectionnez la section **Configuration de l'événement**.

4. Dans la liste des événements qui s'affiche, choisissez un ou plusieurs événements à exporter dans le système SIEM, puis cliquez sur le bouton **Propriétés**.

   S'il faut choisir tous les événements, cliquez sur le bouton **Tout sélectionner**.

5. Dans la fenêtre des propriétés de l'événement qui s'affiche, cochez la case **Exporter dans le système SIEM selon le protocole Syslog** pour marquer les événements sélectionnés pour l'exportation au format Syslog. Désélectionnez la case à cocher **Exporter dans le système SIEM selon le protocole Syslog** pour supprimer la marque des événements sélectionnés pour l'exportation au format Syslog.



Fenêtre des propriétés des événements du Serveur d'administration

6. Cliquez sur le bouton **OK** afin d'enregistrer les modifications.

7. Dans la fenêtre des propriétés de la stratégie, cliquez sur le bouton **OK**.

Les événements marqués seront envoyés au système SIEM via le format Syslog. Les événements dont vous avez désélectionné la case à cocher **Exporter dans le système SIEM selon le protocole Syslog** ne seront pas exportés vers un système SIEM. L'exportation débute directement après l'activation de l'exportation automatique et sélectionne les événements à exporter. Réalisez la configuration du système SIEM afin de garantir la réception des événements de Kaspersky Security Center.

À propos de l'exportation des événements via le format Syslog

Le format Syslog permet d'exporter dans les systèmes SIEM les événements survenus sur le Serveur d'administration et dans d'autres applications de Kaspersky installées sur les appareils administrés.

Syslog est un protocole standard d'enregistrement des messages. Ce protocole permet de distinguer le logiciel qui génère les messages, le système dans lequel les messages sont enregistrés et le logiciel qui analyse les messages et génère les rapports. Chaque message reçoit un code d'appareil qui indique le type de logiciel qui a permis de créer le message et le niveau de gravité.

Le format Syslog est défini par les documents Request for Comments, RFC, publié par l'Internet Engineering Task Force (standards Internet). Le standard RFC 5424 est le standard utilisé pour exporter les événements de Kaspersky Security Center vers les systèmes externes.

Il est possible de configurer l'exportation des événements vers des systèmes externes à l'aide du format Syslog dans Kaspersky Security Center.

Le processus d'exportation comprend deux étapes :

1. Activation de l'exportation des événements automatique. Cette étape correspond à la configuration de Kaspersky Security Center de telle sorte que les événements soient envoyés au système SIEM. L'envoi des événements de Kaspersky Security Center commence dès l'activation de l'exportation automatique.

2. Sélection des événements à exporter vers le système externe. Cette étape correspond à la sélection des événements à exporter vers le système SIEM.

À propos de l'exportation des événements via les formats CEF et LEEF

Vous pouvez utiliser les formats CEF et LEEF pour exporter vers les systèmes SIEM des événements généraux, ainsi que les événements transférés par les applications Kaspersky vers le Serveur d'administration. L'ensemble des événements à exporter est défini préalablement et il est impossible de sélectionner les événements à exporter. Avant d'envoyer des événements au système SIEM (QRadar, ArcSight ou Splunk), il est nécessaire d'interpréter les événements de Kaspersky Security Center en événements au format CEF et LEEF en utilisant les règles indiquées dans le fichier siem_conversion_rules.xml.

Choisissez le format d'exportation en fonction du système SIEM que vous utilisez. Le tableau suivant reprend les systèmes SIEM et les formats d'exportation qui leur correspond.

Formats d'exportation des événements dans le système SIEM

Système SIEM	Format d'exportation
QRadar	LEEF
ArcSight	CEF
Splunk	CEF

- LEEF est un format spécial des événements pour IBM Security QRadar SIEM. QRadar peut intégrer, identifier et traiter les événements LEEF. Le protocole LEEF requiert l'utilisation du codage UTF-8. Pour en savoir plus sur le protocole LEEF, consultez la page Internet du IBM Knowledge Center.

- CEF est un standard d'administration de type " journal ouvert " qui améliore la compatibilité des informations du système de sécurité de différents appareils et applications réseau. Le protocole CEF permet d'utiliser le format général du journal des événements pour que les systèmes d'administration de l'entreprise puissent recevoir et regrouper facilement les données pour l'analyse. Le protocole CEF requiert l'utilisation du codage UTF-8.

Lors de l'exportation automatique, Kaspersky Security Center envoie les événements généraux au système SIEM. L'exportation automatique des événements dès l'activation. Cette section décrit la procédure d'activation de l'exportation des événements automatique.

Configuration de Kaspersky Security Center pour l'exportation des événements vers le système SIEM

Vous pouvez activer l'exportation automatique des événements dans Kaspersky Security Center.

Seuls les événements généraux peuvent être exportés depuis les applications administrées aux formats CEF et LEEF. Les règles d'interprétation utilisées pour convertir les événements aux formats CEF et LEEF sont indiquées dans le fichier siem_conversion_rules.xml inclus dans le kit de distribution de Kaspersky Security Center. Les événements propres aux applications ne peuvent pas être exportés depuis les applications administrées aux formats CEF et LEEF. Si vous devez exporter les événements des applications administrées ou un ensemble d'événements défini par l'utilisateur et configuré à l'aide des stratégies des applications administrées, vous devez exporter les événements dans le format Syslog.

Pour activer l'exportation automatique des événements, procédez comme suit :

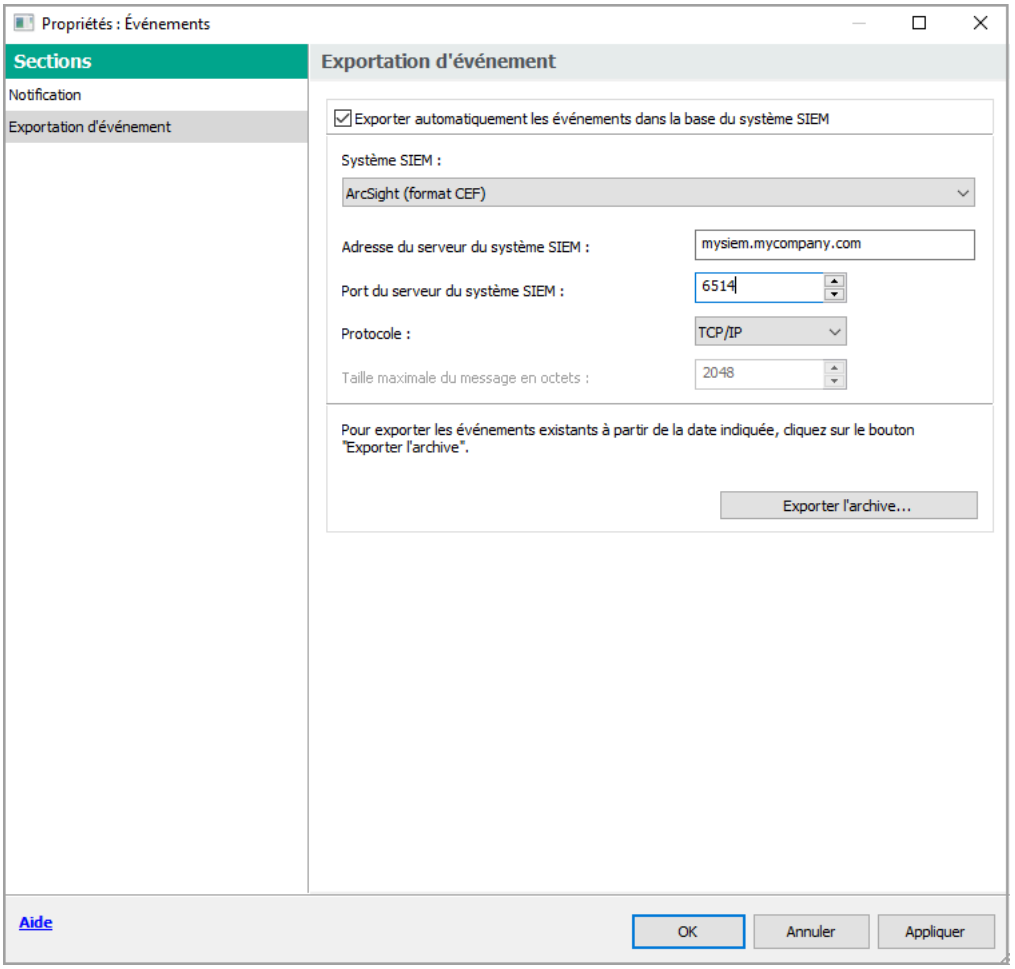
1. Dans l'arborescence de la console de Kaspersky Security Center, sélectionnez l'entrée qui porte le nom du Serveur d'administration dont il faut exporter les événements.

2. Dans l'espace de travail du Serveur d'administration sélectionné, sélectionnez l'onglet **Événements**.

3. Cliquez sur la flèche déroulante en regard du lien **Configurer les paramètres des notifications et d'exportation des événements** et sélectionnez **Configurer l'exportation vers le système SIEM** dans la liste déroulante.

   La fenêtre des propriétés des événements s'ouvre, affichant la section **Exportation d'événement**.

4. Dans la section **Exportation d'événement**, définissez les paramètres d'exportation suivants :



Section Exportation des événements de la fenêtre des propriétés des événements

- **Exporter automatiquement les événements dans la base du système SIEM**

  Cochez cette case pour activer l'exportation automatique des événements dans le système SIEM. Si vous cochez cette case, tous les champs de la section **Exportation des événements** peuvent être modifiés.

- **Système SIEM**

  Sélectionnez le système SIEM pour exporter les événements suivants : QRadar® (format LEEF), ArcSight (format CEF), Splunk® (format CEF) et format Syslog (RFC 5424).

  Si vous sélectionnez le format Syslog, vous devez spécifier :

  Taille maximale du message en octets

  Indiquez la taille maximale en octets d'un message transmis au système SIEM. Chaque événement entraîne l'envoi d'un message. Si la longueur réelle du message dépasse la valeur indiquée, le message est tronqué et vous risquez de perdre des données. Par défaut, la taille du message est de 2048 octets. Ce champ est accessible uniquement si vous avez choisi le format Syslog dans le champ **Système SIEM**.

- **Adresse du serveur du système SIEM**

Renseignez l'adresse du serveur du système SIEM. L'adresse du serveur peut être renseignée au format DNS, sous la forme du nom NetBIOS ou en tant qu'adresse IP.

- **Port du serveur du système SIEM**

  Indiquez le numéro de port pour la connexion au serveur du système SIEM. Ce numéro doit correspondre au numéro de port défini dans les paramètres du récepteur du système SIEM pour recevoir les événements (cf. section Configuration du système SIEM).

- **Protocole**

Choisissez le protocole de transfert des messages dans le système SIEM. Vous avez le choix entre les protocoles TCP/IP, UDP ou TLS par TCP.

Précisez les paramètres TLS suivants si vous sélectionnez le protocole TLS par TCP :

- **Authentification du serveur SIEM**

  Choisissez l'une des méthodes suivantes pour authentifier le serveur du système SIEM :

  - **En utilisant les certificats CA**. Vous pouvez recevoir un fichier avec la liste des certificats des autorités de certification de confiance et charger le fichier dans Kaspersky Security Center. Kaspersky Security Center vérifie si le certificat du serveur du système SIEM est également signé par une autorité de certification de confiance ou non.

    Pour ajouter un certificat de confiance, cliquez sur le bouton **Parcourir**, puis téléchargez le certificat.

    Si vous choisissez l'option **En utilisant les certificats CA**, vous pouvez définir les objets dans le champ **Sujets des certificats du serveur (facultatif)**. *Le nom du sujet* est un nom de domaine pour lequel le certificat est reçu. Kaspersky Security Center ne peut pas se connecter au serveur du système SIEM si le nom de domaine du serveur du système SIEM ne correspond pas au nom du sujet du certificat du serveur du système SIEM. Cependant, le serveur du système SIEM peut changer son nom de domaine si vous changez le nom du sujet dans le certificat. Dans ce cas, vous pouvez spécifier des noms de sujet dans le champ **Sujets des certificats du serveur (facultatif)**. Si l'un des noms du sujet spécifiés correspond au nom du sujet du certificat du système SIEM, Kaspersky Security Center valide le certificat du serveur du système SIEM.

  - **En utilisant les empreintes SHA1 des certificats du serveur**. Vous pouvez spécifier les empreintes SHA-1 des certificats du système SIEM dans Kaspersky Security Center. Pour ajouter une empreinte SHA-1, saisissez-la dans le champ sous l'option.

- **Authentification du client**

  Pour l'authentification du client, vous pouvez insérer votre certificat ou le générer dans Kaspersky Security Center.

  - **Insert certificate**. Vous pouvez utiliser un certificat que vous avez reçu de n'importe quelle source, par exemple, de n'importe quelle autorité de certification de confiance. Pour insérer un certificat existant, cliquez sur le bouton **Parcourir le certificat**. Dans la fenêtre **Certificat** qui s'ouvre, choisissez l'un des types de certificats suivants, puis renseignez le certificat et sa clé privée :

    - **Certificat X.509**. Chargez un fichier avec une clé privée dans le champ **Clé privée (*.prk, *.pem)** et un fichier avec un certificat dans le champ **Certificat (*.cer)**. Pour ce faire, cliquez sur le bouton **Parcourir** situé à droite du champ correspondant, puis ajoutez le fichier requis. Les deux fichiers ne dépendent pas l'un de l'autre, et l'ordre de chargement des fichiers est sans importance. Lorsque les deux fichiers sont téléchargés, indiquez le mot de passe pour le décodage de la clé privée dans le champ **Mot de passe**. Le mot de passe peut présenter une valeur vide si la clé privée n'est pas encodée.

    - **Conteneur PKCS#12**. Téléchargez un seul fichier qui contient un certificat et sa clé privée dans le champ **Fichier du certificat**. Pour ce faire, cliquez sur le bouton **Parcourir** situé à droite du champ, puis ajoutez le fichier requis. Lorsque le fichier a été téléchargé, indiquez le mot de passe pour le décodage de la clé privée dans le champ **Mot de passe**. Le mot de passe peut présenter une valeur vide si la clé privée n'est pas encodée.

  - **Generate key**. Vous pouvez générer un certificat auto-signé dans Kaspersky Security Center. Cliquez sur le bouton **Générer un certificat**, puis saisissez un nom d'objet dans le champ **Objet**. Le certificat client est généré pour ce nom d'objet et l'empreinte SHA-1 de ce certificat s'affiche dans le champ **Empreinte SHA1 du certificat client**. Par conséquent, Kaspersky Security Center stocke le certificat auto-signé généré et vous pouvez transmettre la partie publique du certificat ou l'empreinte SHA-1 au système SIEM.

5. Si vous souhaitez exporter vers la base de données système SIEM les événements survenus après une date définie dans le passé, cliquez sur le bouton **E&xporter l'archive**, puis indiquez la date à partir de laquelle les événements seront exportés. Par défaut, l'exportation des événements débute directement après l'activation.

6. Pour vérifier que la connexion au système SIEM a été configurée, cliquez sur le bouton **Tester les paramètres**.

   L'application tente d'établir une connexion avec le serveur système SIEM et d'envoyer un événement de test. Si la connexion n'est pas établie, un message d'erreur s'affiche. Si la connexion est établie, aucun message ne s'affiche. Vous pouvez consulter l'événement test dans l'onglet **Événements**, si nécessaire.

7. Cliquez sur le bouton **OK**.

L'exportation automatique des événements est activée.

Une fois que l'exportation automatique des événements a été activée, il faut sélectionner les événements à exporter dans le système SIEM.

Exportation des événements directement depuis la base de données

Vous pouvez extraire les événements directement de la base de données de Kaspersky Security Center sans passer par l'interface de Kaspersky Security Center. Il est possible de créer des requêtes directement pour des représentations publiques et d'extraire de celles-ci les données relatives aux événements ou de créer vos propres représentations sur la base des représentations publiques existantes et de les sonder pour obtenir les données requises.

Représentations publiques

Pour vous simplifier la tâche, la base de données de Kaspersky Security Center contient une sélection de représentations publiques. Le document klakdb.chm contient une description des représentations publiques.

La représentation publique v_akpub_ev_event contient un ensemble des champs correspondant aux paramètres des événements dans la base de données. Le document klakdb.chm contient aussi les informations relatives aux représentations publiques en rapport avec d'autres objets de Kaspersky Security Center, par exemple, les appareils, les applications, les utilisateurs. Vous pouvez utiliser ces informations lors de la création des requêtes.

Cette section fournit les instructions relatives à l'exécution d'une requête SQL à l'aide de l'utilitaire klsql2 ainsi qu'un exemple d'une telle requête.

Vous pouvez également utiliser n'importe quelles autres applications de gestion de bases de données pour créer des requêtes SQL et des représentations de bases de données. Les informations sur l'affichage des paramètres de connexion à la base de données de Kaspersky Security Center, comme le nom d'instance et le nom de la base de données figurent dans la section correspondante.

Exécution d'une requête SQL à l'aide de l'utilitaire klsql2

Cette section fournit des instructions sur le téléchargement et l'utilisation de l'utilitaire klsql2 ainsi que sur l'exécution d'une requête SQL à l'aide de cet utilitaire.

Pour utiliser l'utilitaire klsql2 :

1. Localisez l'utilitaire klsql2 dans le dossier d'installation de Kaspersky Security Center. Chemin d'installation par défaut est <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center. N'utilisez pas les versions de l'utilitaire klsql2 destinées aux anciennes versions de Kaspersky Security Center.

2. Créez un fichier avec l'extension .sql dans n'importe quel éditeur de texte et placez le fichier dans le même dossier que l'utilitaire.

3. Dans le fichier .sql créé, entrez la requête SQL souhaitée, puis enregistrez le fichier.

4. Sur l'appareil sur lequel le Serveur d'administration de Kaspersky Security Center est installé, saisissez la commande suivante dans la ligne de commande pour exécuter la requête SQL depuis le fichier .sql et enregistrer les résultats dans le fichier result.xml :
   ```
   klsql2 -i src.sql -u <nom d'utilisateur> -p <mot de passe> -o result.xml
   ```
   où `<nom d'utilisateur>` et `<mot de passe>` sont les identifiants du compte qui a accès à la base de données.

5. Si nécessaire, saisissez le login et le mot de passe du compte qui a accès à la base de données.

6. Ouvrez les fichiers result.xml obtenus et consultez les résultats de l'exécution de la requête SQL.

Vous pouvez modifier le fichier .sql et créer dans celui-ci, n'importe quelle requête SQL de représentation publique. Ensuite, lancez la requête SQL et l'enregistrement des résultats dans un fichier via la ligne de commande.

Exemple de requête SQL créée à l'aide de l'utilitaire klsql2

Cette section fournit un exemple de requête SQL exécutée à l'aide de l'utilitaire klsql2.

Les exemples suivants montrent comment récupérer la liste des événements survenus sur les appareils des utilisateurs au cours des sept derniers jours et la trier selon l'heure de l'événement. Les événements les plus récents sont affichés en premier.

Exemple pour Microsoft SQL Server :

```
SELECT
  /* identificateur d'événement */
  e.nId,

  /* heure de l'événement */
  e.tmRiseTime,

  /* nom interne du type d'événement */
  e.strEventType,

  /* nom de l'événement affiché */
  e.wstrEventTypeDisplayName,

  /* description de l'événement affichée */
  e.wstrDescription,

  /* nom du groupe où se trouve l'appareil */
  e.wstrGroupName,

  /* nom de l'appareil affiché sur lequel l'événement s'est produit */
  h.wstrDisplayName,
  CAST(((h.nIp / 16777216) & 255) AS varchar(4)) + '.' +
  CAST(((h.nIp / 65536) & 255) AS varchar(4)) + '.' +
  CAST(((h.nIp / 256) & 255) AS varchar(4)) + '.' +

  /* adresse IP de l'appareil sur lequel l'événement s'est produit */
  CAST(((h.nIp) & 255) AS varchar(4)) as strIp
FROM v_akpub_ev_event e
  INNER JOIN v_akpub_host h ON h.nId=e.nHostId
WHERE e.tmRiseTime>=DATEADD(Day, -7, GETUTCDATE())
ORDER BY e.tmRiseTime DESC
```

Exemple pour PostgreSQL :

```
SELECT
  /* identificateur d'événement */
  "e"."nId",

  /* heure de l'événement */
  "e"."tmRiseTime",

  /* nom interne du type d'événement */
  "e"."strEventType",

  /* nom de l'événement affiché */
  "e"."wstrEventTypeDisplayName",

  /* description de l'événement affichée */
  "e"."wstrDescription",

  /* description de l'événement affichée */
  "e"."wstrGroupName",

  /* nom de l'appareil affiché sur lequel l'événement s'est produit */
  "h"."wstrDisplayName",
  (
    CAST((("h"."nIp" / 16777216 )& 255 ) AS VARCHAR(4))  || '.'  ||
    CAST((("h"."nIp" / 65536 )& 255 ) AS VARCHAR(4))  || '.'  ||
    CAST((("h"."nIp" / 256 )& 255 ) AS VARCHAR(4))  || '.'  ||

    /* adresse IP de l'appareil sur lequel l'événement s'est produit */
    CAST((("h"."nIp" )& 255 ) AS VARCHAR(4))
  )  AS "strIp"
FROM "v_akpub_ev_event"  AS "e"
  INNER JOIN  "v_akpub_host"  AS "h" ON "h"."nId" = "e"."nHostId"
WHERE "e"."tmRiseTime" >= NOW() AT TIME ZONE 'utc'  + make_interval(days => CAST(-7  AS INT))
ORDER BY "e"."tmRiseTime" DESC ;
```

Exemple pour MySQL ou MariaDB :

```
SELECT

  /* identificateur d'événement */
  `e`.`nId`,

  /* heure de l'événement */
  `e`.`tmRiseTime`,

  /* nom interne du type d'événement */
  `e`.`strEventType`,

  /* nom de l'événement affiché */
  `e`.`wstrEventTypeDisplayName`,

  /* description de l'événement affichée */
  `e`.`wstrDescription`,

  /* nom du groupe d'appareils */
  `e`.`wstrGroupName`,

  /* nom de l'appareil affiché sur lequel l'événement s'est produit */
  `h`.`wstrDisplayName`,
  CONCAT(
    LEFT(CAST(((`h`.`nIp`  DIV  1677721) & 255) AS CHAR), 4), '.',
    LEFT(CAST(((`h`.`nIp`  DIV  65536) & 255) AS CHAR), 4), '.',
    LEFT(CAST(((`h`.`nIp`  DIV  256) & 255) AS CHAR), 4), '.',

    /* adresse IP de l'appareil sur lequel l'événement s'est produit */
    LEFT(CAST(((`h`.`nIp`) & 255) AS CHAR), 4)
  )  AS `strIp`
FROM `v_akpub_ev_event`  AS `e`
  INNER JOIN  `v_akpub_host`  AS `h` ON `h`.`nId` = `e`.`nHostId`
WHERE `e`.`tmRiseTime` >= ADDDATE( UTC_TIMESTAMP( ) , INTERVAL -7  DAY)
ORDER BY `e`.`tmRiseTime` DESC ;
```

Consultation du nom de la base de données de Kaspersky Security Center

Il peut être utile de connaître le nom de la base de données si vous avez besoin, par exemple, d'envoyer une requête SQL et de vous connecter à la base de données depuis votre éditeur de script SQL.

Pour consulter le nom de la base de données de Kaspersky Security Center, procédez comme suit :

1. Dans l'arborescence de la console de Kaspersky Security Center, ouvrez le menu contextuel du dossier **Serveur d'administration**, puis sélectionnez **Propriétés**.

2. Dans la fenêtre des propriétés du Serveur d'administration, dans le volet Sections, sélectionnez **Avancé**, puis **Détails sur la base de données utilisée**.

3. Dans la section **Détails sur la base de données utilisée**, notez les propriétés de base de données suivantes (voir figure ci-dessous) :

- **Nom d'instance**

  Nom d'instance de base de données de Kaspersky Security Center utilisée. La valeur par défaut est *.\KAV_CS_ADMIN_KIT*.

- **Nom de la base de données**

  Nom de la base de données SQL de Kaspersky Security Center. La valeur par défaut est égale à *KAV*.

- **Espace alloué à la base de données de Kaspersky Security Center**

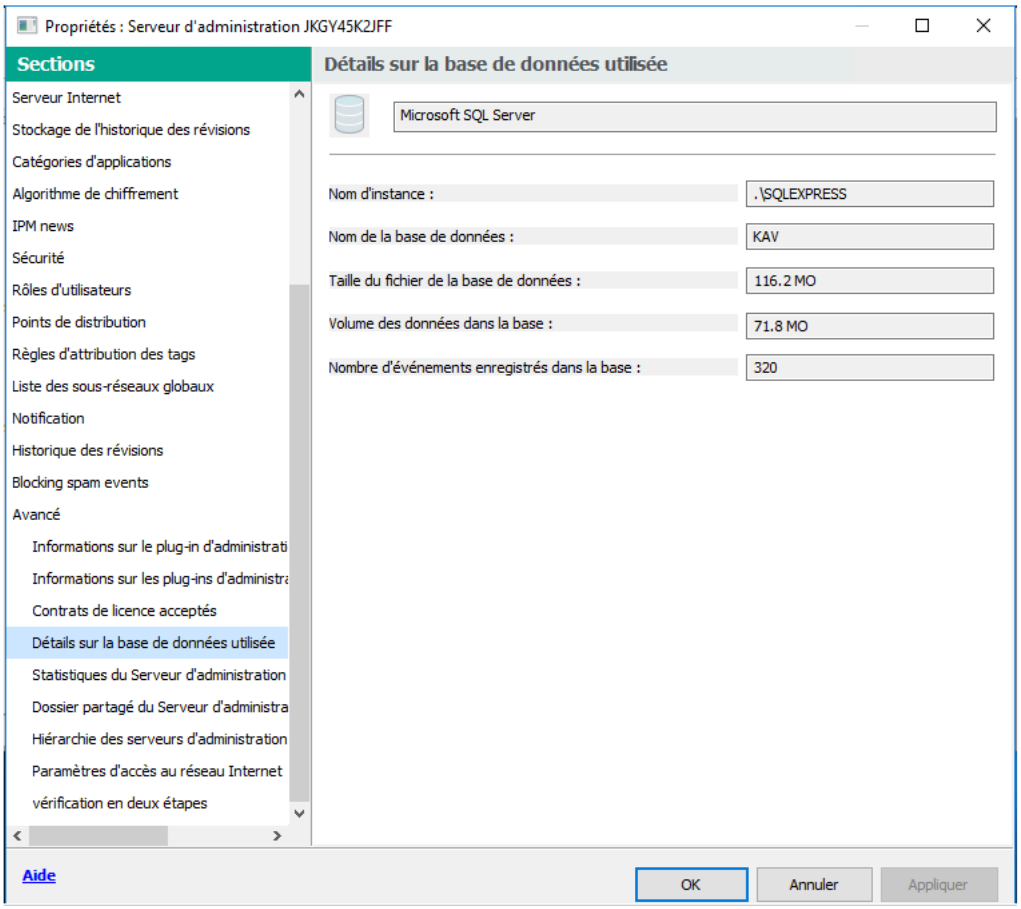
  La taille du fichier de base de données. Si vous souhaitez nettoyer les données inutiles, configurez la compression de la base de données à l'aide de la tâche *Maintenance du Serveur d'administration*.

- **Taille des données dans l'ensemble de la base de données**

  La taille réelle des données actuellement utilisées dans le SGBD. L'article suivant décrit comment diagnostiquer le SGBD : la taille de la base de données dépasse la limite.

- **Nombre d'événements enregistrés dans la base**

Le nombre d'événements actuellement stockés dans le SGBD. Reportez-vous à l'article suivant pour plus de détails : Traitement et stockage des événements.



Section Informations relatives à la base de données utilisée du Serveur d'administration

4. Cliquez sur **OK** pour fermer la fenêtre des propriétés du Serveur d'administration.

Utilisez ce nom de base de données pour vous connecter à la base de données et pour l'invoquer dans vos requêtes SQL.

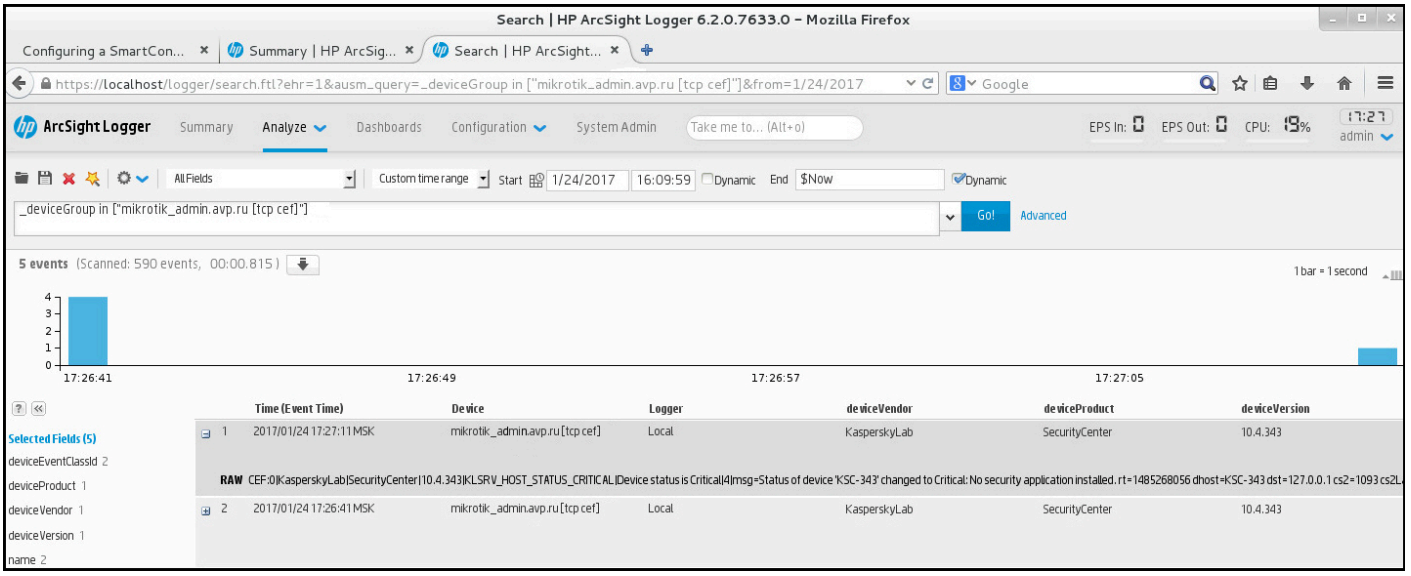
Consultation des résultats de l'exportation

Vous pouvez voir si l'exportation a réussi. Pour cela, vérifiez si le système SIEM a reçu les messages contenant les événements à exporter.

Si les événements envoyés par Kaspersky Security Center ont été reçus et correctement interprétés par le système SIEM, cela signifie que la configuration des deux côtés est correcte. Dans le cas contraire, vérifiez et le cas échéant, modifiez les paramètres de Kaspersky Security Center et du système SIEM.

Vous trouverez ci-après un exemple d'événements exportés dans le système ArcSight. Par exemple, le premier événement est un événement critique du Serveur d'administration : " *État de l'appareil Critique* ".

L'affichage des événements exportés varie en fonction du système SIEM utilisé.



Exemple d'événements

Utilisation du service SNMP pour envoyer des statistiques à des applications tierces

Cette section explique comment obtenir des informations à partir du Serveur d'administration en utilisant Simple Network Management Protocol (SNMP) sous Windows. Kaspersky Security Center contient un agent SNMP qui transfère les statistiques des performances du Serveur d'administration aux applications auxiliaire à l'aide d'identificateurs d'objet (OID).

Cette section contient également des informations sur la résolution des problèmes que vous êtes susceptibles de rencontrer lors de l'utilisation de SNMP pour Kaspersky Security Center.

Configuration du service SNMP à utiliser avec Kaspersky Security Center

Cette section décrit comment configurer le service SNMP sous Windows pour obtenir des informations du Serveur d'administration à l'aide du Protocole SNMP (Simple Network Management Protocol).

La prise en charge de SNMP est désactivée par défaut sous Windows.

Pour activer la prise en charge de SNMP dans Windows :

1. Accédez au **Panneau de configuration**.
2. Ouvrez le menu **Ajouter ou supprimer des programmes**.
3. Cliquez sur **Activer ou désactiver les fonctionnalités Windows**.
4. Dans la liste des fonctionnalités Windows, accédez à la fonctionnalité SNMP, puis cliquez sur **OK**.

5. Accédez à **Panneau de configuration** → **Outils d'administration** → **Services**.

6. Choisissez le **service SNMP** et exécutez-le.

7. Assurez-vous que l'écoute fonctionne en le testant avec `netstat` pour un port UDP standard.

La prise en charge SNMP est activée sous Windows.

Pour configurer les services SNMP sous Windows, procédez comme suit :

1. Assurez-vous que le module **Agent SNMP** de Kaspersky Security Center a été installé dans le cadre de l'installation régulière ou silencieuse.

2. Assurez-vous que les services **Service SNMP** et **Interruption SNMP** de Windows fonctionnent.

3. Assurez-vous que le navigateur ManageEngine MIB est installé sur votre système.

4. Dans les propriétés du **service SNMP**, sous l'onglet **Sécurité**, ajoutez deux communautés avec les privilèges suivants :

Communauté	Privilèges
`kaspersky`	`NOTIFY`
`public`	`READ WRITE`

5. Dans le champ **Accepter les paquets SNMP provenant de ces hôtes**, ajoutez l'adresse IP de l'appareil sur lequel le navigateur ManageEngine MIB est installé, par exemple, 10.10.10.105.

6. Sous l'onglet **Interruptions**, saisissez `kaspersky` dans le champ **Nom de la communauté**.

7. Cliquez sur le bouton **OK** pour enregistrer les modifications et fermer la fenêtre des propriétés de la stratégie.

8. Dans le navigateur ManageEngine MIB, chargez le fichier adminkit.mib depuis le dossier d'installation de Kaspersky Security Center. Par défaut, le fichier adminkit.mib se trouve dans le dossier <Disk>:\Program Files\Kaspersky Lab\Kaspersky Security Center\snmp.

9. Dans le champ **Hôte** de la fenêtre du navigateur ManageEngine MIB, ajoutez l'adresse IP de l'appareil sur lequel le Serveur d'administration de Kaspersky Security Center est installé.

Le service SNMP est configuré pour obtenir des informations du Serveur d'administration à l'aide du Protocole SNMP (Simple Network Management Protocol).

Agent SNMP et identificateurs d'objets

Pour Kaspersky Security Center, l'agent SNMP est mise en œuvre en tant que bibliothèque dynamique `klsnmpag.dll` enregistrée par le programme d'installation lors de l'installation du Serveur d'administration. Le fonctionnement de agent SNMP s'inscrit dans le cadre du processus `snmp.exe` (qui est un service Windows). Des applications tierces utilisent SNMP pour recevoir des statistiques, qui se présentent sous la forme de compteurs, sur les performances du Serveur d'administration.

Chaque compteur a un *identificateur d'objet* unique (également appelé OID). Un identificateur d'objet est une séquence numérique divisée par des points. Les identificateurs d'objet du Serveur d'administration commencent par le préfixe 1.3.6.1.4.1.23668.1093. L'OID du compteur est une concaténation de ce préfixe et d'un suffixe correspondant au compteur. Par exemple, le compteur avec la valeur OID de 1.3.6.1.4.1.23668.1093.1.1.4 a le suffixe avec la valeur de 1.1.4.

Vous pouvez utiliser un client SNMP (tel que Zabbix) pour surveiller l'état de votre système. Afin d'obtenir les informations, vous pouvez rechercher une valeur d'OID correspondant aux informations et saisir cette valeur dans votre client SNMP. Ensuite, votre client SNMP vous renverra une autre valeur qui caractérise l'état de votre système.

La liste des compteurs et des types de compteurs se trouve dans le fichier `adminkit.mib` sur le Serveur d'administration. *MIB* est l'acronyme de « Management Information Base », qui signifie base d'informations de gestion. Vous pouvez importer et analyser des fichiers `.mib` au moyen de l'application MIB Viewer qui est conçue pour demander et afficher les valeurs de compteur.

Obtention d'un nom de compteur de chaîne à partir d'un identificateur d'objet

Afin d'utiliser un identificateur d'objet (OID) pour transférer des informations vers des applications tierces, vous devrez peut-être obtenir un nom de compteur de chaîne à partir de cet OID.

Pour obtenir un nom de compteur de chaîne à partir d'un OID :

1. Ouvrez le fichier `adminkit.mib`, qui se trouve sur le Serveur d'administration, dans un éditeur de texte.

2. Localisez l'espace de noms décrivant la première valeur (de gauche à droite).

   Par exemple, pour le suffixe OID 1.1.4, il s'agirait de `"counters" (::= { kladminkit 1 })`.

3. Localisez l'espace de noms décrivant la deuxième valeur.

   Par exemple, pour le suffixe OID 1.1.4, il s'agirait de `counters 1`, qui signifie `deployment`.

4. Localisez l'espace de noms décrivant la troisième valeur.

   Par exemple, pour le suffixe OID 1.1.4, il s'agirait du `deployment 4`, qui signifie `hostsWithAntivirus`.

Le nom du compteur de chaîne est la concaténation de ces valeurs, par exemple, `<MIB base namespace>.counters.deployment.hostsWithAntivirus`, et correspond à l'OID dont la valeur est 1.3.6.1.4.1.23668.1093.1.1.4.

Valeurs des identificateurs d'objet pour SNMP

Dans le tableau ci-dessous figurent les valeurs et descriptions des identificateurs d'objet (également connu sous le nom de d'OID), utilisés pour transférer des informations sur les performances du Serveur d'administration vers des applications tierces.

Valeurs et descriptions des identificateurs d'objet pour SNMP

Valeur de l'identificateur d'objet	Type de données numériques	OID	Description
`deploymentStatus`	`INTEGER { ok(0), info(1), warning(2), critical(3) }`	.1.3.6.1.4.1.23668.1093.1.1.1	État du déploiement. L'état peut correspondre à l'un des cas de figure ci-après : • **Information**. La licence n'est plus valide pour N appareils. • **Avertissement**. Une des licences suivantes : Les applications Kaspersky sont installées sur M appareils sur un total de N appareils des groupes du Serveur d'administration (N > M). La licence L expire pour N appareils dans M jours. La tâche T d'installation des applications a été effectuée avec succès pour N appareils et un redémarrage est nécessaire pour les M appareils. • **Critique**. Licence expirée pour N appareils. • **OK**. Aucune de ces réponses.
`noAntivirusSoftware`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.1.2.1	Le motif `deploymentStatus` indique que, dans le groupe du Serveur d'administration, trop d'appareils sont dépourvus d'applications administrées. La valeur est égale à 1 lorsqu'il apparaît que quelques appareils ne comportent pas d'application administrée et à 0 dans le cas contraire.
`remoteInstallTaskFailed`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.1.2.2	Le motif `deploymentStatus` indique que la tâche d'installation à distance a échoué pour certains appareils. Le nombre de ces appareils peut être obtenu par `hostsRemoteInstallFailed`.
`licenceExpiring`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.1.2.3	Le motif `deploymentStatus` indique que la licence pour certains appareils a expiré au cours des 7 jours suivants. Le nombre de ces appareils peut être obtenu via `hostsLicenseExpiring`.
`licenceExpired`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.1.2.4	Le motif `deploymentStatus` indique que la licence a expiré pour certains appareils. Vous pouvez obtenir le nombre de ces appareils via `hostsLicenseExpired`.
`hostsInGroups`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.1.3	Nombre d'appareils dans les groupes du Serveur d'administration.
`hostsWithAntivirus`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.1.4	Nombre d'appareils dans les groupes de Serveur d'administration avec des applications administrées installées
`hostsRemoteInstallFailed`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.1.5	Nombre d'appareils pour lesquels la tâche de l'installation à distance a échoué.
`licenceExpiringSerial`	`OCTET STRING`	.1.3.6.1.4.1.23668.1093.1.1.6	ID d'une clé de licence qui expire bientôt (dans moins de 7 jours).
`licenceExpiredSerial`	`OCTET STRING`	.1.3.6.1.4.1.23668.1093.1.1.7	ID de la clé de licence expirée.
`licenceExpiringDays`	`Unsigned32`	.1.3.6.1.4.1.23668.1093.1.1.8	Nombre de jours restants avant l'expiration de la licence. Pour ce paramètre, la licence est considérée comme expirée s'il reste moins de 7 jours avant son expiration. S'il reste plus de 7 jours avant la date d'expiration, la valeur est 0.
`hostsLicenceExpiring`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.1.9	Nombre d'appareils dont la licence expire bientôt (dans moins de 7 jours).
`hostsLicenceExpired`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.1.10	Nombre d'appareils dont la licence a expiré.

Valeur de l'identificateur d'objet	Type de données numériques	OID	Description
updatesStatus	INTEGER { ok(0), info(1), warning(2), critical(3) }	.1.3.6.1.4.1.23668.1093.1.2.1	État actuel de la mise à jour des bases antivirus. L'état peut correspondre à l'un des cas de figure ci-après : • **Information**. Les bases antivirus sur le Serveur d'administration ou sur les appareils n'ont pas été mises à jour depuis plus d'un jour et moins d'un jour s'est écoulé depuis l'installation de l'application. • **Avertissement**. Les bases antivirus sur le Serveur d'administration ou sur les appareils n'ont pas été mises à jour depuis plus de trois jours. Cette valeur peut être modifiée dans les paramètres du groupe. • **Critique**. Les bases antivirus sur le Serveur d'administration ou sur les appareils n'ont pas été mises à jour depuis plus de sept jours. Cette valeur peut être modifiée dans les paramètres du groupe. • **OK**. Aucune de ces réponses.
serverNotUpdated	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.2.2.1	Ce motif indique que le Serveur d'administration n'a pas été mis à jour pour une heure d'entrée au journal. La période considérée comme longue est spécifiée dans updatesStatus.
notUpdatedHosts	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.2.2.2	Cette raison montre que certains appareils n'ont pas été mis à jour pendant une longue période (par défaut, 7 jours ou plus pour **Critique** et 3 jours pour **Avertissement**). Vous pouvez obtenir le nombre de ces appareils via hostsNotUpdated.
lastServerUpdateTime	OCTET STRING	.1.3.6.1.4.1.23668.1093.1.2.3	Mise à jour la plus récente des bases antivirus sur le Serveur d'administration.
hostsNotUpdated	Counter32	.1.3.6.1.4.1.23668.1093.1.2.4	Nombre d'appareils contenant des bases antivirus qui ne sont pas mises à jour depuis longtemps (par défaut, 7 jours ou plus pour **Critique** et 3 jours pour **Avertissement**). S'il existe des appareils avec l'état de mise à jour **Critique**, seuls ces appareils sont comptabilisés. Vous pouvez obtenir l'état de la mise à jour via updatesStatus.
protectionStatus	INTEGER { ok(0), warning(2), critical(3) }	.1.3.6.1.4.1.23668.1093.1.3.1	État de la protection en temps réel. Une des licences suivantes : • **Avertissement**. Une des licences suivantes : une faille de sécurité est détectée sur un appareil appartenant au groupe de Serveur d'administration. Des erreurs de chiffrement ont conduit certains appareils à modifier l'état de la protection. Une analyse complète n'a pas été effectuée depuis longtemps. • **Critique**. La protection antivirus ne fonctionne pas sur certains appareils des groupes de Serveur d'administration. • **OK**. Aucune de ces réponses.
antivirusNotRunning	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.1	Ce motif indique que l'application de sécurité ne fonctionne pas sur certains appareils. Vous pouvez obtenir le nombre de ces appareils via hostsAntivirusNotRunning.
realtimeNotRunning	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.2	Ce motif indique que la protection en temps réel ne fonctionne pas sur certains appareils. Vous pouvez obtenir le nombre de ces appareils via hostsRealtimeNotRunning.
notCuredFound	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.4	Ce motif indique que certains appareils contiennent des objets qui n'ont pas pu être désinfectés. Vous pouvez obtenir le nombre de ces appareils via hostsNotCuredObject.
tooManyThreats	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.5	Ce motif indique que des menaces sont détectées sur certains appareils. Vous pouvez obtenir le nombre de ces appareils via hostsTooManyThreats.

Valeur de l'identificateur d'objet	Type de données numériques	OID	Description
virusOutbreak	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.6	Ce motif indique l'état d'épidémie virale du système. La valeur est égale à 1 si une certaine quantité de virus a été détectée pendant un certain temps, et à 0 dans le cas contraire. La quantité de virus et la durée sont spécifiées sur le Serveur d'administration, en utilisant les paramètres d'Virus attack.
hostsAntivirusNotRunning	Counter32	.1.3.6.1.4.1.23668.1093.1.3.3	Nombre d'appareils dont les applications de sécurité ne fonctionnent pas.
hostsRealtimeNotRunning	Counter32	.1.3.6.1.4.1.23668.1093.1.3.4	Nombre d'appareils pour lesquels la protection en temps réel ne fonctionne pas.
hostsRealtimeLevelChanged	Counter32	.1.3.6.1.4.1.23668.1093.1.3.5	Le nombre d'appareils dont le niveau de protection en temps réel n'est pas acceptable.
hostsNotCuredObject	Counter32	.1.3.6.1.4.1.23668.1093.1.3.6	Nombre d'appareils contenant des objets non désinfectés.
hostsTooManyThreats	Counter32	.1.3.6.1.4.1.23668.1093.1.3.7	Nombre d'appareils contenant des menaces.
fullscanStatus	INTEGER { ok(0), info(1), warning(2), critical(3) }	.1.3.6.1.4.1.23668.1093.1.4.1	État de l'analyse complète de l'antivirus. Une des licences suivantes : • **Information**. Moins de 7 jours se sont écoulés depuis le moment où l'application a été installée. • **Avertissement**. L'analyse complète de l'antivirus n'a pas été effectuée depuis plus de 7 jours à compter du moment de l'installation de l'application. • **Critique**. L'analyse complète de l'antivirus n'a pas été effectuée depuis plus de 14 jours à compter du moment de l'installation de l'application. • **OK**. Aucune de ces réponses.
notScannedLately	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.4.2.1	Ce motif indique que certains appareils n'ont pas été analysés depuis un certain temps. Vous pouvez obtenir le nombre de ces appareils via hostsNotScannedLately. La durée est spécifiée dans fullScanStatus.
hostsNotScannedLately	Counter32	.1.3.6.1.4.1.23668.1093.1.4.3	Nombre d'appareils qui n'ont pas été analysés depuis un certain temps. La durée est spécifiée dans fullScanStatus.
logicalNetworkStatus	INTEGER { ok(0), warning(1), critical(2) }	.1.3.6.1.4.1.23668.1093.1.5.1	État du réseau logique du Serveur d'administration. Une des licences suivantes : • **Avertissement**. S'il existe des appareils inaccessibles dont l'état est « avertissement » qui ne sont pas accessibles ou lorsque des appareils n'appartiennent à aucun groupe du Serveur d'administration. • **Critique**. Lorsqu'il existe des appareils dont le Serveur d'administration a perdu le contrôle, ou des hôtes dont l'état est critique qui ne sont pas accessibles. • **OK**. Aucune de ces réponses.
notConnectedLongTime	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.5.2.1	Ce motif indique que certains appareils ne sont pas connectés au Serveur d'administration depuis longtemps (7 jours ou plus pour un appareil dont l'état est **Avertissement** et 4 jours pour un appareil dont l'état est **Critique**). Vous pouvez obtenir le nombre de ces appareils via hostsNotConnectedLongTime.
controlLost	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.5.2.2	Ce motif indique qu'il existe des appareils dont le Serveur d'administration a perdu le contrôle. Vous pouvez obtenir le nombre de ces appareils via hostsControlLost.
hostsFound	Counter32	.1.3.6.1.4.1.23668.1093.1.5.3	Nombre d'appareils détectés par le Serveur d'administration qui n'appartiennent à aucun groupe de Serveur d'administration.
groupsCount	Counter32	.1.3.6.1.4.1.23668.1093.1.5.4	Nombre de groupes sur le Serveur d'administration.

Valeur de l'identificateur d'objet	Type de données numériques	OID	Description
`hostsNotConnectedLongTime`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.5.5	Nombre d'appareils qui n'ont pas été connectés au Serveur d'administration depuis longtemps. La période considérée comme longue est spécifiée dans `notConnectedLongTime`.
`hostsControlLost`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.5.6	Nombre d'appareils qui ne sont pas contrôlés par le Serveur d'administration.
`eventsStatus`	`INTEGER { ok(0), warning(1), critical(2) }`	.1.3.6.1.4.1.23668.1093.1.6.1	État du sous-système événements. Une des licences suivantes : • **Avertissement**. Une des licences suivantes : Les appareils du groupe du Serveur d'administration n'ont pas recherché de mises à jour Windows depuis longtemps. Il existe des appareils présentant des problèmes d'état. • **Critique**. Une des licences suivantes : un événement d'importance « Critique » est survenu sur au moins un appareil. Un événement considéré comme une « Erreur » est survenu sur au moins un appareil. Un événement constituant un « échec de l'exécution de la tâche » est survenu sur au moins un appareil. Les appareils du groupe du Serveur d'administration n'ont pas recherché de mises à jour Windows depuis longtemps. Il existe des appareils présentant des problèmes d'état. • **OK**. Aucune de ces réponses.
`criticalEventOccured`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.6.2.1	Le motif `eventsStatus` indique que des événements critiques sont survenus sur le Serveur d'administration. Vous pouvez obtenir le nombre de ces événements via `criticalEventsCount`. La valeur est égale à 1 lorsqu'au moins un événement critique est survenu sur un appareil, quel qu'il soit, et à 0 dans le cas contraire.
`criticalEventsCount`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.6.3	Nombre d'événements critiques sur le Serveur d'administration.

Elimination des défaillances

Dans cette section, vous trouverez des solutions à quelques problèmes typiques que vous pourriez rencontrer lors de l'utilisation du service SNMP.

Une application tierce ne peut pas se connecter au service SNMP

Assurez-vous que le service SNMP est installé et configuré comme décrit dans la section Configuration du service SNMP pour une utilisation avec Kaspersky Security Center.

Le service SNMP fonctionne mais l'application tierce ne peut pas obtenir de valeur.

Autorisez le traçage de l'agent SNMP et assurez-vous qu'un fichier non vide est créé. Cela signifie que l'agent SNMP est correctement enregistré et qu'il fonctionne. Après cela, autorisez les connexions à partir du service SNMP dans les paramètres de service secondaires. Si un service auxiliaire fonctionne sur le même hôte que l'agent SNMP, la liste des adresses IP doit contenir soit l'adresse IP de cet hôte, soit le `loopback 127.0.0.1`.

Un service SNMP qui communique avec les agents doit être exécuté sous Windows. Vous pouvez spécifier les chemins d'accès aux agents SNMP dans le registre Windows par le biais de regedit.

- Pour Windows 10 :
  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\ExtensionAgents
- Pour Windows Vista et Windows Server 2008 :
  HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SNMP\Parameters\ExtensionAgents

Vous pouvez également autoriser le traçage d'agent SNMP via regedit.

- Pour les systèmes 32 bits :
  HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1093\1.0.0.0\SNMP\Debug
- Pour les systèmes 64 bits :
  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1093\1.0.0.0\SNMP\Deb
  "TraceLevel"=dword:00000004
  "TraceDir"="C:\\"

Les valeurs ne correspondent pas aux états de la Console d'administration

Afin de réduire la charge sur le Serveur d'administration, la mise en cache des valeurs est mise en oeuvre pour l'agent SNMP. La latence entre l'actualisation de la mémoire cache en cours d'actualisation et la modification des valeurs sur le Serveur d'administration peut entraîner des incohérences entre les valeurs renvoyées par l'agent SNMP et les valeurs réelles. Lorsque vous travaillez avec des applications tierces, vous devez tenir compte de cette latence possible.

Fonctionnement dans le Cloud

Cette section fournit des informations relatives au déploiement et à la maintenance de Kaspersky Security Center dans les Clouds comme Amazon Web Services, Microsoft Azure et Google Cloud.

Les adresses des pages Web citées dans ce document sont correctes à la date de publication de Kaspersky Security Center.

La fonctionnalité de mises à jour (y compris la fourniture de mises à jour des signatures antivirus et des bases de code), ainsi que la fonctionnalité KSN peuvent ne pas être disponibles dans le logiciel aux États-Unis.

À propos de l'utilisation dans le Cloud

Kaspersky Security Center 15.1 fonctionne uniquement avec les appareils physiques, mais il possède également des fonctionnalités spéciales pour travailler dans le Cloud. Kaspersky Security Center fonctionne avec les machines virtuelles suivantes :

- Instances Amazon EC2 (ci-après également appelées *instances*). Une instance Amazon EC2 est une machine virtuelle créée sur la base de la plateforme Amazon Web Services (AWS). Kaspersky Security Center utilise l'*API* AWS (Application Programming Interface).
- Machines virtuelles Microsoft Azure. Kaspersky Security Center utilise l'API Azure.
- Instances de machines virtuelles Google Cloud. Kaspersky Security Center utilise l'API Google.

Vous pouvez déployer Kaspersky Security Center sur une instance ou sur une machine virtuelle pour administrer la protection des appareils dans le Cloud et exploiter les fonctions spéciales de Kaspersky Security Center pour travailler dans le Cloud. Parmi ces fonctionnalités, citons :

- Sondage des Appareil dans le Cloud à l'aide des outils de l'API
- Utilisation des outils de l'API pour installer l'Agent d'administration et les applications de sécurité sur les appareils dans le Cloud
- La recherche de Appareil fonction de l'appartenance à un segment dans le Cloud déterminé

Vous pouvez aussi utiliser une instance ou une machine virtuelle dotée du Serveur d'administration de Kaspersky Security Center pour protéger les appareils physiques (par exemple, si un serveur Cloud s'avère plus pratique pour vous au niveau de la maintenance et du contenu qu'un serveur physique). Dans ce cas, l'utilisation du Serveur d'administration est identique au cas de figure où le Serveur d'administration serait installé sur un appareil sur site.

Dans une version de Kaspersky Security Center déployée depuis une image machine Amazon (AMI) payée (dans AWS) ou depuis un SKU (dans Azure) facturé mensuellement en fonction de l'utilisation (dans Azure), la Gestion des vulnérabilités et des correctifs (y compris l'intégration aux systèmes SIEM) est activée automatiquement il est impossible d'activer l'administration des appareils mobiles.

Le Serveur d'administration est installé avec la Console d'administration. Kaspersky Security for Windows Server est également installé automatiquement sur l'appareil sur lequel le Serveur d'administration est installé.

Vous pouvez configurer Kaspersky Security Center à l'aide de l'Assistant de configuration pour une utilisation dans le Cloud, en tenant compte des particularités du travail dans le Cloud.

Scénario : déploiement pour une utilisation dans le Cloud

Cette section présente le déploiement de Kaspersky Security Center en vue d'une utilisation dans un cloud, comme Amazon Web Services, Microsoft Azure et Google Cloud.

Après l'exécution du scénario de déploiement, le Serveur d'administration de Kaspersky Security Center et la Console d'administration sont lancés et configurés avec les paramètres par défaut. La protection antivirus administrée par Kaspersky Security Center est déployée sur les instances Amazon EC2 ou les machines virtuelles Microsoft Azure sélectionnées. Ensuite, vous pouvez configurer Kaspersky Security Center de manière plus précise, créer une structure complexe de groupes d'administration, créer pour les groupes diverses stratégies et tâches.

Le déploiement de Kaspersky Security Center pour une utilisation dans un environnement Cloud comprend les étapes suivantes :

1. Préparatifs
2. Déploiement du Serveur d'administration
3. Installation des applications antivirus de Kaspersky sur les appareils virtuels à protéger
4. Configuration des paramètres de téléchargement des mises à jour
5. Configuration des paramètres pour l'administration des rapports sur l'état de la protection des appareils

L'Assistant de configuration pour une utilisation dans le Cloud est destiné à effectuer la configuration initiale. Il démarre automatiquement la première fois que Kaspersky Security Center est déployé à partir d'une image prête à l'emploi. Vous pouvez lancer l'Assistant manuellement à tout moment. De plus, vous pouvez effectuer manuellement toutes les actions qu'il effectue.

Il est recommandé de consacrer au moins une heure au déploiement du Serveur d'administration de Kaspersky Security Center dans le Cloud et au moins une journée de travail en tout au déploiement de la protection dans le Cloud.

Le déploiement de Kaspersky Security Center dans le Cloud suit les étapes suivantes :

1. **Planification de la configuration des segments dans le Cloud**

   Découvrez le fonctionnement de Kaspersky Security Center dans un environnement Cloud. Planifiez l'emplacement de déploiement du Serveur d'administration (dans le Cloud ou hors du Cloud). Définissez également le nombre de segments dans le Cloud que vous souhaitez protéger. Si vous avez l'intention d'installer le Serveur d'administration hors du Cloud, ou si vous avez l'intention de protéger plus de 5000 appareils, vous devrez installer manuellement le Serveur d'administration.

   Pour travailler avec Google Cloud, vous pouvez uniquement installer le Serveur d'administration manuellement.

2. **Planification des ressources**

   Vérifiez que vous avez tout ce qui est nécessaire pour le déploiement.

3. **Abonnement à Kaspersky Security Center sous la forme d'une image prête**

   Sélectionnez une des AMI prêtes à l'emploi dans AWS Marketplace ou sélectionnez un SKU facturé mensuellement en fonction de l'utilisation dans la place de marché Azure, réalisez le paiement conformément aux règles de la place de marché, le cas échéant (ou utilisez le modèle BYOL), et utilisez l'image pour déployer une instance Amazon EC2 ou une machine virtuelle Microsoft Azure avec l'instance de Kaspersky Security Center installée.

   Cette étape est requise si vous avez l'intention de déployer le Serveur d'administration sur une instance ou une machine virtuelle dans le Cloud et si vous allez également déployer la protection sur un maximum de 5000 appareils. Dans le cas contraire, cette étape n'est pas requise et vous devez installer vous-même le Serveur d'administration, la Console d'administration et le SGBD.

   Cette étape n'est pas disponible pour Google Cloud.

4. **Définition de l'emplacement du SGBD**

   Déterminez l'emplacement de votre SGBD.

   Si vous comptez utiliser une base de données hors du Cloud, assurez que vous disposez d'une base de données fonctionnelle.

   Si vous prévoyez d'utiliser Amazon Relational Database Service (RDS), créez une base de données avec RDS dans le cloud AWS.

   Si vous prévoyez d'utiliser le SGBD Microsoft Azure SQL, créez une base de données avec le service Azure Database dans le cloud Microsoft Azure.

   Si vous prévoyez d'utiliser Google MySQL, créez une base de données dans Google Cloud (veuillez consulter https://cloud.google.com/sql/docs/mysql pour plus de détails).

5. **Installation manuelle du Serveur d'administration et de la Console d'administration (basée sur MMC et/ou sur le Web) des appareils sélectionnés**

   Installez le Serveur d'administration, la Console d'administration et le SGBD sur les appareils sélectionnés comme décrit dans le scénario principal d'installation de Kaspersky Security Center.

   Cette étape est nécessaire si vous avez l'intention de placer le Serveur d'administration hors du Cloud ou si vous avez l'intention de déployer la protection sur plus de 5000 appareils. Assurez-vous ensuite que votre Serveur d'administration est conforme à la configuration matérielle requise. Dans le cas contraire, cette étape n'est pas requise et il suffit d'un abonnement à Kaspersky Security Center sous la forme d'une image prête à l'emploi dans AWS Marketplace, la Place de marché Azure ou Google Cloud.

6. **Garantie des privilèges pour le fonctionnement du Serveur d'administration avec les API du Cloud**

   Dans AWS, accédez à la console de gestion AWS et créez un rôle IAM ou un compte utilisateur IAM. Le rôle IAM (ou le compte utilisateur IAM) créé permet à Kaspersky Security Center d'utiliser AWS API : sondage des segments dans le Cloud et déploiement de la protection.

   Dans Azure, créez un abonnement et un ID de l'application avec mot de passe. Kaspersky Security Center utilise ces identifiants pour fonctionner avec Azure API : sondage des segments dans le Cloud et déploiement de la protection.

   Dans Google Cloud, enregistrez un projet, obtenez votre ID de projet et une clé privée. Kaspersky Security Center utilise ces informations d'identification pour interroger les segments dans le Cloud à l'aide de l'API de Google.

7. **Création d'un rôle IAM pour les instances protégées (pour AWS uniquement).**

   Vous créez dans la console de gestion AWS le rôle IAM qui définit l'ensemble des permissions pour l'exécution des requêtes adressées à AWS. Le rôle créé sera ensuite attribué aux nouvelles instances. Le rôle IAM est nécessaire pour l'installation des applications sur les instances à l'aide de Kaspersky Security Center.

8. **Préparation d'une base de données à l'aide d'Amazon Relational Database Service (RDS) ou de Microsoft Azure SQL**

   Si vous avez l'intention d'utiliser une base de données Amazon Relational Database Service (RDS), créez une instance de base de données Amazon RDS et un compartiment S3 pour le stockage de la sauvegarde de la base de données. Vous pouvez ignorer cette étape si vous voulez une base de données sur la même instance EC2 où se trouve le Serveur d'administration ou si vous voulez que votre base de données se trouve ailleurs.

   Si vous avez l'intention d'utiliser Microsoft Azure SQL, créez un compte de stockage et une base de données dans Microsoft Azure.

   Si vous prévoyez d'utiliser Google MySQL, créez une base de données dans Google Cloud. (Veuillez consulter https://cloud.google.com/sql/docs/mysql pour plus de détails).

9. **Obtention d'une licence Kaspersky Security Center pour fonctionner dans le Cloud**

Confirmez que vous avez obtenu une licence de Kaspersky Security Center en vue d'une utilisation dans le Cloud et fourni un code d'activation ou un fichier clé afin que l'application l'ajoute au stockage de licences. Cette étape peut être réalisée dans la configuration de l'environnement cloud.

Cette étape est obligatoire si vous utilisez une version de Kaspersky Security Center installée depuis une image AMI prête à l'emploi et gratuite selon le modèle BYOL ou si vous installez Kaspersky Security Center indépendamment sans utilisation d'images AMI. Dans chacun de ces cas, l'activation de Kaspersky Security Center requiert une licence pour Kaspersky Security for Virtualization ou une licence pour Kaspersky Hybrid Cloud Security.

Cette étape n'est pas nécessaire et la fenêtre correspondante de l'Assistant de configuration pour une utilisation dans le Cloud est inaccessible si vous utilisez Kaspersky Security Center installé à partir d'une image prête à l'emploi.

10. **Autorisation dans le cloud**

    Fournissez à Kaspersky Security Center vos identifiants AWS, Azure ou Google Cloud afin que Kaspersky Security Center puisse fonctionner avec les autorisations nécessaires. Cette étape peut être réalisée lors de l'autorisation dans l'environnement Cloud.

11. **Réception par le Serveur d'administration des informations sur les appareils dans le segment dans le cloud via le sondage du segment dans le cloud**

    Lancez le sondage des segments dans le Cloud. Dans l'environnement AWS, Kaspersky Security Center obtient les adresses et les noms de toutes les instances accessibles sous les privilèges du rôle IAM (ou du compte utilisateur IAM). Dans l'environnement Microsoft Azure, Kaspersky Security Center obtient les adresses et les noms de toutes les machines virtuelles accessibles sous les privilèges du rôle Lecteur.

    Ensuite, vous pouvez installer à l'aide de Kaspersky Security Center des applications de Kaspersky et d'autres éditeurs sur les instances ou les machines virtuelles détectées.

    Kaspersky Security Center lance le sondage régulièrement. Par conséquent, si de nouvelles instances ou machines virtuelles apparaissent, elles seront détectées automatiquement.

12. **Regroupement de tous les appareils du réseau dans le groupe d'administration Cloud**

    Déplacez toutes les instances ou machines virtuelles dans le groupe d'administration **Appareils administrés\Cloud** afin qu'ils puissent être administrés centralement. Si vous voulez répartir les appareils en sous-groupes, par exemple, en fonction de système d'exploitation qui y est installé, vous pouvez créer plusieurs groupes d'administration à l'intérieur du groupe **Appareils administrés\Cloud**. Vous pouvez configurer le déplacement automatique de tous les appareils qui seront détectés pendant les sondages réguliers vers le groupe **Appareils administrés\Cloud**.

13. **Communication des appareils dans le réseau avec le Serveur d'administration à l'aide de l'Agent d'administration**

    Installez l'Agent d'administration sur les appareils dans le Cloud. L'Agent d'administration est le module Kaspersky Security Center qui assure la communication des appareils avec le Serveur d'administration. Les paramètres de l'Agent d'administration sont automatiquement configurés par défaut.

    Vous pouvez installer l'Agent d'administration sur chaque appareil localement. Vous pouvez installer aussi l'Agent d'administration sur les appareils à distance à l'aide de Kaspersky Security Center. Ou vous pouvez sauter cette étape et installer l'Agent d'administration avec les versions les plus récentes des applications de sécurité.

14. **Installation des dernières versions des applications de sécurité sur les appareils du réseau.**

    Choisissez les appareils sur lesquels vous souhaitez installer les applications de sécurité, puis installez les versions les plus récentes de l'application de protection sur ces appareils. Vous pouvez réaliser l'installation à distance, via Kaspersky Security Center sur le Serveur d'administration ou localement.

    Vous devrez peut-être créer manuellement des paquets d'installation pour ces programmes.

    L'application Kaspersky Endpoint Security for Linux est destinée aux instances et aux machines virtuelles tournant sous Linux.

L'application Kaspersky Security for Windows Server est destinée aux instances et aux machines virtuelles tournant sous Windows.

15. **Configuration des paramètres des mises à jour**

La tâche **Recherche de vulnérabilités et de mises à jour requises** est créée automatiquement lorsque vous commencez à configurer l'environnement cloud. Vous pouvez également la créer manuellement. Cette tâche assure la recherche automatique et le téléchargement des mises à jour requises pour les applications en vue d'une installation ultérieure sur les appareils à l'aide de Kaspersky Security Center.

Il est recommandé d'effectuer l'étape suivante une fois la configuration de l'environnement cloud terminée :

1. **Configuration de l'utilisation des rapports**

   Vous pouvez consulter les Rapports sous l'onglet **Surveillance** dans l'espace de travail de l'entrée **Serveur d'administration**. Vous pouvez également recevoir des rapports par email. Par défaut, les rapports sous l'onglet **Surveillance** sont accessibles. Pour configurer la réception des rapports par email, indiquez les adresses email sur lesquelles sont reçus les rapports, puis configurez le format des rapports.

Résultats

À la fin du scénario, vous pouvez vous assurer que la configuration initiale a réussi :

- Vous pouvez vous connecter au Serveur d'administration via la Console d'administration ou via Kaspersky Security Center Web Console.
- Les dernières versions des applications de sécurité de Kaspersky sont installées et s'exécutent sur des appareils administrés.
- Kaspersky Security Center a créé les stratégies et les tâches par défaut pour tous les appareils administrés.

Conditions indispensables pour le déploiement de Kaspersky Security Center our une utilisation dans le Cloud

Avant de déployer le Kaspersky Security Center dans l'environnement du Cloud Amazon Web Services ou Microsoft Azure, vérifiez les éléments suivants :

- Accès Internet
- Un des comptes suivants :
  - Compte Amazon Web Services (pour une utilisation avec AWS)
  - Compte Microsoft (pour une utilisation avec Azure)
  - Compte Google (pour une utilisation avec Google Cloud)

- Une des licences suivantes :
  - Licence pour Kaspersky Security for Virtualization
  - Licence pour Kaspersky Hybrid Cloud Security
  - Fonds destinés à acheter une telle licence (Kaspersky Security for Virtualization ou Kaspersky Hybrid Cloud Security)
  - Fonds pour payer une image prête à l'emploi sur la place de marché Azure
- Manuels pour les versions les plus récentes de Kaspersky Endpoint Security for Linux et Kaspersky Security for Windows Server.

Configuration matérielle requise pour le Serveur d'administration dans le Cloud

Pour le déploiement dans des environnements Cloud, les exigences du Serveur d'administration et du serveur de base de données sont les mêmes que celles du Serveur d'administration physique (en fonction du nombre d'appareils que vous souhaitez administrer). Pour en savoir plus, veuillez consulter la documentation des environnements Cloud.

Options de licence pour le Cloud

L'utilisation dans le cloud ne fait pas partie des fonctions de base de Kaspersky Security Center et requiert dès lors une licence distincte.

Il existe deux options de licence de Kaspersky Security Center pour travailler dans le Cloud :

- AMI payée (dans Amazon Web Services) ou SKU (dans Azure) facturé mensuellement en fonction de l'utilisation (dans Microsoft Azure).

  Cela octroie une licence pour Kaspersky Security Center ainsi que des licences pour Kaspersky Endpoint Security for Linux et Kaspersky Security for Windows Server. Vous devez effectuer le paiement selon les règles de l'environnement Cloud que vous utilisez.

  Ce modèle vous permet d'avoir un maximum de 200 appareils clients par Serveur d'administration.

- Une image gratuite et prête à l'emploi avec une licence exclusive conformément au modèle BYOL (Bring Your Own License).

  Pour être autorisé à utiliser Kaspersky Security Center dans AWS ou Azure, vous devez avoir une licence pour l'une des applications suivantes :

  - Kaspersky Security for Virtualization
  - Kaspersky Hybrid Cloud Security

  Le modèle BYOL permet d'avoir jusqu'à 100 000 appareils clients par Serveur d'administration. Ce modèle permet également d'administrer des appareils hors de l'environnement AWS, Azure ou Google.

  Vous pouvez choisir le modèle BYOL dans les cas suivants :

  - Vous disposez déjà d'une licence valide pour l'application Kaspersky Security for Virtualization.
  - Vous disposez déjà d'une licence valide pour l'application Kaspersky Hybrid Cloud Security.
  - Vous voulez acheter une licence directement avant de déployer Kaspersky Security Center.

  Lors de l'étape de configuration initiale, Kaspersky Security Center vous demande le code d'activation ou le fichier clé.

  Si vous avez choisi l'option BYOL, vous ne devez pas payer l'utilisation de Kaspersky Security Center via la place de marché Azure ou AWS Marketplace.

Dans les deux cas, la Gestion des vulnérabilités et des correctifs est activée automatiquement et l'Administration des appareils mobiles ne peut pas être activée.

Si une erreur se produit lors de la tentative d'activation de la fonctionnalité Prise en charge de l'environnement cloud à l'aide de la licence pour Kaspersky Hybrid Cloud Security, utilisez le fichier clé.

Lorsque vous vous abonnez à Kaspersky Security Center, vous obtenez une instance Amazon Elastic Compute Cloud (Amazon EC2) ou une machine virtuelle Microsoft Azure avec un Serveur d'administration de Kaspersky Security Center. Les paquets d'installation de Kaspersky Security for Windows Server et Kaspersky Endpoint Security for Linux sont disponibles sur le Serveur d'administration. Vous pouvez installer ces applications sur les appareils dans le Cloud. Il n'est pas nécessaire d'avoir une licence pour ces applications.

Si un appareil administré n'est pas visible pour le Serveur d'administration pendant plus d'une semaine, l'application (Kaspersky Security for Windows Server ou Kaspersky Endpoint Security for Linux) sur celle-ci passera au mode limité. Pour activer à nouveau l'application, il faudra à nouveau rendre l'appareil sur lequel elle est installée visible pour le Serveur d'administration.

Options pour les bases de données pour travailler dans le Cloud

L'utilisation de Kaspersky Security Center requiert une base de données. Quand vous déployez Kaspersky Security Center dans AWS, dans Microsoft Azure ou dans Google Cloud, vous avez trois options :

- Créez une base de données locale sur le même appareil doté du Serveur d'administration. Kaspersky Security Center est livré avec une base de données SQL Server Express qui peut prendre en charge d'un maximum de 5 000 appareils administrés. Choisissez cette option si SQL Server Express Edition suffit à vos besoins.

- Créez une base de données à l'aide du Relational Database Service (RDS) dans le Cloud AWS ou via le service de base de données Azure dans le Cloud Microsoft Azure. Sélectionnez cette option si vous souhaitez un SGBD différent de SQL Express. Vos données seront transférées et conservées dans le Cloud et vous n'aurez aucun frais supplémentaires. Si vous travaillez déjà avec Kaspersky Security Center sur site et que vous avez des données dans votre base de données, vous pouvez les transférer vers la nouvelle base de données.

  Sur la plate-forme Google Cloud, vous pouvez utiliser uniquement Cloud SQL pour MySQL.

- Utilisez un serveur de base de données existant. Choisissez cette option si vous avez déjà un serveur de base de données et que vous voulez l'utilisez pour Kaspersky Security Center. Si le serveur est en dehors du Cloud, vos données seront transférées via Internet, ce qui pourrait entraîner des frais supplémentaires.

La procédure de déploiement de Kaspersky Security Center dans le Cloud possède une étape spéciale pour créer (choisir) une base de données.

Utilisation de l'environnement Cloud Amazon Web Services

Cette section explique les préparatifs à suivre pour utiliser Kaspersky Security Center dans Amazon Web Services.

> Les adresses des pages Web citées dans ce document sont correctes à la date de publication de Kaspersky Security Center.

À propos de l'utilisation de l'environnement Cloud d'Amazon Web Services

Vous pouvez acquérir Kaspersky Security Center dans le magasin d'applications AWS Marketplace sous la forme d'une image AMI (image machine Amazon), une image prête d'une machine virtuelle déjà configurée. Vous pouvez vous abonner à une image AMI payée ou à une image AMI selon le principe BYOL et créer sur la base de celle-ci une instance Amazon EC2 dotée du Serveur d'administration de Kaspersky Security Center.

Pour utiliser la plateforme AWS et plus particulièrement, pour pouvoir acheter des apps dans AWS Marketplace et créer des instances, il faut disposer d'un compte utilisateur dans Amazon Web Services. Vous pouvez créer un compte gratuit à l'adresse https://aws.amazon.com. Vous pouvez aussi utiliser un compte utilisateur Amazon existant.

Si vous êtes abonné à une image AMI disponible dans AWS Marketplace, vous recevez l'instance avec une copie de Kaspersky Security Center prête à l'emploi. Vous n'avez pas besoin d'installer l'application indépendamment. Dans ce cas, le Serveur d'administration de Kaspersky Security Center est installé sur l'instance sans votre intervention. Après l'installation, vous pouvez lancer la Console d'administration et vous connecter au Serveur d'administration pour commencer à travailler avec Kaspersky Security Center.

Pour en savoir plus sur les images AMI et sur le fonctionnement de la boutique d'apps AWS Marketplace, consultez la page d'aide d'AWS Marketplace. Pour en savoir plus sur l'utilisation de la plateforme AWS, sur l'utilisation d'instances et sur les notions liées à celles-ci, consultez la documentation d'Amazon Web Services.

Les adresses des pages Web citées dans ce document sont correctes à la date de publication de Kaspersky Security Center.

Création de rôles IAM et de comptes utilisateurs IAM pour les instances Amazon EC2

Cette section décrit les actions à exécuter pour garantir le bon fonctionnement du Serveur d'administration. Ces actions comprennent l'utilisation des rôles IAM (Identity and Access Management) d'AWS et des comptes utilisateurs. Elle décrit également les actions à exécuter sur les appareils clients pour y installer l'Agent d'administration, puis installer Kaspersky Security for Windows Server et Kaspersky Endpoint Security for Linux.

Garantie des privilèges pour le fonctionnement du Serveur d'administration de Kaspersky Security Center avec AWS

Les normes d'utilisation du cloud Amazon Web Services recommandent l'affectation d'un rôle IAM spécial à l'instance du Serveur d'administration pour fonctionner avec les services AWS. Vous créez dans la console AWS le rôle IAM qui définit l'ensemble des permissions pour l'exécution des requêtes adressées aux services AWS. Le rôle IAM garantit les privilèges de sondage des segments dans le Cloud et d'installation d'applications sur les instances.

Après avoir créé un rôle IAM et l'avoir désigné sur un Serveur d'administration, vous pourrez déployer la protection des instances en utilisant ce rôle et sans offrir à Kaspersky Security Center aucune information complémentaire.

Cependant, dans certains cas, il peut être préférable de refuser de créer un rôle IAM pour un Serveur d'administration :

- Si les appareils dont vous avez l'intention d'administrer la protection sont des instances EC2 au sein du Cloud Amazon Web Services et si le Serveur d'administration se trouve hors de celui-ci.
- Si vous envisagez d'administrer la protection des instances non pas seulement à l'intérieur de votre segment dans le Cloud, mais aussi au sein d'autres segments créés sous un autre compte utilisateur dans AWS. Dans ce cas, le rôle IAM est nécessaire uniquement pour protéger votre segment dans le Cloud. La protection d'un autre segment dans le Cloud ne requiert pas un rôle IAM.

Dans de tels cas, il ne faut pas créer un rôle IAM, mais un *compte utilisateur IAM* sous lequel Kaspersky Security Center va utiliser les services AWS. Avant de commencer à utiliser le Serveur d'administration, créez un compte utilisateur IAM avec une *clé d'accès AWS IAM* (par la suite *clé d'accès IAM*).

La création d'un rôle IAM ou d'un compte utilisateur IAM requiert une console de gestion AWS. Pour pouvoir utiliser la console de gestion AWS, il vous faut un nom d'utilisateur et un mot de passe d'un compte utilisateur dans AWS.

Création d'un rôle IAM pour le Serveur d'administration

Avant de déployer le Serveur d'administration, créez dans la console de gestion AWS le rôle IAM disposant privilèges nécessaires à l'installation des applications sur les instances. Pour plus de détails, consultez les sections d'aide AWS sur les rôles IAM.

Pour créer une rôle IAM pour le Serveur d'administration, procédez comme suit :

1. Ouvrez la console de gestion AWS et connectez-vous sous votre compte utilisateur AWS.
2. Dans la section **Rôles**, créez un rôle avec les autorisations suivantes :
   - **AmazonEC2ReadOnlyAccess**, si vous envisagez de lancer seulement le sondage des segments dans le Cloud et que vous n'envisagez pas l'installation d'applications sur les instances EC2 à l'aide de l'API AWS.
   - **AmazonEC2ReadOnlyAccess** et **AmazonSSMFullAccess**, si vous prévoyez de lancer le sondage des segments dans le Cloud et d'installer les applications sur les instances EC2 à l'aide de l'API AWS. Dans ce cas, il faudra désigner également sur les instances EC2 protégées un rôle IAM avec les privilèges AmazonEC2RoleforSSM.

Il faudra désigner ce rôle sur l'instance EC2 que vous allez utiliser en tant que Serveur d'administration.

Le rôle créé est accessible à toutes les applications sur le Serveur d'administration. Pour cette raison, n'importe quelle application qui fonctionne sur le Serveur d'administration doit pouvoir sonder les segments dans le Cloud ou installer des applications sur les instances EC2 à l'intérieur d'un segment dans le Cloud.

Les adresses des pages Web citées dans ce document sont correctes à la date de publication de Kaspersky Security Center.

Création d'un compte utilisateur IAM pour utiliser Kaspersky Security Center

Un compte utilisateur IAM est indispensable à l'utilisation de Kaspersky Security Center quand aucun rôle IAM doté des privilèges de recherche d'appareils et d'installation des applications sur les instances n'a été attribué sur le Serveur d'administration. Le même compte, ou un compte différent, est également requis pour la tâche de création de la copie de sauvegarde des données du Serveur d'administration si vous utilisez un compartiment S3. Vous pouvez créer un compte utilisateur IAM avec toutes les permissions nécessaires ou vous pouvez créer deux comptes utilisateurs séparés.

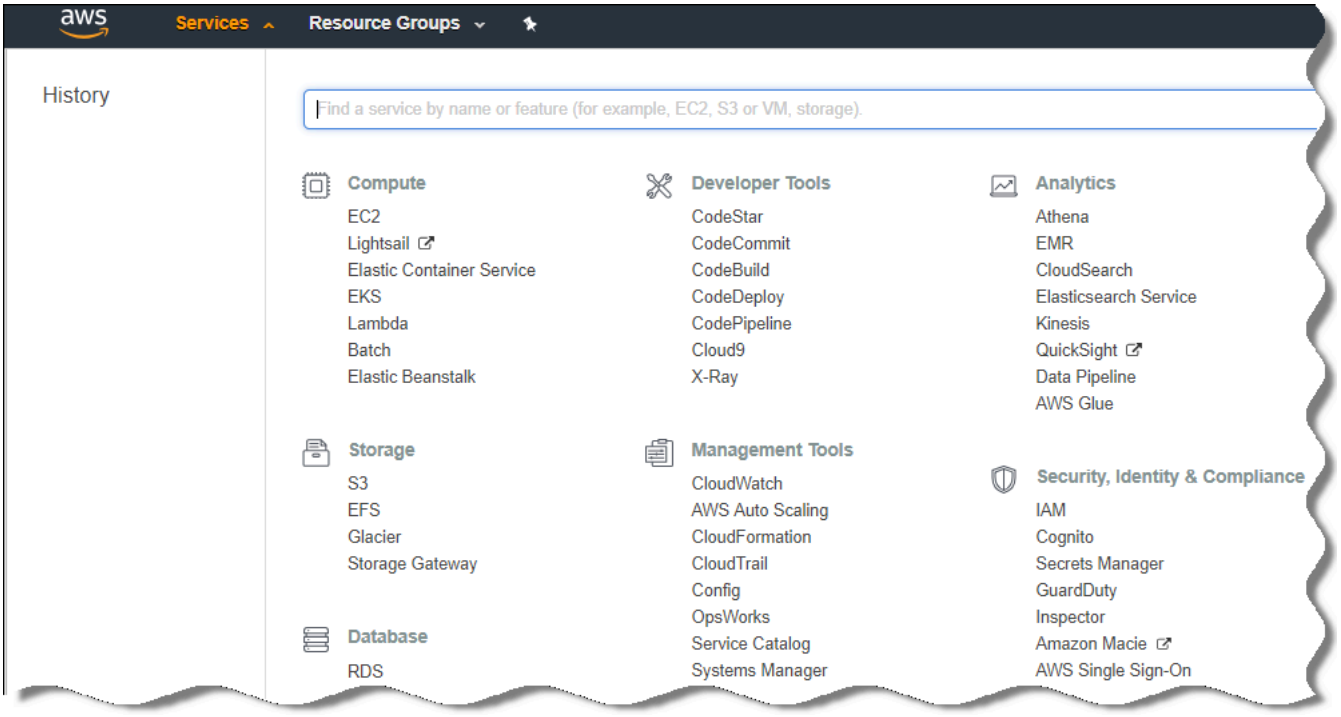
La *clé d'accès IAM* est créée automatiquement pour l'utilisateur IAM. Cette clé doit être présentée à Kaspersky Security Center lors de la configuration initiale. La clé d'accès IAM est composée de l'ID de clé d'accès et de la clé secrète. Pour en savoir plus sur le service IAM, consultez les pages d'aide d'AWS suivantes :

- http://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html.
- http://docs.aws.amazon.com/IAM/latest/UserGuide/IAM_UseCases.html#UseCase_EC2.

Pour créer un compte utilisateur IAM doté des privilèges requis, procédez comme suit :

1. Ouvrez la console de gestion AWS et connectez-vous sous votre compte utilisateur.

2. Dans la liste des services AWS, sélectionnez **IAM** (comme indiqué dans la figure ci-dessous).



Liste des services dans la Console de gestion AWS

Une fenêtre contenant une liste de noms d'utilisateur et le menu qui permet d'utiliser l'outil s'ouvre.

3. Parcourez les zones de la console qui traitent des comptes utilisateurs et ajoutez un ou plusieurs noms d'utilisateur ou noms.

4. Pour chaque utilisateur que vous ajoutez, définissez les propriétés AWS suivantes :

   - Type d'accès : **accès programmé**.
   - Limite des permissions non définies.
   - Permissions :
     - **ReadOnlyAccess** : si vous envisagez seulement de lancer le sondage des segments dans le Cloud et que vous n'envisagez pas l'installation d'applications sur les instances EC2 à l'aide de l'API d'AWS.
     - **ReadOnlyAccess** et **AmazonSSMFullAccess** : si vous prévoyez de lancer le sondage des segments dans le Cloud et d'installer des applications sur les instances EC2 à l'aide de l'API d'AWS. Dans ce cas, vous devez désigner un rôle IAM avec les privilèges AmazonEC2RoleforSSM sur les instances EC2 protégées.

   Après que vous avez ajouté des permissions, révisez-les pour confirmer leur exactitude. En cas d'erreur de sélection, revenez à l'écran précédent et opérez une nouvelle sélection.

5. Après la création du compte utilisateur, un tableau contenant la clé d'accès IAM du nouvel utilisateur IAM s'affiche. L'ID de clé d'accès s'affiche dans la colonne **ID de clé d'accès**. La clé secrète s'affiche sous forme d'astérisques dans la colonne **Clé d'accès secrète**. Pour voir la clé secrète, cliquez sur **Afficher**.

Le compte utilisateur créé apparaît dans la liste des comptes utilisateurs IAM qui correspondent à votre compte utilisateur dans AWS.

Lors du déploiement de Kaspersky Security Center dans le segment dans le Cloud, vous devez indiquer que vous possédez un compte utilisateur IAM et donner à Kaspersky Security Center l'ID de clé d'accès et la clé d'accès secrète.

Les adresses des pages Web citées dans ce document sont correctes à la date de publication de Kaspersky Security Center.

Création du rôle IAM pour l'installation des applications sur l'instance Amazon EC2

Avant de déployer la protection sur les instances EC2 à l'aide des outils de Kaspersky Security Center, créez dans la Console d'administration AWS le rôle IAM disposant des privilèges nécessaires à l'installation des applications sur les instances. Pour plus d'informations, consultez les sections d'Aide AWS sur les rôles IAM.

Le rôle IAM est nécessaire pour l'attribuer à toutes les instances EC2 sur lesquelles vous prévoyez d'installer des applications de sécurité à l'aide de Kaspersky Security Center. Si vous n'attribuez pas à l'instance un rôle IAM doté des privilèges nécessaires, l'installation des applications à l'aide de l'API AWS sur cette instance se soldera par une erreur.

Pour pouvoir utiliser la console de gestion AWS, il vous faut un nom d'utilisateur et un mot de passe d'un compte utilisateur dans AWS.

Pour créer un rôle IAM en vue d'installer les applications sur les instances, procédez comme suit :

1. Ouvrez la console de gestion AWS et connectez-vous sous votre compte utilisateur AWS.
2. Dans le menu de gauche, choisissez l'option **Roles**.
3. Cliquez sur le bouton **Create Role**.
4. Dans la liste des services qui s'ouvre, choisissez **EC2**, puis encore **EC2** dans la liste **Select Your Use case**.
5. Cliquez sur le bouton **Next: Permissions**.
6. Dans la liste qui s'affiche, cochez la case en regard de l'option **AmazonEC2RoleforSSM**.
7. Cliquez sur le bouton **Next: Review**.
8. Saisissez le nom et la description du rôle IAM et appuyez sur le bouton **Create role**.

   Le rôle créé apparaît dans la liste des rôles, sous le nom et avec la description que vous avez saisis.

Par la suite, vous pouvez utiliser le rôle IAM créé lors de la création de nouvelles instances EC2 que vous protégerez à l'aide de Kaspersky Security Center, puis l'associer aux instances déjà existantes.

Les adresses des pages Web citées dans ce document sont correctes à la date de publication de Kaspersky Security Center.

Utilisation avec Amazon RDS

Cette section décrit les actions à réaliser pour préparer une base de données Amazon Relational Database Service (RDS) pour Kaspersky Security Center, la placer dans un groupe d'options, créer un rôle IAM pour l'utilisation d'une base de données RDS, préparer un compartiment S3 pour le stockage et migrer une base de données existantes vers RDS.

Amazon RDS est un service Internet qui aide les utilisateurs AWS à configurer, utiliser et faire évoluer une base de données relationnelles dans le Cloud AWS. Si vous le souhaitez, vous pouvez utiliser une base de données Amazon RDS pour travailler avec Kaspersky Security Center.

Vous pouvez travailler avec les bases de données suivantes :

- Microsoft SQL Server
- SQL Express Edition
- Aurora MySQL 5.7
- Standard MySQL 5.7

Création d'une instance Amazon RDS

Si vous souhaitez utiliser Amazon RDS en tant que SGBD, il faut créer une instance de base de données Amazon RDS. Cette section décrit la manière de sélectionner SQL Express Edition. Si vous souhaitez travailler avec Aurora MySQL ou Standard MySQL (versions 5.7, 8.0), vous devez sélectionner l'un de ces moteurs.

Pour créer une instance de base de données Amazon RDS :

1. Ouvrez la console de gestion AWS à l'adresse https://console.aws.amazon.com et connectez-vous sous votre compte utilisateur.

2. Via l'interface d'AWS, créez une base de données avec les paramètres suivants :

   - Moteur : Microsoft SQL Server, SQL Express Edition
   - Version du moteur de DB : SQL Server 2014 12.00.5546.0v1
   - Catégorie d'instance DB : db.t2.medium
   - Type de stockage : général
   - Stockage attribué : au moins 50 GiO
   - Groupe de sécurité : le même groupe que celui dans lequel l'instance EC2 avec le Serveur d'administration de Kaspersky Security Center va se trouver

   Créez un identificateur, un nom d'utilisateur et un mot de passe pour votre instance RDS.

   Vous pouvez conserver les paramètres par défaut dans tous les autres champs. Mais vous pouvez aussi modifier les valeurs par défaut si vous souhaitez personnaliser votre instance Amazon RDS. Pour obtenir de l'aide, consultez les pages d'informations d'AWS.

3. A la dernière étape, AWS affiche les résultats du processus. Si vous souhaitez voir les détails de votre instance Amazon RDS, cliquez sur **Afficher les détails de l'instance DB**. Si vous souhaitez passer à l'action suivante, lancez la création d'un groupe d'options pour votre instance Amazon RDS.

La création d'une instance Amazon RDS peut durer plusieurs minutes. Une fois que l'instance a été créée, vous pouvez l'utiliser avec des données de Kaspersky Security Center.

Les adresses des pages Web citées dans ce document sont correctes à la date de publication de Kaspersky Security Center.

Création d'un groupe d'options pour une instance Amazon RDS

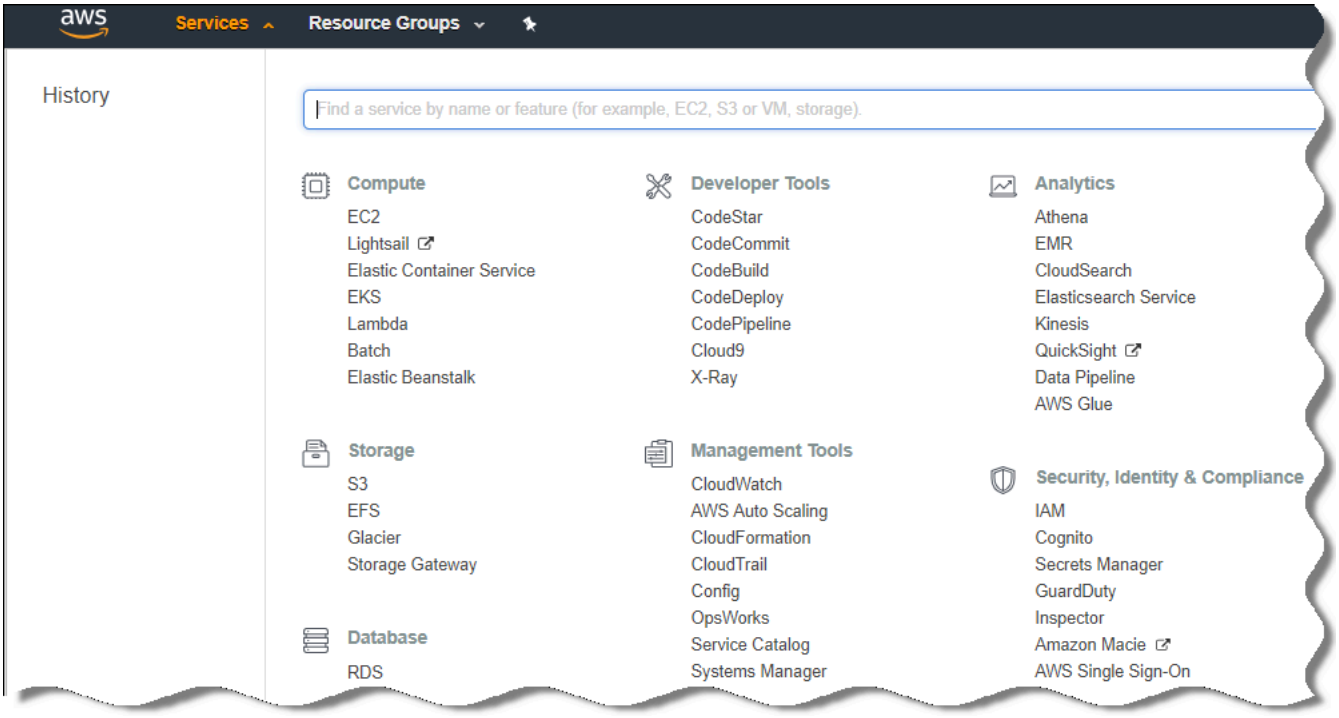
Vous devez placer votre instance Amazon RDS dans un groupe d'options.

Pour créer un groupe d'options pour votre instance Amazon RDS, procédez comme suit :

1. Vérifiez que vous êtes dans la Console de gestion AWS (https://console.aws.amazon.com) et que vous êtes connecté sous votre compte.

2. Dans la ligne du menu, cliquez sur **Services**.

   La liste des services disponibles s'affiche (cf. figure ci-dessous).



Liste des services dans la Console de gestion AWS

3. Dans la liste. cliquez sur **RDS**.

4. Dans le volet gauche, cliquez sur **Groupes d'options**.

5. Cliquez sur le bouton **Créer un groupe**.

6. Créez un groupe d'options avec les paramètres suivants si vous avez choisi SQL Serveur à l'étape de la création de l'instance Amazon RDS :

   - Moteur : SQLserver-ex
   - Version majeur du moteur : 12.00

   Si vous avez choisi une base de données SQL différente au moment de la création de l'instance Amazon RDS, choisissez le moteur correspondant.

Le groupe est créé et s'affiche dans la liste de vos groupes.

Une fois que le groupe d'options a été créé, placez votre instance Amazon RDS dans celui-ci.

Les adresses des pages Web citées dans ce document sont correctes à la date de publication de Kaspersky Security Center.

Modification du groupe d'options

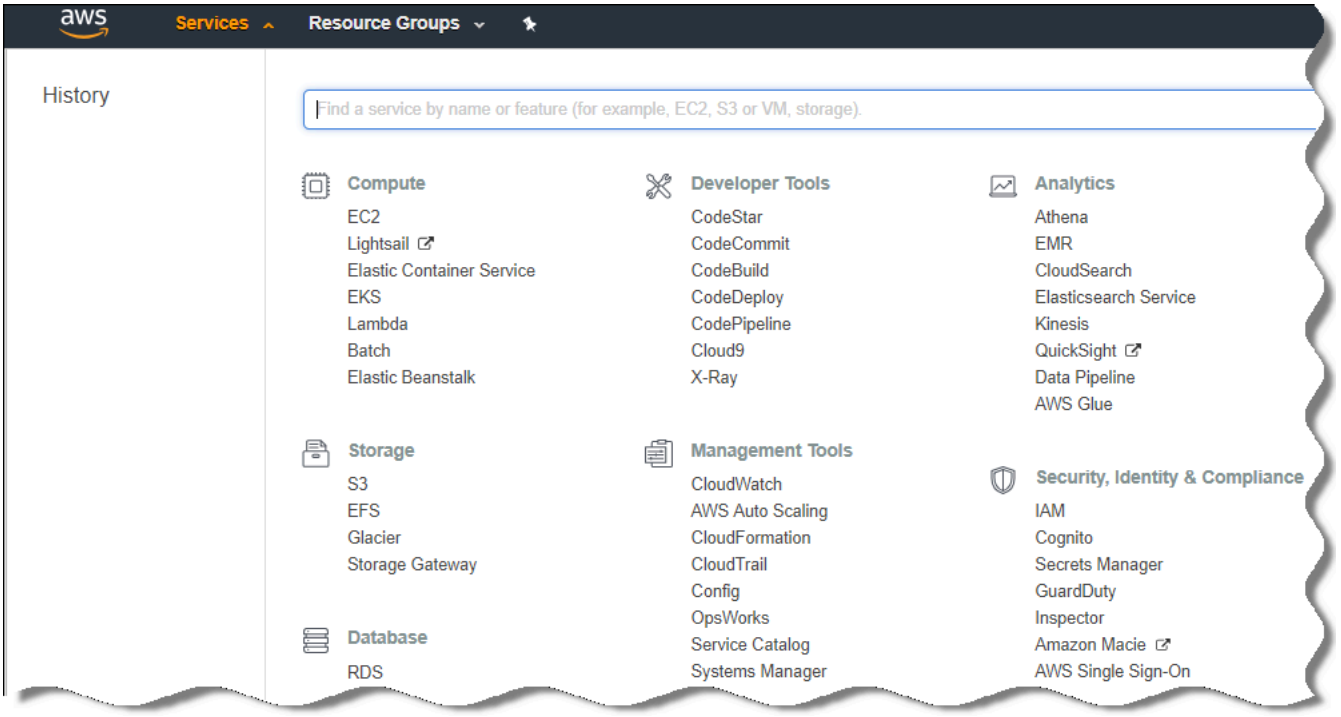
La configuration par défaut du groupe d'options dans lequel vous avez placé l'instance d'Amazon RDS ne suffit pas pour une utilisation avec la base de données de Kaspersky Security Center. Vous devez ajouter des options au groupe d'options et créer un nouveau rôle IAM pour l'utilisation avec la base de données.

Pour modifier le groupe d'options et créer un rôle IAM :

1. Vérifiez que vous êtes dans la Console de gestion AWS (https://console.aws.amazon.com) et que vous êtes connecté sous votre compte.

2. Dans la ligne du menu, cliquez sur **Services**.

   La liste des services disponibles s'affiche (cf. figure ci-dessous).



Liste des services dans la Console de gestion AWS

3. Dans la liste, sélectionnez RDS.

4. Dans le volet gauche, cliquez sur **Groupes d'options**.

   La liste des groupes d'options est affichée.

5. Sélectionnez le groupe d'options dans lequel vous avez placé votre instance Amazon RDS et cliquez sur le bouton **Ajouter une option**.

   La fenêtre **Ajouter une option** s'ouvre.

6. Dans la section du rôle IAM, sélectionnez l'option **Créer un rôle** / **Oui** et saisissez un nom pour le nouveau rôle IAM.

   Le rôle est créé avec un ensemble de permissions par défaut. Par la suite, il faudra modifier ses permissions.

7. Dans la section compartiment S3, choisissez un des éléments suivants :

   - Si vous n'avez pas créé une instance de compartiment Amazon S3 pour la sauvegarde des données, sélectionnez le lien **Créez un compartiment S3** et créez un compartiment S3 via l'interface d'AWS.
   - Si vous avez déjà créé une instance de compartiment Amazon S3 pour la tâche de sauvegarde des données du Serveur d'administration, sélectionnez votre compartiment S3 dans la liste déroulante.

8. Terminez d'ajouter des options en cliquant sur le bouton **Ajoutez une option** en bas de la page.

Vous avez modifié le groupe d'options et créé un rôle IAM pour l'utilisation avec la base de données RDS.

Les adresses des pages Web citées dans ce document sont correctes à la date de publication de Kaspersky Security Center.

Modifications des permissions pour un rôle IAM pour une instance de base de données Amazon RDS

Après avoir ajouté des options au groupe d'options, vous devez attribuer les autorisations requises au rôle IAM que vous avez créé en vue d'utiliser l'instance de base de données Amazon RDS.

Pour attribuer les permissions requises au rôle IAM que vous avez créé en vue d'utiliser l'instance de base de données Amazon RDS, procédez comme suit :

1. Vérifiez que vous êtes dans la Console de gestion AWS (https://console.aws.amazon.com) et que vous êtes connecté sous votre compte.
2. Dans la liste des services, sélectionnez **IAM**.

   Une fenêtre contenant une liste de noms d'utilisateur et le menu qui permet d'utiliser l'outil s'ouvre.

3. Dans le menu, sélectionnez **Rôles**.
4. Dans la liste des rôles IAM affichés dans l'espace de travail, sélectionnez le rôle que vous avez créé lors de l'ajout d'une option au groupe d'options.
5. A l'aide de l'interface d'AWS, supprimez la stratégie **sqlNativeBackup-<date>**.
6. À l'aide de l'interface d'AWS, associez la stratégie **AmazonS3FullAccess** au rôle.

Le rôle IAM obtient les permissions requises pour fonctionner avec Amazon RDS.

Les adresses des pages Web citées dans ce document sont correctes à la date de publication de Kaspersky Security Center.

Préparation d'un compartiment Amazon S3 pour la base de données

Si vous avez l'intention d'utiliser une base de données Amazon Relational Database System (Amazon RDS), vous devez créer une instance de compartiment Amazon Simple Storage Service (Amazon S3) dans lequel la sauvegarde régulière de la base de données sera stockée. Pour en savoir plus sur Amazon S3 et les seaux S3, consultez les pages d'aide d'Amazon. Pour en savoir plus sur la création d'une instance Amazon S3, consultez la page d'aide d'Amazon S3.

Pour créer un compartiment Amazon S3 :

1. Confirmez que la Console de gestion AWS est ouverte et que vous avez ouvert une session sous votre compte.
2. Dans la liste des services AWS, sélectionnez S3.
3. Parcourez la console pour créer un compartiment en suivant les instructions de l'Assistant.
4. Sélectionnez la même région que celle où se trouve votre Serveur d'administration (ou dans laquelle il va se trouver).
5. Une fois que l'Assistant a terminé, confirmez que le nouveau compartiment apparaît dans la liste des seaux.

Un seau S3 est créé est apparaît dans votre liste de seaux. Il faut définir ce compartiment au moment de l'ajout d'options au groupe d'options. Il faudra indiquer l'adresse de votre compartiment S3 à Kaspersky Security Center quand Kaspersky Security Center crée la tâche de *Sauvegarde des données du Serveur d'administration*.

Les adresses des pages Web citées dans ce document sont correctes à la date de publication de Kaspersky Security Center.

Migration de la base de données vers Amazon RDS

Vous pouvez migrer votre base de données Kaspersky Security Center depuis un appareil sur site vers une instance Amazon S3 compatible avec Amazon RDS. Pour cela, il vous faut un seau S3 pour une base de données RDS et un compte utilisateur IAM avec la permission AmazonS3FullAccess pour ce seau S3.

Pour migrer la base de données :

1. Confirmez que vous avez créé une instance RDS (consultez les pages de référence d'Amazon RDS pour en savoir plus).
2. Sur votre Serveur d'administration physique (sur site), exécutez l'utilitaire de la copie de sauvegarde de Kaspersky pour sauvegarder données du Serveur d'administration.

   Vous devez vous assurer que le fichier est intitulé backup.zip.
3. Copiez le fichier backup.zip sur l'instance EC2 sur laquelle le Serveur d'administration est installé.

Veillez à ce que le disque de l'instance EC2 sur lequel le Serveur d'administration est installé possède l'espace suffisant sur le disque. Il est possible d'ajouter dans l'environnement AWS plus d'espace disque à votre instance pour faciliter le processus de migration de la base de données.

4. Sur le Serveur d'administration AWS, lancez à nouveau l'utilitaire de la copie de sauvegarde de Kaspersky en mode interactif.

   L'Assistant de sauvegarde et de restauration des données démarre.

5. À l'étape **Sélectionnez une action**, sélectionnez **Restaurer les données du Serveur d'administration**, puis cliquez sur **Suivant**.

6. À l'étape **Paramètres de restauration**, cliquez sur le bouton **Parcourir** en regard du **Dossier d'enregistrement des copies de sauvegarde**.

7. Dans la fenêtre **Se connecter au stockage cloud** qui s'ouvre, remplissez les champs suivants, puis cliquez sur **OK** :

   - **Nom du compartiment S3**

     Le nom de votre compartiment S3.

   - **Dossier de sauvegarde**

     Désignez l'emplacement du dossier de stockage prévu pour la sauvegarde.

   - **ID de clé d'accès**

     ID de clé d'accès AWS IAM qui appartient à l'utilisateur IAM doté des permissions d'utilisation du compartiment S3 (permission AmazonS3FullAccess).

   - **Clé secrète**

     Clé secrète AWS IAM qui appartient à l'utilisateur IAM doté des permissions d'utilisation du compartiment S3 (permission AmazonS3FullAccess).

8. Sélectionnez l'option **Migrer depuis la sauvegarde locale**. Le bouton **Parcourir** est désormais disponible.

9. Appuyez sur le bouton **Parcourir** pour sélectionner le dossier sur le Serveur d'administration AWS où vous avez copié le fichier backup.zip.

10. Cliquez sur **Suivant** et terminez la procédure.

    Vos données sont restaurées dans la base de données RDS à l'aide de votre compartiment S3. Vous pouvez utiliser cette base de données pour continuer à travailler avec Kaspersky Security Center dans l'environnement AWS.

Les adresses des pages Web citées dans ce document sont correctes à la date de publication de Kaspersky Security Center.

Manipulation dans le Cloud Microsoft Azure

Cette section fournit des informations sur la manière de déployer et de maintenir Kaspersky Security Center dans l'environnement Cloud de la plateforme Microsoft Azure et sur la manière de déployer la protection sur les des machines virtuelles au sein de l'environnement Cloud.

Dans un Kaspersky Security Center qui a été déployé depuis un SKU facturé mensuellement en fonction de l'utilisation, la Gestion des vulnérabilités et des correctifs est activée automatiquement et il est impossible d'activer l'Administration des appareils mobiles.

À propos de l'utilisation de Microsoft Azure

Pour utiliser la plateforme Microsoft Azure et plus particulièrement, pour pouvoir acheter des applications dans Azure Marketplace et créer des machines virtuelles, il faut disposer d'un abonnement Azure. Avant de déployer le Serveur d'administration, créez un ID de l'application Azure avec les permissions requises pour l'installation d'applications sur les machines virtuelles.

Si vous achetez une image de Kaspersky Security Center dans la Place de marché Azure, vous pouvez déployer une machine virtuelle à l'aide de votre Serveur d'administration de Kaspersky Security Center prêt à l'emploi. Vous devez définir les paramètres de la machine virtuelle, mais vous ne devez pas installer l'application vous même. Après l'installation, vous pouvez lancer la Console d'administration et vous connecter au Serveur d'administration pour commencer à travailler avec Kaspersky Security Center.

Vous pouvez aussi utiliser une machine virtuelle Azure dotée du Serveur d'administration de Kaspersky Security Center pour protéger les appareils physiques (par exemple, si un tel serveur Cloud s'avère plus pratique au niveau de la maintenance et du contenu qu'un serveur physique). Dans ce cas, l'utilisation du Serveur d'administration est identique au cas de figure où le Serveur d'administration serait installé sur un appareil sur site. Si vous n'avez pas l'intention d'utiliser l'API d'Azure, vous n'avez pas besoin d'un ID de l'application Azure. Dans ce cas, l'abonnement Azure suffit.

Création d'un abonnement, d'un ID de l'application et d'un mot de passe

Pour travailler avec Kaspersky Security Center dans l'environnement Microsoft Azure, il vous faut un abonnement Azure, un ID de l'application Azure et un mot de passe de l'application Azure. Vous pouvez utiliser un abonnement existant si vous en possédez déjà un.

L'abonnement Azure permet à son détenteur d'accéder au portail d'administration de la plateforme Microsoft Azure et aux services Microsoft Azure. L'abonné peut utiliser la plateforme Microsoft Azure pour gérer des services comme Azure SQL et le Stockage Azure.

Pour créer un abonnement Microsoft Azure,

Accédez à https://learn.microsoft.com/en-us/azure/cost-management-billing/manage/create-subscription et suivez les instructions qui s'y trouvent.

Pour en savoir plus sur la création d'un abonnement, consultez le site Internet de Microsoft. Vous obtiendrez un ID d'abonnement que vous communiquerez plus tard à Kaspersky Security Center avec l'ID de l'application et le mot de passe.

Pour créer et enregistrer l'identifiant de l'application Azure et le mot de passe,

1. Rendez-vous sur https://portal.azure.com et confirmez que vous êtes connecté.
2. A l'aide des instructions reprises sur la page de référence, créez votre identifiant de l'application.
3. Accédez à la section **Clés** des paramètres de l'application.
4. Dans la section **Clés**, remplissez les champs **Description** et **Expire le** et laissez le champ **Valeur** vide.
5. Cliquez sur **Enregistrer**.

   Quand vous cliquez sur **Enregistrer**, le système remplit automatiquement le champ **Valeur** avec une longue séquence de caractères. Cette séquence est votre mot de passe de l'application Azure (par exemple, yXyPOy6Tre9PYgP/j4XVyJCvepPHk2M/UYJ+QlfFvdU=). La description est affichée comme vous l'avez saisie.
6. Copiez le mot de passe et enregistrez-le afin que vous puissiez transmettre plus tard l'ID de l'application et le mot de passe à Kaspersky Security Center.

   Vous pouvez copier le mot de passe uniquement lors de sa création. Par la suite, le mot de passe ne sera plus affiché et il ne peut être récupéré.

Les adresses des pages Web citées dans ce document sont correctes à la date de publication de Kaspersky Security Center.

Attribution d'un rôle à un identifiant de l'application Azure

Si vous souhaitez uniquement détecter les machines virtuelles à l'aide de la recherche d'appareils, votre ID de l'application Azure doit avoir le rôle de Lecteur. Si vous voulez non seulement détecter les machines virtuelles, mais également déployer la protection sur les machines virtuelles, votre ID de l'application Azure doit avoir le rôle de contributeur des machines virtuelles.

Suivez les instructions reprises sur le site Internet de Microsoft pour attribuer un rôle à votre ID de l'application Azure.

Déploiement du Serveur d'administration dans Microsoft Azure et sélection d'une base de données

Pour déployer le Serveur d'administration dans l'environnement Microsoft Azure :

1. Connectez-vous à Microsoft Azure sous votre compte.
2. Rendez-vous sur le portail Azure.
3. Dans le volet de gauche, cliquez sur le signe « + » vert.
4. Tapez « Kaspersky Hybrid Cloud Security » dans le champ de recherche du menu.

   Kaspersky Hybrid Cloud Security est une combinaison de Kaspersky Security Center et de deux applications de sécurité pour la protection des instances : Kaspersky Endpoint Security for Linux et Kaspersky Security for Windows Server.

5. Dans la liste des résultats, sélectionnez Kaspersky Hybrid Cloud Security ou Kaspersky Hybrid Cloud Security (BYOL).

   Dans la partie droite de l'écran, une fenêtre d'informations s'ouvre.

6. Lisez ces informations, puis cliquez sur le bouton Créer en bas de la fenêtre d'informations.

7. Remplissez tous les champs requis. Utilisez les astuces pour obtenir des informations et de l'aide.

8. Pour la taille, sélectionnez un des trois options avec une étoile.

   Dans la majorité des cas, 8 Go de mémoire RAM suffisent. Toutefois, il est possible, dans Azure, d'augmenter la mémoire vive et d'autres ressources de la machine virtuelle à tout moment.

9. Au moment de choisir une base de données, opérez la sélection en fonction de votre plan :

   - Locale, si vous voulez une base de données sur la même machine virtuelle que celle où le Serveur d'administration va être déployé. Kaspersky Security Center est livré avec une base de données SQL Server Express. Choisissez cette option si SQL Server Express suffit à vos besoins.

   - Nouvelle, si vous voulez une nouvelle base de données RDS dans l'environnement Azure. Sélectionnez cette option si vous souhaitez un SGBD différent de SQL Server Express. Vos données seront transférées et conservées dans le Cloud et vous n'aurez aucun frais supplémentaires.

   - Existante, si vous voulez utiliser un serveur de base de données existant. Dans ce cas, vous devez indiquer son emplacement. Si le serveur se trouve hors de l'environnement Azure, vos données seront transférées via Internet, ce qui pourrait entraîner des frais supplémentaires.

10. Au moment de saisir l'ID d'abonnement, utilisez l'abonnement que vous aviez créé plus tôt.

    Après le déploiement, vous pouvez vous connecter au Serveur d'administration via RDP. Vous pouvez utiliser la Console d'administration pour travailler avec le Serveur d'administration.

Utilisation d'Azure SQL

Cette section décrit les actions à réaliser pour préparer une base de données Microsoft Azure pour Kaspersky Security Center, préparer un compte du stockage Azure et migrer une base de données existante vers Azure SQL.

La base de données SQL est un service polyvalent administré de base de données relationnelle dans Microsoft Azure.

Les adresses des pages Web citées dans ce document sont correctes à la date de publication de Kaspersky Security Center.

Création d'un compte du stockage Azure

Vous devez créer un compte de stockage dans Microsoft Azure pour utiliser la base de données Azure SQL et pour les scripts de déploiement.

Pour créer un compte de stockage, procédez comme suit :

1. Connectez-vous sur le portail Azure.
2. Dans le volet gauche, sélectionnez **Comptes de stockage** pour ouvrir la fenêtre **Comptes de stockage**.
3. Dans la fenêtre **Comptes de stockage**, cliquez sur le bouton **Ajouter** pour ouvrir la fenêtre **Créer un compte de stockage**.
4. Remplissez tous les champs requis pour créer un compte de stockage :
   - Emplacement : doit être identique à l'emplacement du Serveur d'administration.
   - Autres champs : vous pouvez conserver les valeurs par défaut.

   Consultez les astuces pour en savoir plus sur chaque champ.

   Une fois le compte de stockage créé, la liste de vos comptes de stockage s'affiche.
5. Dans la liste de vos comptes de stockage, cliquez sur le nom du compte qui vient d'être créé afin de voir les informations à son sujet.
6. Veillez à connaître le nom du compte utilisateur, le groupe de ressources et les clés d'accès pour ce compte de stockage. Ces informations seront nécessaires pour travailler avec Kaspersky Security Center.

Vous pouvez consulter le site Internet d'Azure pour obtenir de l'aide.

Si vous avez déjà un compte de stockage, vous pouvez l'utiliser avec Kaspersky Security Center.

Création de la base de données Azure SQL et du serveur SQL

Il vous faut une base de données SQL et un serveur SQL dans l'environnement Azure.

Pour créer une base de données Azure SQL et un serveur SQL :

1. Suivez les instructions sur le site Internet d'Azure.

   Vous pouvez créer un nouveau serveur lorsque Microsoft Azure vous y invite. Si vous avez déjà un serveur Azure SQL Server, vous pouvez l'utiliser pour Kaspersky Security Center au lieu d'en créer un nouveau.
2. Après avoir créé la base de données SQL et le serveur SQL, confirmez que vous connaissez le nom de la ressource et le groupe de ressources :
   a. Rendez-vous sur https://portal.azure.com et confirmez que vous êtes connecté.
   b. Dans la partie gauche de la fenêtre, sélectionnez **Bases de données SQL**.
   c. Cliquez sur le nom de la base de données dans la liste de vos bases de données.

      La fenêtre des propriétés s'ouvre.
   d. Le nom de la base de données est le nom de la ressource. Le nom du groupe de ressources est affiché dans la section **Aperçu** de la fenêtre Propriétés.

Vous avez besoin du nom de la ressource et du groupe de ressources de la base de données pour migrer la base de données vers Azure SQL.

Migration de la base de données vers Azure SQL

Après le déploiement du Serveur d'administration dans l'environnement Azure, vous pouvez migrer votre base de données de Kaspersky Security Center depuis un appareil sur site vers Azure SQL. Il vous faut pour cela un compte du stockage Azure pour une base de données Azure SQL. Votre Serveur d'administration doit également être muni de Microsoft SQL Server Data-Tier Application Framework (DacFx) et de SQLSysCLRTypes.

Pour migrer la base de données :

1. Confirmez que vous avez créé un compte du stockage Azure.

2. Assurez-vous que SQLSysCLRTypes et DacFx se trouvent sur votre Serveur d'administration.

   Vous pouvez télécharger Microsoft SQL Server Data-Tier Application Framework (17.0.1 DacFx) et SQLSysCLRTypes (choisissez la version correspondant à la version de votre serveur SQL) sur le site officiel de Microsoft.

3. Sur votre Serveur d'administration physique (sur site), exécutez l'utilitaire de la copie de sauvegarde de Kaspersky pour sauvegarder les données du Serveur d'administration avec l'option **Migrer au format Azure** activée.

4. Copiez le fichier de sauvegarde sur le Serveur d'administration Azure.

   > Veillez à ce que le disque de la machine virtuelle Azure sur lequel le Serveur d'administration est installé possède assez d'espace. Il est possible d'ajouter dans l'environnement Azure plus d'espace disque à vos machines virtuelles pour faciliter le processus de migration de la base de données.

5. Sur le Serveur d'administration situé dans l'environnement Microsoft Azure, lancez à nouveau l'utilitaire de la copie de sauvegarde de Kaspersky en mode interactif.

   L'Assistant de sauvegarde et de restauration des données démarre.

6. À l'étape **Sélectionnez une action**, sélectionnez **Restaurer les données du Serveur d'administration**, puis cliquez sur **Suivant**.

7. À l'étape **Paramètres de restauration**, cliquez sur le bouton **Parcourir** en regard du **Dossier d'enregistrement des copies de sauvegarde**.

8. Dans la fenêtre **Se connecter au stockage cloud** qui s'ouvre, remplissez les champs suivants, puis cliquez sur **OK** :

   - **Nom du compte du stockage Azure**

     Vous avez créé le nom du Compte du stockage Azure pour utiliser Kaspersky Security Center.

   - **Dossier de sauvegarde**

     Désignez l'emplacement du dossier de stockage prévu pour la sauvegarde.

   - **Identifiant de l'abonnement Azure**

     Vous avez créé l'abonnement sur le portail Azure.

   - **Mot de passe de l'application Azure**

     Vous avez obtenu le mot de passe de l'identifiant de l'application quand vous avez créé celui-ci.

     Les caractères de la mot de passe s'affichent sous la forme d'astérisques. Après que vous avez commencé à saisir le mot de passe, le bouton **Afficher** apparaît. Maintenez ce bouton enfoncé pour voir les caractères saisis.

   - **Clé d'accès au stockage Azure**

     Disponible dans les propriétés de votre compte de stockage, dans la sections Clés d'accès. Vous pouvez utiliser n'importe quelle clé (clé1 ou clé2).

   - **Nom du serveur SQL Azure**

     Disponible dans les propriétés de votre serveur SQL Azure.

   - **Groupe de ressources du serveur SQL Azure**

     Disponible dans les propriétés de votre serveur SQL Azure.

   - **ID de l'application Azure**

     Vous avez créé cet identifiant de l'application sur le portail Azure.

     Vous pouvez fournir un identifiant de l'application Azure pour le sondage et d'autres fins. Si vous souhaitez sonder un autre segment Azure, il faut d'abord supprimer la connexion Azure existante.

9. Sélectionnez l'option **Migrer depuis la sauvegarde locale**.

   Le bouton **Parcourir** est désormais disponible.

10. Cliquez sur le bouton **Parcourir** pour sélectionner le dossier sur le Serveur d'administration d'Azure dans lequel vous avez copié le fichier de sauvegarde.

11. Cliquez sur **Suivant** et terminez la procédure.

    Les données sont restaurées dans la base de données Azure SQL à l'aide de votre utilisation du stockage Azure. Vous pouvez utiliser cette base de données pour continuer à travailler avec Kaspersky Security Center dans l'environnement Azure.

Les adresses des pages Web citées dans ce document sont correctes à la date de publication de Kaspersky Security Center.

Travailler dans Google Cloud

Cette section fournit des informations sur l'utilisation de Kaspersky Security Center dans le cloud fourni par Google.

Création d'un email client, d'un identifiant de projet et d'une clé privée

Vous pouvez utiliser l'API Google pour travailler avec Kaspersky Security Center dans Google Cloud Platform. Un compte Google est requis. Pour en savoir plus, veuillez consulter la documentation Google à l'adresse https://cloud.google.com.

Vous devrez créer et fournir à Kaspersky Security Center les informations d'identification suivantes :

- **Email client**

  L'email client est l'adresse email que vous avez utilisée pour enregistrer votre projet sur Google Cloud.

- **Identifiant du projet**

  L'identifiant du projet est l'identifiant que vous avez reçu lors de l'enregistrement de votre projet sur Google Cloud.

- **Clé privée**

  La clé privée est la séquence de caractères que vous avez reçue comme clé privée lors de l'enregistrement de votre projet sur Google Cloud. Envisagez de copier et coller cette séquence pour éviter les erreurs.

Utilisation de l'instance Google Cloud SQL for MySQL

Vous pouvez créer une base de données dans Google Cloud et utiliser cette base de données pour Kaspersky Security Center.

Kaspersky Security Center fonctionne avec MySQL 5.7 et 5.6. Les autres versions de MySQL n'ont pas été testées.

Pour créer et configurer une base de données MySQL, procédez comme suit :

Dans votre navigateur, accédez à la page https://cloud.google.com/sql/docs/mysql/create-instance#create-2nd-gen et suivez les instructions fournies.

Lors de la configuration d'une base de données MySQL, utilisez les indicateurs suivants :

- **sort_buffer_size** 10000000
- **join_buffer_size** 20000000
- **innodb_lock_wait_timeout** 300
- **max_allowed_packet** 32000000
- **innodb_thread_concurrency** 20
- **max_connections** 151
- **tmp_table_size** 67108864
- **max_heap_table_size** 67108864
- **lower_case_table_names** 1

Conditions indispensables pour des appareils clients dans l'environnement Cloud en vue de l'utilisation avec Kaspersky Security Center

Les appareils sur lesquels vous envisagez d'installer le Serveur d'administration, l'Agent d'administration et les applications de sécurité de Kaspersky doivent remplir les conditions suivantes :

- Les paramètres des groupes de la sécurité rendent accessibles les ports suivants sur le Serveur d'administration (ensemble minimum de ports nécessaire au déploiement) :

  - 8060 HTTP : pour le transfert du Serveur d'administration aux instances protégées des paquets d'installation de l'Agent d'administration et des applications de sécurité
  - 8061 HTTPS : pour le transfert du Serveur d'administration aux instances protégées des paquets d'installation de l'Agent d'administration et des applications de sécurité
  - 13000 TCP : pour le transfert des instances protégées et des Serveurs d'administration secondaires au Serveur d'administration principal à l'aide de SSL
  - 13000 UDP : pour le transfert sur le Serveur d'administration des informations sur la désactivation des instances
  - 14000 TCP : pour le transfert des instances protégées et des Serveurs d'administration secondaires au Serveur d'administration principal sans SSL
  - 13291 : pour la connexion de la Console d'administration au Serveur d'administration
  - 40080 : pour le fonctionnement des scripts de déploiement

  Vous pouvez configurer les groupes de sécurité dans la console de gestion AWS ou sur le portail Azure. Si vous avez l'intention d'utiliser Kaspersky Security Center dans une configuration autre que la configuration par défaut, consultez la Base de connaissances. Parmi les exemples de configurations autres que la configuration par défaut, citons la non-installation de la Console d'administration sur l'appareil du Serveur d'administration mais bien sur votre poste de travail ou l'utilisation d'un serveur proxy KSN.

- Sur les appareils clients, le port 15000 UDP (pour l'accueil des requêtes de connexion au Serveur d'administration) est accessible.

- Dans le cloud AWS :
  - Si vous avez l'intention d'utiliser l'API d'AWS, le rôle IAM sous lequel les applications vont être installées sur les instances est défini.
  - L'agent SMM (Systems Manager Agent) est installé et exécuté sur chaque instance Amazon EC2.
  - L'agent SMM permet à Kaspersky Security Center d'installer automatiquement des applications sur des appareils et des groupes d'appareil sans demander à chaque fois la confirmation de l'administrateur.
  - L'agent SMM est installé et fonctionne sur les instances qui tourne sous Windows et qui ont été déployées au départ d'images AMI après novembre 2016. Sur tous les autres appareils, vous devrez installer l'agent SMM vous-même. Pour en savoir plus sur l'installation de l'agent SMM sur des appareils tournant sous les systèmes d'exploitation Windows et Linux, consultez la page d'aide d'AWS.
- Dans le cloud Microsoft Azure :
  - L'agent VM Azure est installé et exécuté sur chaque machine virtuelle Azure.

    Une nouvelle machine virtuelle est créée par défaut avec l'agent VM Azure et il n'est pas nécessaire de l'installer ou de l'activer manuellement. Consultez l'aide de Microsoft pour en savoir plus sur l'agent Azure VM sur les appareils Windows et les appareils Linux.
  - Votre ID de l'application Azure possède les rôles suivants :
    - Lecteur (pour rechercher les machines virtuelles par le sondage)
    - Contributeur des machines virtuelles (pour déployer la protection sur les machines virtuelles)
    - Contributeur de SQL Server (pour utiliser une bases de données SQL dans l'environnement Microsoft Azure)

    Si vous souhaitez réaliser toutes ces opérations, attribuez les trois rôles à votre ID de l'application Azure.

Création des paquets d'installation requis pour configurer l'environnement cloud

L'Assistant de configuration pour une utilisation dans le Cloud dans Kaspersky Security Center est disponible si vous disposez des paquets d'installation et des plug-ins d'administration pour les programmes suivants :

- Kaspersky Endpoint Security for Linux
- Kaspersky Endpoint Security for Windows

  > Le déploiement de Kaspersky Endpoint Security for Windows dans un environnement Cloud sera disponible après la prochaine version de Kaspersky Endpoint Security 12.0 for Windows.

- Kaspersky Security for Windows Server

Ces paquets d'installation sont nécessaires à l'installation des applications sur les instances ou les machines virtuelles que vous souhaitez protéger. Si vous ne disposez pas de ces paquets d'installation, vous devez les créer. Sinon, l'Assistant de configuration pour une utilisation dans le Cloud ne peut pas fonctionner.

Pour créer des paquets d'installation, procédez comme suit :

1. Téléchargez les versions les plus récentes des applications et des plug-ins sur le site Web de Kaspersky :
   - Le programme d'installation et le plug-in d'administration de Kaspersky Security for Windows Server.
   - Le programme d'installation, les fichiers pour l'installation à distance via Kaspersky Security Center et le plug-in d'administration de Kaspersky Endpoint Security for Linux.
2. Enregistrez tous les fichiers sur l'instance (ou la machine virtuelle) sur laquelle le Serveur d'administration est installé.
3. Extrayez les fichiers de tous les paquets.
4. Démarrez Kaspersky Security Center.
5. Dans l'arborescence de la console, accédez à **Avancé** → **Installation à distance** → **Paquets d'installation** et cliquez sur **Créer un paquet d'installation**.
6. Sélectionner **Créer un paquet d'installation Kaspersky**.
7. Précisez le nom du paquet et le chemin d'accès au programme d'installation de l'application :<dossier>\<nom du fichier>.kud, puis cliquez sur **Suivant**.
8. Lisez le Contrat de licence utilisateur final et cochez la case confirmant que vous acceptez ses conditions, puis cliquez sur **Suivant**.

Le paquet d'installation sera chargé sur le Serveur d'administration et sera disponible dans la liste des paquets d'installation.

La configuration de l'environnement cloud devient disponible dès que vous créez les paquets d'installation et installez les plug-ins d'administration sur le Serveur d'administration.

Configuration de l'environnement cloud

Pour configurer Kaspersky Security Center à l'aide de l'Assistant de configuration pour une utilisation dans le Cloud, vous devez disposer des éléments suivants :

- Les informations d'identification particulières pour un environnement cloud :
  - Un rôle IAM qui a reçu l'autorisation de sonder le segment dans le Cloud ou un compte utilisateur IAM qui a reçu l'autorisation de sonder le segment dans le Cloud (pour une utilisation avec Amazon Web Services)
  - Un ID de l'application Azure, un mot de passe et un abonnement (pour une utilisation avec Microsoft Azure)
  - Adresse email du client Google, ID du projet et clé privée (pour une utilisation avec Google Cloud)
- Paquets d'installation :
  - Agent d'administration pour Windows
  - Agent d'administration pour Linux
  - Kaspersky Endpoint Security for Linux

- Plug-in Internet pour Kaspersky Endpoint Security for Linux
- Au moins un des éléments suivants :
  - Paquet d'installation et plug-in Internet pour Kaspersky Endpoint Security for Windows (recommandé)
  - Paquet d'installation et plug-in Internet pour Kaspersky Security for Windows Server

Si vous ne souhaitez pas utiliser la possibilité de travailler dans l'environnement cloud (par exemple, si vous voulez administrer la protection uniquement d'appareils clients physiques), vous pouvez quitter l'Assistant de configuration pour une utilisation dans le Cloud et lancer manuellement l'Assistant de configuration initiale du Serveur d'administration standard.

L'opération de configuration pour une utilisation dans le Cloud démarre automatiquement à la première connexion via la Console d'administration au Serveur d'administration si vous déployez Kaspersky Security Center depuis une image AMI prête. Vous pouvez également démarrer l'Assistant de configuration pour une utilisation dans le Cloud à tout moment.

Pour lancer l'Assistant de configuration pour une utilisation dans le Cloud manuellement, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez l'entrée **Serveur d'administration**.
2. Dans le menu contextuel du nœud, choisissez l'option **Toutes les tâches → Configurer l'&environnement cloud**.

La séance de travail moyenne dure environ 15 minutes.

À propos de l'Assistant de configuration pour une utilisation dans le Cloud

L'Assistant de configuration pour une utilisation dans le Cloud permet de configurer Kaspersky Security Center en tenant compte des particularités du travail dans le Cloud.

L'assistant crée les objets suivants :

- Stratégie de l'Agent d'administration avec les paramètres par défaut
- Stratégie pour Kaspersky Endpoint Security for Linux
- Stratégie pour Kaspersky Security for Windows Server
- Groupe d'administration pour les instances et une règle pour placer automatiquement ces instances dans ce groupe d'administration
- Tâche de sauvegarde des données du Serveur d'administration
- Tâches d'installation de la protection sur des appareils Linux et Windows
- Tâches pour chacun des appareils administrés :
  - Analyse des logiciels malveillants rapide
  - Téléchargement des mises à jour

Si vous avez choisi l'option de licence BYOL, la configuration de l'environnement cloud active également Kaspersky Security Center à l'aide d'un fichier clé ou d'un code d'activation et place le fichier clé ou le code d'activation dans le stockage des licences.

Étape 1. Sélection de la méthode d'activation de l'application

Cette étape ne s'affiche pas si vous vous êtes inscrit à l'une des AMI prêtes à l'emploi (sur AWS Marketplace) ou pour une SKU facturée mensuellement en fonction de l'utilisation (sur la Place de marché Azure). Dans ce cas, l'assistant passe immédiatement à l'étape suivante. Vous ne pouvez cependant pas acheter une AMI prête à l'emploi pour Google Cloud.

Si vous avez choisi la licence Kaspersky Security Center selon le modèle BYOL, l'Assistant vous invite à sélectionner la méthode d'activation de l'application.

Activez l'application à l'aide d'un code d'activation ou (ou d'un fichier clé) pour l'application Kaspersky Security for Virtualization ou Kaspersky Hybrid Cloud Security.

Vous pouvez activer l'application selon un des moyens suivants :

- Saisir le code d'activation.

  L'activation en ligne démarre. Ce processus implique la vérification du code d'activation indiqué ainsi que l'émission et l'activation d'un fichier clé.

- Indiquer le fichier clé.

  L'application vérifie le fichier clé, puis l'active s'il contient les informations correctes ou propose de renseigner un autre fichier clé.

Kaspersky Security Center place la clé de licence dans le stockage des licences et la désigne comme clé automatiquement distribuée sur les appareils administrés.

Si vous connectez à une instance à l'aide de l'application standard Microsoft Windows Remote Desktop Connection ou d'une application similaire, indiquez dans les propriétés de la connexion à distance le disque de l'appareil physique que vous utilisez pour établir la connexion. Ainsi vous garantissez l'accès depuis l'instance aux fichiers sur votre appareil physique et vous pouvez sélectionner et désigner le fichier clé.

Lors de l'utilisation de Kaspersky Security Center, déployé depuis une image AMI payante ou pour un SKU facturé mensuellement en fonction de l'utilisation, il est impossible d'ajouter des fichiers clés ou des codes d'activation au stockage de licences.

Étape 2. Sélection de l'environnement du Cloud

Sélectionnez le Cloud dans lequel vous déployez Kaspersky Security Center : AWS, Azure ou Google Cloud.

Étape 3. Autorisation dans le cloud

AWS

Confirmez lors de cette étape que vous possédez un rôle IAM doté des privilèges nécessaires ou octroyez à Kaspersky Security Center une clé d'accès AWS IAM. Sans rôle IAM ou clé d'accès AWS IAM, il est impossible de sonder les segments dans le Cloud.

Définissez les paramètres suivants de la connexion qui interviendra à l'avenir dans le sondage du segment dans le Cloud :

- **Nom de la connexion**

  Saisissez un nom pour la connexion. Le nom ne peut pas contenir plus de 256 caractères. Seuls les caractères Unicode sont admis.

  Ce nom servira aussi pour le groupe d'administration des appareils dans le cloud.

  Si vous prévoyez de travailler avec plusieurs environnements Cloud, vous pourriez inclure le nom de l'environnement dans le nom de la connexion, par exemple, " Segment Azure ", " Segment AWS " ou " Segment Google ".

- **Utiliser le rôle AWS IAM**

  Sélectionnez cette option, si vous avez déjà créé un rôle IAM pour l'utilisation du Serveur d'administration avec les services AWS.

- **Utiliser le compte utilisateur AWS IAM**

  Choisissez cette option, si vous avez un compte utilisateur IAM doté des privilèges requis et si vous pouvez saisir l'identifiant de la clé et la clé secrète.

  - **ID de clé d'accès**

    L'ID de clé d'accès IAM est une suite de caractères alphanumériques. Vous avez reçu l'ID de clé lors de la création du compte utilisateur IAM.

    Ce champ est accessible si vous avez opté pour l'autorisation à l'aide d'une clé d'accès AWS IAM et non pas d'un rôle IAM.

  - **Clé secrète**

    La clé secrète que vous avez reçue avec l'ID de clé d'accès quand vous avez créé le compte utilisateur IAM.

    Les caractères de la clé secrète s'affichent sous la forme d'astérisques. Après que vous avez commencé à saisir la clé secrète, le bouton **Afficher** apparaît. Cliquez sur ce bouton pendant le temps qu'il vous faut pour consulter les caractères saisis.

    Ce champ est accessible si vous avez opté pour l'autorisation à l'aide d'une clé d'accès AWS IAM et non pas d'un rôle IAM.

La connexion sera enregistrée dans les paramètres de l'application. Vous ne pouvez créer qu'une seule clé d'accès AWS IAM avec la configuration de l'environnement cloud. Par la suite, vous pouvez indiquer d'autres connexions pour l'administration d'autres segments dans le Cloud.

Si vous voulez installer les applications sur les instances via Kaspersky Security Center, il faut que votre rôle IAM (ou l'utilisateur IAM dont le compte utilisateur correspond à la clé que vous avez saisie) possède les autorisations requises.

Azure

Si vous avez choisi Azure, configurez les paramètres suivants de la connexion qui interviendra à l'avenir dans le sondage du segment dans le Cloud :

- **Nom de la connexion**

  Saisissez un nom pour la connexion. Le nom ne peut pas contenir plus de 256 caractères. Seuls les caractères Unicode sont admis.

  Ce nom servira aussi pour le groupe d'administration des appareils dans le cloud.

  Si vous prévoyez de travailler avec plusieurs environnements Cloud, vous pourriez inclure le nom de l'environnement dans le nom de la connexion, par exemple, « Segment Azure », « Segment AWS » ou « Segment Google ».

- **ID de l'application Azure**

  Vous avez créé cet identifiant de l'application sur le portail Azure.

  Vous pouvez fournir un identifiant de l'application Azure pour le sondage et d'autres fins. Si vous souhaitez sonder un autre segment Azure, il faut d'abord supprimer la connexion Azure existante.

- **Identifiant de l'abonnement Azure**

  Vous avez créé l'abonnement sur le portail Azure.

- **Mot de passe de l'application Azure**

  Vous avez obtenu le mot de passe de l'identifiant de l'application quand vous avez créé celui-ci.

  Les caractères de la mot de passe s'affichent sous la forme d'astérisques. Après que vous avez commencé à saisir le mot de passe, le bouton **Afficher** apparaît. Maintenez ce bouton enfoncé pour voir les caractères saisis.

- **Nom du compte du stockage Azure**

  Vous avez créé le nom du Compte du stockage Azure pour utiliser Kaspersky Security Center.

- **Clé d'accès au stockage Azure**

  Vous avez reçu un mot de passe (une clé) lorsque vous avez créé le compte du stockage Azure pour utiliser Kaspersky Security Center.

  La clé est disponible dans la section " Aperçu du compte du stockage Azure ", dans la sous-section " Clés ".

La connexion sera enregistrée dans les paramètres de l'application.

Google Cloud

Si vous avez choisi Google Cloud, configurez les paramètres suivants de la connexion qui interviendra à l'avenir dans le sondage du segment dans le Cloud :

- **Nom de la connexion**

  Saisissez un nom pour la connexion. Le nom ne peut pas contenir plus de 256 caractères. Seuls les caractères Unicode sont admis.

  Ce nom servira aussi pour le groupe d'administration des appareils dans le cloud.

  Si vous prévoyez de travailler avec plusieurs environnements Cloud, vous pourriez inclure le nom de l'environnement dans le nom de la connexion, par exemple, « Segment Azure », « Segment AWS » ou « Segment Google ».

- **Email client**

  L'email client est l'adresse email que vous avez utilisée pour enregistrer votre projet sur Google Cloud.

- **Identifiant du projet**

  L'identifiant du projet est l'identifiant que vous avez reçu lors de l'enregistrement de votre projet sur Google Cloud.

- **Clé privée**

  La clé privée est la séquence de caractères que vous avez reçue comme clé privée lors de l'enregistrement de votre projet sur Google Cloud. Envisagez de copier et coller cette séquence pour éviter les erreurs.

La connexion sera enregistrée dans les paramètres de l'application.

Étape 4. Configuration de la synchronisation avec Cloud et détermination des étapes à suivre

Cette étape marque le début du sondage des segments dans le Cloud et la création d'un groupe d'administration spécial pour les instances. Les instances trouvées lors du sondage sont placées dans ce groupe. C'est ici aussi que vous allez programmer le sondage du segment dans le Cloud (par défaut, toutes les 5 minutes).

La règle de déplacement automatique **Synchronisation avec Cloud** est créée à cette étape. À chaque analyse ultérieur du réseau Cloud, les appareils virtuels détectés sont déplacés dans le sous-groupe correspondant au sein du groupe **Appareils administrés\Cloud**.

Sur la page **Synchronisation avec le segment dans le cloud**, vous pouvez définir les paramètres suivants :

- **&Synchronisez la structure du groupe d'administration avec le segment dans le cloud**

  Quand cette option est activée, le groupe **Cloud** est créé automatiquement dans le groupe **Appareils administrés** et la Recherche d'appareils dans le Cloud démarre. Les machines virtuelles détectées à chaque analyse du réseau Cloud sont déplacées dans le groupe Cloud. La structure des sous-groupes d'administration au sein de ce groupe correspond à la structure de votre segment dans le Cloud (dans AWS, les zones d'accessibilité et les groupes de déplacement ne sont pas représentés dans la structure dans Azure, les sous-réseaux ne sont pas représentés dans la structure). Les appareils qui ne sont pas identifiés en tant qu'instances dans le Cloud se trouvent dans le groupe **Appareils non définis**. Cette structure de groupes permet d'installer les applications antivirus sur les instances à l'aide des tâches d'installation de groupe et de configurer de différentes stratégies pour différents groupes.

  Quand l'option est désactivée, le groupe **Cloud** est aussi créé et une recherche d'appareil est lancée toutefois, les sous-groupes qui correspondent à la structure du segment dans le Cloud ne sont pas créés au sein du groupe. Toutes les instances détectées se trouvent dans le groupe d'administration **Cloud** et s'affichent dans une liste commune. Si lors de l'utilisation de Kaspersky Security Center, vous devez effectuer une synchronisation, vous pourrez modifier les propriétés de la règle **Synchronisation avec Cloud** et la forcer. Le forcement de la règle reconstruit la structure des groupes à l'intérieur du groupe Cloud de manière à ce qu'elle corresponde à la structure de votre segment dans le Cloud.

  Cette option est Inactif par défaut.

- **Déployer la protection**

  Quand cette option est sélectionnée, l'Assistant crée une tâche d'installation d'applications de sécurité sur les instances. La fin de l'assistant est automatiquement suivie du lancement de l'assistant de déploiement de la protection sur vos segments dans le Cloud, et vous pouvez installer sur celles-ci l'Agent d'administration et les applications de sécurité.

  Kaspersky Security Center peut réaliser le déploiement à l'aide de ses propres outils. Si vous n'avez pas les permissions pour installer les applications sur les instances EC2 ou les machines virtuelles Azure, vous pouvez configurer la tâche **Installation à distance** manuellement et précisez un compte disposant des permissions requises. Dans ce cas, la tâche Installation à distance ne fonctionnera pas pour les appareils détectés par l'API d'AWS ou Azure. Cette tâche fonctionne uniquement pour les appareils détectés à l'aide du sondage Active Directory, du sondage des domaines Windows ou du sondage des plages IP.

  Si cette option n'est pas sélectionnée, l'Assistant de déploiement de la protection ne démarre pas et la création des tâches d'installation des applications de sécurité sur les instances n'a pas lieu. Vous pouvez réaliser ces deux opérations manuellement plus tard.

Pour Google Cloud, vous ne pouvez effectuer le déploiement qu'avec les outils natifs de Kaspersky Security Center. Si vous avez sélectionné Google Cloud, l'option **Déployer la protection** n'est pas disponible.

Étape 5. Configuration de Kaspersky Security Network dans l'environnement Cloud

Indiquer les paramètres du transfert des informations sur le fonctionnement de Kaspersky Security Center dans la base de connaissances de Kaspersky Security Network. Sélectionnez l'une des options ci-dessous :

- **J'accepte les termes du Kaspersky Security Network**

  Kaspersky Security Center et les applications administrées installées sur les appareils client transfèrent automatiquement les détails de leurs opérations à Kaspersky Security Network. La coopération avec Kaspersky Security Network garantit une mise à jour plus rapide des bases de données sur les virus et les menaces, ce qui améliore la vitesse de réaction face aux menaces naissantes.

- **Je refuse les termes du Kaspersky Security Network**

  Kaspersky Security Center et les applications administrées ne fourniront aucune information à Kaspersky Security Network.

  Si vous sélectionnez cette option, l'utilisation de Kaspersky Security Network sera désactivée.

Kaspersky recommande la participation au Kaspersky Security Network.

Étape 6. Configuration des notifications par Email dans l'environnement Cloud

Configurez l'envoi des notifications sur les événements enregistrés lors du fonctionnement des applications de Kaspersky sur les appareils clients virtuels. Ces paramètres seront utilisés comme paramètres par défaut pour les stratégies d'applications.

Pour configurer la diffusion des notifications relatives aux événements qui surviennent dans les applications de Kaspersky, utilisez les paramètres suivants :

- **Destinataire (adresses email)**

  Les adresses email des utilisateurs auxquels l'application va envoyer les notifications. Vous pouvez entrer une ou plusieurs adresse(s). Si vous entrez plusieurs adresses, séparez-les par un point-virgule.

- **Serveurs SMTP**

  L'adresse ou les adresses des serveurs de messagerie de votre organisation.

  Si vous entrez plusieurs adresses, séparez-les par un point-virgule. Vous pouvez utiliser les valeurs suivantes du paramètre :

  - Adresse IPv4 ou IPv6
  - Nom de réseau Windows (nom NetBIOS) de l'appareil
  - Nom complet du serveur SMTP

- **Port du serveur SMTP**

  Numéro du port de communication du serveur SMTP. Si vous utilisez plusieurs serveurs SMTP, la connexion à ceux-ci est établie via le port de communication indiqué. Le numéro de port par défaut est 25.

- **Utiliser l'authentification ESMTP**

  Activation de la prise en charge de l'authentification ESMTP. Après avoir coché la case, dans les champs **Nom d'utilisateur** et **Mot de passe**, vous pouvez définir les paramètres d'authentification ESMTP. Celle-ci est décochée par défaut.

Vous pouvez vérifier les paramètres définis pour l'envoi des notifications par email à l'aide du bouton **Envoyer un message d'essai**. Si le message d'essai est bien remis aux adresses reprises dans le champ **Destinataires (adresses email)**, cela signifie que la configuration est correcte.

Étape 7. Création d'une configuration initiale pour la protection de l'environnement Cloud

A cette étape, Kaspersky Security Center crée automatiquement des stratégies et des tâches. La fenêtre **Création de la configuration initiale de la protection** affiche une liste des tâches et des stratégies créées par l'application.

Si vous utilisez une base de données RDS dans le Cloud AWS, il faut fournir une paire de clé d'accès IAM à Kaspersky Security Center lors de la création de la tâche de sauvegarde du certificat du Serveur d'administration. Dans ce cas, remplissez les champs suivants :

- **Nom du compartiment S3**

  Le nom du compartiment S3 que vous avez créé pour la Sauvegarde.

- **ID de clé d'accès**

  Vous avez reçu l'ID de clé (séquence de caractères alphanumériques) lorsque vous avez créé le compte utilisateur IAM pour travailler avec l'instance de stockage du seau S3.

  Le champ est disponible si vous avez sélectionné la base de données RDS sur un seau S3.

- **Clé secrète**

  La clé secrète que vous avez reçue avec l'ID de clé d'accès quand vous avez créé le compte utilisateur IAM.

  Les caractères de la clé secrète s'affichent sous la forme d'astérisques. Après que vous avez commencé à saisir la clé secrète, le bouton **Afficher** apparaît. Cliquez sur ce bouton pendant le temps qu'il vous faut pour consulter les caractères saisis.

  Ce champ est accessible si vous avez opté pour l'autorisation à l'aide d'une clé d'accès AWS IAM et non pas d'un rôle IAM.

Si vous utilisez une bases de données Azure SQL dans l'environnement Cloud Azure, il faut fournir les informations à votre serveur SQL Azure à Kaspersky Security Center lors de la création de la tâche de sauvegarde du certificat du Serveur d'administration. Dans ce cas, remplissez les champs suivants :

- **Nom du compte du stockage Azure**

  Vous avez créé le nom du Compte du stockage Azure pour utiliser Kaspersky Security Center.

- **Identifiant de l'abonnement Azure**

  Vous avez créé l'abonnement sur le portail Azure.

- **Mot de passe de l'application Azure**

  Vous avez obtenu le mot de passe de l'identifiant de l'application quand vous avez créé celui-ci.

  Les caractères de la mot de passe s'affichent sous la forme d'astérisques. Après que vous avez commencé à saisir le mot de passe, le bouton **Afficher** apparaît. Maintenez ce bouton enfoncé pour voir les caractères saisis.

- **ID de l'application Azure**

  Vous avez créé cet identifiant de l'application sur le portail Azure.

  Vous pouvez fournir un identifiant de l'application Azure pour le sondage et d'autres fins. Si vous souhaitez sonder un autre segment Azure, il faut d'abord supprimer la connexion Azure existante.

- **Nom du serveur SQL Azure**

  Le nom et le groupe de ressources sont disponibles dans les propriétés du Serveur Azure SQL

- **Groupe de ressources du serveur SQL Azure**

  Le nom et le groupe de ressources sont disponibles dans les propriétés du Serveur Azure SQL

- **Clé d'accès au stockage Azure**

  Disponible dans les propriétés de votre compte de stockage, dans la sections Clés d'accès. Vous pouvez utiliser n'importe quelle clé (clé1 ou clé2).

Si vous déployez le Serveur d'administration dans Google Cloud, vous devez sélectionner un dossier dans lequel les copies de sauvegarde seront stockées. Sélectionnez un dossier sur votre appareil local ou un dossier sur une instance de machine virtuelle.

Le bouton **Suivant** est disponible après la création de l'ensemble des tâches et des stratégies indispensables à la configuration minimale de la protection.

Si un appareil sur lequel les tâches sont censées être exécutées n'est pas visible pour le Serveur d'administration, les tâches débutent uniquement lorsque l'appareil devient visible. Quand vous avez créé une instance EC2 ou une machine virtuelle Azure, celle devient visible pour le Serveur d'administration au bout d'un certain temps. Si vous voulez que l'Agent d'administration et les applications de sécurité soient installés sur tous les nouveaux appareils dès que possible, assurez-vous que l'option **Lancer les tâches non exécutées** est activée pour les tâches **Installation à distance d'une application**. Dans le cas contraire, une nouvelle instance/machine virtuelle n'obtiendra pas l'Agent d'administration et les applications de sécurité avant le lancement de la tâche selon sa programmation.

Étape 8. Sélection de l'action si le système d'exploitation doit être redémarré pendant l'installation (pour l'environnement Cloud)

Si vous avez déjà sélectionné **Déployer la protection**, vous devez choisir ce qu'il faut faire lorsque le système d'exploitation d'un dispositif cible doit être redémarré. Si vous n'avez pas sélectionné l'option **Déployer la protection**, cette étape est ignorée.

Sélectionnez s'il faut ou non redémarrer l'appareil si le système d'exploitation doit être redémarré pendant l'installation des applications :

- **Ne pas redémarrer l'appareil**

  Si cette option a été sélectionnée, l'appareil ne sera pas redémarré après l'installation de l'application de sécurité.

- **Redémarrer l'appareil**

  Si cette option a été sélectionnée, l'appareil sera redémarré après l'installation de l'application de sécurité.

Si vous voulez forcer la fermeture de toutes les applications dans les sessions bloquées sur les instances avant le redémarrage, cochez la case **Forcer la fermeture des applications dans les sessions bloquées**. Si la case n'est pas cochée, il faudra fermer manuellement toutes les applications en cours d'exécution sur les instances bloquées.

Étape 9. Réception des mises à jour par le Serveur d'administration

Cette étape présente la progression du chargement des mises à jour indispensables au fonctionnement correct du Serveur d'administration. Vous pouvez cliquer sur le bouton **Suivant** sans attendre la fin du chargement pour passer à la dernière page de l'Assistant.

L'Assistant se termine.

Contrôle de réussite de la configuration

Pour confirmer que Kaspersky Security Center 15.1 est configuré pour fonctionner correctement dans le Cloud, procédez comme suit :

1. Lancez Kaspersky Security Center et confirmez que vous pouvez vous connecter au Serveur d'administration via la Console d'administration.

2. Dans l'arborescence de la console, sélectionnez **Appareils administrés\Cloud**.

3. Lors de la consultation d'un sous-groupe quelconque au sein du groupe **Appareils administrés\Cloud**, assurez-vous que l'onglet **Appareils** affiche tous les Appareils de ce sous-groupe.

   Si les appareils ne sont pas affichés, vous pouvez sonder les segments dans le Cloud correspondant manuellement pour les trouver.

4. Assurez-vous que sous l'onglet **Stratégies**, des stratégies actives soient activées pour les applications suivantes :

   - Agent d'administration de Kaspersky Security Center
   - Kaspersky Security for Windows Server
   - Kaspersky Endpoint Security for Linux

   Si elles ne figurent pas dans la liste, vous pouvez les créer manuellement.

5. Assurez-vous que sous l'onglet **Tâches** figurent les tâches suivantes :

   - **Sauvegarde des données du Serveur d'administration**
   - **Tâche de mise à jour pour Windows Server**
   - **Maintenance du Serveur d'administration**
   - **Télécharger les mises à jour dans le stockage du serveur d'administration**
   - **Recherche de vulnérabilités et de mises à jour requises**
   - **Installer la protection pour Windows**
   - **Installer la protection pour Linux**
   - **Tâche d'analyse rapide pour Windows Server**
   - **Analyse rapide**
   - **Installer la Mise à jour pour Linux**

   Si elles ne figurent pas dans la liste, vous pouvez les créer manuellement.

Kaspersky Security Center 15.1 est configuré pour fonctionner correctement dans l'environnement Cloud, procédez comme suit.

Groupe d'appareils Cloud

Vous pouvez gérer les appareils cloud en les combinant en groupes. A l'étape de la configuration initiale de Kaspersky Security Center, le groupe d'administration **Appareils administrés\Cloud**, qui reprend les appareils du Cloud détectés lors du sondage, est créé par défaut.

Si vous avez sélectionné l'option **&Synchronisez la structure du groupe d'administration avec le segment dans le cloud** lors de la configuration de la synchronisation, la structure des sous-groupes au sein de ce groupe d'administration est identique à la structure de vos segments dans le Cloud. (Toutefois, dans AWS, les zones d'accessibilité et les groupes de placement ne sont pas représentés dans la structure ; dans Microsoft Azure, les sous-réseaux ne sont pas représentés dans la structure.) Les sous-groupes qui se vident à l'intérieur du groupe et qui sont détectés lors du sondage sont supprimés automatiquement.

Vous pouvez également créer vous-même des groupes d'administration qui réunissent touts les appareils ou un ensemble d'appareils.

Par défaut, le groupe **Appareils administrés\Cloud** hérite des stratégies et des tâches du groupe **Appareils administrés**. Vous pouvez modifier les configurations des paramètres si les case **La modification est autorisée** ont été cochées dans les propriétés des paramètres des stratégies et des tâches correspondantes.

Sondage du segment dans le cloud

Le Serveur d'administration reçoit les informations sur la structure du réseau et les appareils qui en font partie au cours des sondages réguliers des segments dans le Cloud à l'aide des outils de l'API d'AWS, de l'API d'Azure et de l'API de Google. Kaspersky Security Center utilise ces informations pour mettre à jour le contenu des dossiers **Appareils non définis** et **Appareils administrés**. Si vous avez configuré le déplacement automatique des appareils dans les groupes d'administration, les appareils détectés sont inclus dans les groupes d'administration.

Pour que le Serveur d'administration puisse sonder les segments dans le Cloud, vous devez posséder les privilèges fournis avec un rôle IAM ou le compte utilisateur IAM (dans AWS) ou avec l'ID de l'application et le mot de passe (dans Azure) ou avec un e-mail client de Google, un identifiant de projet Google et une clé privée.

Vous pouvez ajouter et supprimer des connexions, ainsi que configurer une programmation du sondage pour chaque segment dans le Cloud.

Ajout de connexions pour le sondage des segments dans le Cloud

Pour ajouter une connexion pour le sondage des segments dans le Cloud à la liste des connexions disponibles, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez l'entrée **Recherche d'appareils → Cloud**.
2. Dans l'espace de travail de la fenêtre, cliquez sur **Configurer les paramètres du sondage**.

   Une fenêtre de propriétés reprenant la liste des connexions utilisées pour le sondage des segments dans le Cloud s'ouvre.
3. Cliquez sur le bouton **Ajouter**.

   La fenêtre **Connexion** s'ouvre.

4. Définissez le nom de l'environnement Cloud de la connexion qui interviendra à l'avenir dans le sondage des segments dans le Cloud :

   Cloud

   L'environnement dans lequel les instances EC2 (ou les machines virtuelles) sont situées peut être Amazon Web Services (AWS), Microsoft Azure ou Google Cloud.

   Si vous avez sélectionné AWS, spécifiez les paramètres suivants :

   - **Nom de la connexion**

     Saisissez un nom pour la connexion. Le nom ne peut pas contenir plus de 256 caractères. Seuls les caractères Unicode sont admis.

     Ce nom servira aussi pour le groupe d'administration des appareils dans le cloud.

     Si vous prévoyez de travailler avec plusieurs environnements Cloud, vous pourriez inclure le nom de l'environnement dans le nom de la connexion, par exemple, " Segment Azure ", " Segment AWS " ou " Segment Google ".

   - **Utiliser le rôle AWS IAM**

     Sélectionnez cette option, si vous avez déjà créé un rôle IAM pour l'utilisation du Serveur d'administration avec les services AWS.

   - **Utiliser le compte utilisateur AWS IAM**

     Choisissez cette option, si vous avez un compte utilisateur IAM doté des privilèges requis et si vous pouvez saisir l'identifiant de la clé et la clé secrète.

     - **ID de clé d'accès**

       L'ID de clé d'accès IAM est une suite de caractères alphanumériques. Vous avez reçu l'ID de clé lors de la création du compte utilisateur IAM.

       Ce champ est accessible si vous avez opté pour l'autorisation à l'aide d'une clé d'accès AWS IAM et non pas d'un rôle IAM.

     - **Clé secrète**

       La clé secrète que vous avez reçue avec l'ID de clé d'accès quand vous avez créé le compte utilisateur IAM.

       Les caractères de la clé secrète s'affichent sous la forme d'astérisques. Après que vous avez commencé à saisir la clé secrète, le bouton **Afficher** apparaît. Cliquez sur ce bouton pendant le temps qu'il vous faut pour consulter les caractères saisis.

       Ce champ est accessible si vous avez opté pour l'autorisation à l'aide d'une clé d'accès AWS IAM et non pas d'un rôle IAM.

   L'Assistant de configuration pour une utilisation dans le Cloud ne permet d'indiquer qu'une seule clé d'accès AWS IAM. Par la suite, vous pouvez indiquer d'autres connexions pour l'administration d'autres segments dans le Cloud.

Si vous avez sélectionné Azure, spécifiez les paramètres suivants :

- **Nom de la connexion**

  Saisissez un nom pour la connexion. Le nom ne peut pas contenir plus de 256 caractères. Seuls les caractères Unicode sont admis.

  Ce nom servira aussi pour le groupe d'administration des appareils dans le cloud.

  Si vous prévoyez de travailler avec plusieurs environnements Cloud, vous pourriez inclure le nom de l'environnement dans le nom de la connexion, par exemple, « Segment Azure », « Segment AWS » ou « Segment Google ».

- **ID de l'application Azure**

  Vous avez créé cet identifiant de l'application sur le portail Azure.

  Vous pouvez fournir un identifiant de l'application Azure pour le sondage et d'autres fins. Si vous souhaitez sonder un autre segment Azure, il faut d'abord supprimer la connexion Azure existante.

- **Identifiant de l'abonnement Azure**

  Vous avez créé l'abonnement sur le portail Azure.

- **Mot de passe de l'application Azure**

  Vous avez obtenu le mot de passe de l'identifiant de l'application quand vous avez créé celui-ci.

  Les caractères de la mot de passe s'affichent sous la forme d'astérisques. Après que vous avez commencé à saisir le mot de passe, le bouton **Afficher** apparaît. Maintenez ce bouton enfoncé pour voir les caractères saisis.

- **Nom du compte du stockage Azure**

  Vous avez créé le nom du Compte du stockage Azure pour utiliser Kaspersky Security Center.

- **Clé d'accès au stockage Azure**

  Vous avez reçu un mot de passe (une clé) lorsque vous avez créé le compte du stockage Azure pour utiliser Kaspersky Security Center.

  La clé est disponible dans la section « Aperçu du compte du stockage Azure », dans la sous-section « Clés ».

Si vous avez sélectionné Google Cloud, spécifiez les paramètres suivants :

- **Nom de la connexion**

Saisissez un nom pour la connexion. Le nom ne peut pas contenir plus de 256 caractères. Seuls les caractères Unicode sont admis.

Ce nom servira aussi pour le groupe d'administration des appareils dans le cloud.

Si vous prévoyez de travailler avec plusieurs environnements Cloud, vous pourriez inclure le nom de l'environnement dans le nom de la connexion, par exemple, « Segment Azure », « Segment AWS » ou « Segment Google ».

- **Email client**

  L'email client est l'adresse email que vous avez utilisée pour enregistrer votre projet sur Google Cloud.

- **Identifiant du projet**

  L'identifiant du projet est l'identifiant que vous avez reçu lors de l'enregistrement de votre projet sur Google Cloud.

- **Clé privée**

  La clé privée est la séquence de caractères que vous avez reçue comme clé privée lors de l'enregistrement de votre projet sur Google Cloud. Envisagez de copier et coller cette séquence pour éviter les erreurs.

5. Le cas échéant, sélectionnez **Configurer la programmation du sondage** et modifiez les paramètres par défaut.

   La connexion est enregistrée dans les paramètres de l'application.

Après le premier sondage du nouveau segment dans le Cloud, le sous-groupe qui correspond à ce segment apparaît dans le groupe d'administration **Appareils administrés\Cloud**.

Si vous utilisez des identifiants incorrects, aucune instance ne sera détectée lors du sondage des segments dans le Cloud et le nouveau sous-groupe n'apparaîtra pas dans le groupe d'administration **Appareils administrés\Cloud**.

Suppression de connexions pour le sondage des segments dans le Cloud

Si vous n'avez plus besoin de sonder un segment dans le Cloud, vous pouvez supprimer la connexion qui correspond à celui-ci dans la liste des connexions disponibles. Vous pouvez également supprimer la connexion si, par exemple, les droits de sondage du segment dans le Cloud ont été transmis à un autre utilisateur AWS IAM utilisant une autre clé.

Pour supprimer une connexion, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez l'entrée **Recherche d'appareils → Cloud**.
2. Dans l'espace de travail de la fenêtre, sélectionnez l'option **Configurer les paramètres du sondage**.

   Une fenêtre reprenant la liste des connexions utilisées pour le sondage des segments dans le Cloud s'ouvre.

3. Sélectionnez la connexion que vous voulez supprimer puis, cliquez sur le bouton **Supprimer** dans la partie droite de la fenêtre.

4. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **OK** pour confirmer votre choix.

Si vous supprimez une connexion de la liste des connexions disponibles, les Appareil situées dans les segments correspondants sont automatiquement supprimées du groupe d'administration correspondant.

Configuration de la programmation du sondage

Le sondage du segment dans le Cloud est programmé. Vous pouvez définir la fréquence du sondage.

La fréquence de sondage est automatiquement définie sur 5 minutes dans les paramètres de configuration de l'environnement cloud. Vous pouvez modifier cette valeur à tout moment. Toutefois, il est déconseillé de réaliser un sondage à une fréquence supérieure à 5 minutes, car cela pourrait provoquer des erreurs dans le fonctionnement de l'API.

Pour configurer la programmation du sondage du segment dans le Cloud, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez l'entrée **Recherche d'appareils → Cloud**.

2. Dans l'espace de travail, cliquez sur **Configurer les paramètres du sondage**.

   La fenêtre de propriétés du Cloud s'affiche.

3. Dans la liste, sélectionnez la connexion que vous souhaitez, puis cliquez sur le bouton **Propriétés**.

   La fenêtre de propriétés de la connexion s'affiche.

4. Dans la fenêtre des propriétés, cliquez sur le lien **Configurer la programmation du sondage**.

   La fenêtre **Programmation** s'ouvrira.

5. Configurez les paramètres suivants :

- **Programmation**

  Options de programmation du sondage :

  - Tous les N jours

    Le sondage s'exécute régulièrement, selon l'intervalle défini en jours, à partir de la date et heure définis.

    Le sondage s'exécute par défaut chaque jour, à partir de la date et de l'heure actuelle du système.

  - Toutes les N minutes

    Le sondage s'exécute régulièrement, selon l'intervalle défini en minutes, à partir de l'heure définie.

    Le sondage s'exécute par défaut toutes les cinq minutes, à partir de l'heure actuelle du système.

  - Selon les jours de la semaine

    Le sondage s'exécute régulièrement les jours définis de la semaine, à l'heure indiquée.

    Par défaut, le sondage s'exécute chaque vendredi à 18h00.

  - Mensuellement, les jours indiqués des semaines sélectionnées

    Le sondage s'exécute régulièrement les jours définis de chaque mois, à l'heure indiquée.

    Par défaut, aucun jour du mois n'est sélectionné. L'heure de lancement par défaut est 18h00.

- Lancer les tâches non exécutées

  Si le Serveur d'administration est éteint ou s'il n'est pas disponible au moment auquel le sondage a été programmé, le Serveur d'administrateur peut soit lancer le sondage immédiatement après que le Serveur d'administration a été allumé ou attendre la prochaine programmation du sondage.

  Si cette option est activée, le Serveur d'administration lance le sondage directement après qu'il a été allumé.

  Si cette option est désactivée, le Serveur d'administration attend la prochaine programmation du sondage.

  Cette option est activée par défaut.

6. Cliquez sur le bouton **OK** afin d'enregistrer les modifications.

La programmation du sondage est configurée et enregistrée.

Installation des applications sur les appareils dans le Cloud

Vous pouvez installer les applications antivirus de Kaspersky suivante sur les appareils dans le Cloud : Kaspersky Security for Windows Server (pour les appareils Windows) et Kaspersky Endpoint Security for Linux (pour les appareils Linux).

Les appareils client sur lesquels vous allez installer la protection doivent répondre à la configuration définie pour l'utilisation de Kaspersky Security Center dans le Cloud. Vous devez disposer d'une licence valide pour installer des applications sur des instances AWS, des machines virtuelles Microsoft Azure ou des instances de machines virtuelles Google.

Kaspersky Security Center 15.1 prend en charge les scénarios suivants :

- Un appareil client est découvert par le biais d'une API ; l'installation est également réalisée par le biais d'une API. Pour les environnements cloud AWS et Azure, ce scénario est pris en charge.
- Un appareil client est découvert par le sondage Active Directory, le sondage des domaines Windows ou des plages IP l'installation est réalisée à l'aide de Kaspersky Security Center.
- Un appareil client est découvert par le biais de l'API Google ; l'installation est réalisée par le biais de Kaspersky Security Center. Pour Google Cloud, seul ce scénario est pris en charge.

Les autres méthodes d'installation des applications ne sont pas prises en charge.

Pour l'installation des applications sur les appareils virtuels, utilisez les paquets d'installation.

Pour créer une tâche d'installation à distance de l'application sur des instances à l'aide des outils AWS API, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le dossier **Tâches**.
2. Cliquez sur le bouton **Nouvelle tâche**.

   Ceci permet de lancer l'Assistant de création d'une tâche. Suivez les instructions de l'assistant.
3. Sur la page **Sélection du type de tâche**, sélectionnez **Installation à distance d'une application** comme type de tâche.

4. Sur la page **Sélection d'appareils**, choisissez les appareils nécessaires dans le groupe **Appareils administrés\Cloud**.

5. Si aucun Agent d'administration n'est installé sur les appareils sur lesquels vous avez l'intention d'installer l'application, dans la page **Sélection du compte utilisateur pour exécuter la tâche**, sélectionnez **Compte utilisateur requis (&Agent d'administration non utilisé)**, puis cliquez sur le bouton **Ajouter** dans la partie droite de la fenêtre. Dans le menu qui s'ouvre, choisissez :

   - **Compte utilisateur cloud**

     Sélectionnez cette option si vous souhaitez installer des applications sur les instances dans l'environnement AWS et si vous possédez une clé d'accès AWS IAM avec les permissions requises, mais que vous n'avez pas de rôle IAM. Sélectionnez également cette option si vous souhaitez installer des applications sur les appareils dans l'environnement Azure.

     Si vous avez choisi l'option Clé d'accès IAM AWS, attribuez à Kaspersky Security Center dans la fenêtre qui s'ouvre une clé qui autorise l'installation de l'application sur les appareils dont vous avez besoin.

     Sélectionnez le cloud : AWS ou Azure.

     Dans le champ **Nom du compte utilisateur**, saisissez un nom pour ces identifiants. Ce nom s'affichera dans la liste des comptes pour l'exécution de la tâche.

     Si vous avez sélectionné AWS, saisissez dans les champs **ID de clé d'accès** et **Clé secrète** les identifiants du compte utilisateur IAM autorisé à installer des applications sur les appareils désignés.

     Si vous avez sélectionné Azure, saisissez dans les champs **Identifiant de l'abonnement Azure** et **Mot de passe de l'application Azure** les identifiants du compte utilisateur IAM autorisé à installer des applications sur les appareils désignés.

     Si vous désignez des identifiants incorrects, la tâche d'installation à distance échouera sur les appareils pour lesquels elle avait été programmée.

   - **Compte utilisateur**

     Pour les instances qui exécutent Windows, sélectionnez cette option si vous n'avez pas l'intention d'installer l'application à l'aide des outils API d'AWS ou d'Azure. Dans ce cas, confirmez que les appareils dans votre segment dans le Cloud remplissent les conditions nécessaires. Kaspersky Security Center réalisera l'installation des applications par ses propres moyens, sans avoir recours à AWS API.

     Si vous désignez des données incorrectes, la tâche d'installation à distance échouera sur les appareils pour lesquels elle avait été programmée.

   - **Rôle IAM**

     Sélectionnez cette option si vous souhaitez installer des applications sur les instances dans l'environnement AWS et que vous possédez un rôle IAM avec les autorisations requises.

     Si vous sélectionnez cette option mais que vous ne possédez pas un rôle IAM avec les privilèges requis, la tâche d'installation à distance échouera sur une erreur sur les appareils pour lesquels elle a été programmée.

   - **Certificat SSH**

Pour les instances qui exécutent Linux, sélectionnez cette option si vous n'avez pas l'intention d'installer l'application à l'aide des outils API d'AWS ou d'Azure. Dans ce cas, confirmez que les appareils dans votre segment dans le Cloud remplissent les conditions nécessaires. Kaspersky Security Center réalisera l'installation des applications par ses propres moyens, sans avoir recours à AWS API.

Pour spécifier la clé privée du certificat SSH, vous pouvez la générer à l'aide de l'utilitaire ssh-keygen. Notez que Kaspersky Security Center prend en charge le format PEM des clés privées, mais que l'utilitaire ssh-keygen génère par défaut des clés SSH au format OPENSSH. Le format OPENSSH n'est pas pris en charge par Kaspersky Security Center. Pour créer une clé privée au format PEM pris en charge, ajoutez l'option `-m PEM` dans la commande ssh-keygen. Par exemple :

```
ssh-keygen -m PEM -t rsa -b 4096 -C "<user email>"
```

Vous pouvez octroyer plusieurs clés, en cliquant chaque fois sur **Ajouter**. Si différents segments dans le Cloud requièrent différents identifiants, fournissez les identifiants pour tous les segments.

Une fois que l'assistant a terminé, la tâche d'installation à distance de l'application apparaît dans la liste des tâches de l'espace de travail du dossier **Tâches**.

Dans Microsoft Azure, l'installation à distance des applications de sécurité sur une machine virtuelle peut entraîner la suppression de l'extension de script personnalisé sur cette machine virtuelle.

Affichage des propriétés des appareils du Cloud

Pour afficher les propriétés d'un appareil du Cloud, procédez comme suit :

1. Dans l'arborescence, à l'entrée **Recherche d'appareils** → **Cloud**, sélectionnez la sous-entrée qui correspond au groupe où se trouve l'instance qui vous intéresse.

   Si vous ne savez pas dans quel groupe se trouve l'appareil virtuel dont vous avez besoin, utilisez la fonction de recherche :

   a. Faites un clic doit sur le nom de l'entrée **Appareils administrés** → **Cloud**, puis sélectionnez **Rechercher** dans le menu contextuel.

   b. Dans la fenêtre qui s'ouvre, effectuez une recherche.

      S'il existe un appareil qui correspond aux critères saisis, son nom et les informations qui le concernent apparaissent dans la partie inférieure de la fenêtre.

2. Cliquez-droit sur le nom de l'entrée qui vous intéresse. Dans le menu contextuel, sélectionnez l'option **Propriétés**.

   Les propriétés de l'objet apparaissent dans la fenêtre qui s'ouvre.

   La section **System Info** → **Informations générales sur le système** contient les propriétés spécifiques pour les appareils dans le Cloud :

   - **Appareil découvert à l'aide de l'API** (**AWS**, **Azure** ou **Google Cloud** ; si l'appareil n'est pas détecté à l'aide de l'API, la valeur **Non** s'affiche).
   - **Région Cloud**.
   - **Cloud VPC** (pour les appareils AWS et Google Cloud uniquement).
   - **Zone de disponibilité Cloud** (pour les appareils AWS et Google Cloud uniquement).
   - **Sous-réseau Cloud**.
   - **Groupe de placement Cloud** (cette unité n'est affichée que si l'instance appartient à un groupe de placement ; dans le cas contraire, elle n'est pas affichée).

Le bouton **Exporter dans un fichier**, permet d'exporter ces informations dans un fichier csv ou txt.

Synchronisation avec le cloud

Pendant l'utilisation de la Configuration de l'environnement cloud, la règle Synchronisation avec Cloud est créée automatiquement. La règle permet de déplacer automatiquement les instances trouvées à chaque sondage depuis le groupe **Appareils non définis** vers le groupe **Appareils administrés\Cloud** pour que les instances soient accessibles à l'administration centralisée. La règle par défaut est activée une fois créée. Vous pouvez désactiver, modifier ou forcer une règle à tout moment.

Pour modifier les propriétés de la règle Synchronisation avec Cloud et / ou forcer une règle, procédez comme suit :

1. Dans l'arborescence de la console, effectuez un clic droit sur le nom de l'entrée **Recherche d'appareils**.
2. Dans le menu contextuel, sélectionnez l'option **Propriétés**.
3. Dans la fenêtre **Propriétés** qui s'ouvre, sélectionnez **Déplacer les appareils** dans le volet **Sections**.
4. Dans la liste des règles de déplacement des appareils dans l'espace de travail, choisissez **Synchronisation avec Cloud** et cliquez sur le bouton **Propriétés** dans le bas de la fenêtre.

   La fenêtre de propriétés de la règle s'affiche.

5. Le cas échéant, configurez les paramètres suivants dans le groupe de paramètres **Segments dans le Cloud** :

- L'appareil se trouve dans le segment dans le Cloud

  La règle s'applique uniquement aux appareils qui se trouvent dans le segment dans le Cloud sélectionné. Si la case est décochée, la règle s'applique à tous les appareils trouvés.

  Cette option est sélectionnée par défaut.

  - Objets enfants inclus

    Si la case est cochée, cette règle exécutée pour tous les appareils du segment choisi et dans toutes les sous-sections du Cloud. Dans le cas contraire, la règle s'applique uniquement aux appareils qui se trouvent dans le segment racine.

    Cette option est sélectionnée par défaut.

  - Déplacer les appareils des objets enfants vers les sous-groupes correspondants

    Si la case est Activé, les appareils des objets enfants sont déplacés dans les sous-groupes correspondant à leur structure.

    Si l'option est désactivée, les appareils des objets enfants sont déplacés dans la racine du sous-groupe AWS sans décomposition en sous-groupes.

    Cette option est activée par défaut.

    - Créer des sous-groupes qui correspondent aux conteneurs des appareils détectés pour la première fois.

      Quand cette option est activée, quand la structure du groupe **Appareils administrés\Cloud** ne contient aucun sous-groupe correspondant à la section qui contient l'appareil, Kaspersky Security Center crée ces sous-groupes. Par exemple, si un nouveau sous-réseau est découvert pendant la Recherche d'appareils, un nouveau groupe portant le même nom est créé dans le groupe **Appareils administrés\Cloud**.

      Si cette option est désactivée, Kaspersky Security Center ne crée aucun nouveau sous-groupe. Par exemple, si un nouveau sous-réseau est découvert lors du sondage du réseau, un nouveau groupe portant le même nom ne sera pas créé dans le groupe **Appareils administrés\Cloud** et les appareils qui se trouve dans ce sous-réseau seront déplacés vers le groupe **Appareils administrés\Cloud**.

      Cette option est activée par défaut.

    - Supprimer les sous-groupes n'ayant pas de correspondance dans les segments dans le Cloud

      Si cette option est activée, l'application supprime du groupe Cloud tous les sous-groupes qui ne correspondent à aucun objet dans le cloud.

      Si cette option est désactivée, les sous-groupes qui ne correspondent à aucun objet dans le Cloud sont conservés.

      Cette option est activée par défaut.

Si à l'étape d'exécution de la Configuration de l'environnement cloud, vous avez activé l'option **Synchronisation avec Cloud**, la règle Synchronisation avec Cloud est créée avec les cases **Créer les sous-groupes correspondants aux conteneurs des nouveaux appareils** détectés et **Supprimer les sous-groupes sans correspondance dans les segments du Cloud** cochées.

Si vous n'avez pas activé l'option **Synchronisation avec Cloud**, la règle Synchronisation avec Cloud est créée avec les cases décochées. Si l'utilisation de Kaspersky Security Center nécessite que la structure des sous-groupes à l'intérieur du sous-groupe **Appareils administrés\Cloud** corresponde à la structure des segments dans le Cloud, activez les options **Créer les sous-groupes correspondants aux conteneurs des nouveaux appareils détectés** et **Supprimer les sous-groupes sans correspondance dans les segments du Cloud** dans les propriétés de la règle et forcez la règle.

6. Sélectionnez la valeur dans la liste déroulante **Appareil détecté par l'API** :
   - **AWS**. L'appareil est détecté via l'utilisation de l'API AWS, autrement dit, l'appareil est bel et bien dans l'environnement cloud AWS.
   - **Azure**. L'appareil est détecté via l'utilisation de l'API Azure, autrement dit, l'appareil est bel et bien dans l'environnement cloud Azure.
   - **Google Cloud.** L'appareil est détecté via l'utilisation de l'API Google, autrement dit, l'appareil est bel et bien dans le cloud Google.
   - **Non**. L'appareil n'est pas détecté à l'aide de l'API AWS, Azure ou Google, c'est-à-dire qu'il se trouve soit en dehors de l'environnement Cloud, soit dans l'environnement Cloud, mais il ne peut pas être détecté à l'aide d'une API.
7. **Pas de valeur**. Cette condition ne s'applique pas. En cas de besoin, d'autres propriétés de la règle dans d'autres sections.
8. Si nécessaire, appliquez la règle en cliquant sur le bouton **Forcer**, dans la partie inférieure de la fenêtre.

   L'Assistant d'exécution de la règle démarre. Suivez les instructions de l'assistant. Une fois que l'Assistant a terminé, la règle est exécutée et la structure des sous-groupes au sein du sous-groupe **Appareils administrés\Cloud** correspond à la structure de vos segments dans le Cloud.
9. Cliquez sur le bouton **OK**.

Les propriétés sont configurées et enregistrées.

Pour désactiver la règle Synchronisation avec Cloud, procédez comme suit :

1. Dans l'arborescence de la console, effectuez un clic droit sur le nom de l'entrée **Recherche d'appareils**.
2. Dans le menu contextuel, sélectionnez l'option **Propriétés**.
3. Dans la fenêtre **Propriétés** qui s'ouvre, dans le volet **Sections**, sélectionnez **Déplacer les appareils**.
4. Dans la liste des règles de déplacement des appareils de l'espace de travail, décochez l'option **Synchronisation avec Cloud**, puis cliquez sur **OK**.

La règle est désactivée et n'est plus appliquée.

Déploiement de Kaspersky Security Center dans Yandex.Cloud

Vous pouvez déployer Kaspersky Security Center dans Yandex.Cloud. Seul le mode de paiement à l'utilisation est proposé ; les bases de données dans le cloud ne sont pas prises en charge.

Dans Yandex.Cloud, voici les méthodes de déploiement des applications de sécurité proposées :

- Par le biais de Kaspersky Security Center en mode natif, c'est-à-dire via la tâche *Installation à distance* (le déploiement des applications de sécurité n'est possible que si le Serveur d'administration et les machines virtuelles à protéger se trouvent sur le même segment de réseau)

- Via des scripts de déploiement

Pour procéder au déploiement de Kaspersky Security Center dans Yandex.Cloud, vous devez disposer d'un compte de service dans Yandex.Cloud. Vous devez accorder à ce compte l'autorisation marketplace.meteringAgent et associer ce compte à la machine virtuelle (pour en savoir plus, veuillez consulter l'adresse https://cloud.yandex.com/en).

Appendice

Cette section fournit une aide et des informations complémentaires sur l'utilisation de Kaspersky Security Center.

Possibilités complémentaires

Cette section aborde les possibilités complémentaires de Kaspersky Security Center prévues pour étendre les fonctions d'administration centralisée des applications sur les appareils.

Automatisation du fonctionnement de Kaspersky Security Center. Utilitaire klakaut

Vous pouvez automatiser le fonctionnement de Kaspersky Security Center via l'utilitaire klakaut. L'utilitaire klakaut et son système d'aide se trouvent dans le dossier d'installation de Kaspersky Security Center.

Fonctionnement avec les outils externes

Kaspersky Security Center permet de configurer une liste des *outils personnalisés* (ci-après, les *instruments*), à savoir, des applications activées pour un appareil client dans la Console d'administration à l'aide du groupe du **Outils externes** dans le menu contextuel. Pour chaque outil de la liste, une commande de menu est créée, ce qui permet à la Console d'administration de lancer l'application qui correspond à l'outil.

L'application se lance sur le poste de travail de l'administrateur. L'application peut accepter en guise d'arguments de la ligne de commande les attributs de l'appareil client distant (nom NetBIOS, nom DNS, adresse IP). La connexion à l'appareil peut être exécutée à l'aide d'une connexion en tunnel.

Par défaut, la liste des outils externes contient les services suivants pour chaque appareil client :

- **Diagnostic à distance** est un utilitaire de diagnostic à distance de Kaspersky Security Center.
- **Bureau distant** est un module Microsoft Windows standard nommé Connexion Bureau à distance.
- **Administration de l'ordinateur** est module Microsoft Windows standard.

Pour ajouter ou supprimer les outils externes et de modifier leurs paramètres,

Dans le menu contextuel de l'appareil client, sélectionnez **Outils externes** → **Configurer des outils personnalisés**.

Finalement, la fenêtre **Outils externes** s'ouvrira. Dans cette fenêtre, vous pouvez ajouter des outils personnalisés ou modifier leurs paramètres à l'aide des boutons **Ajouter** et **Modifier**. Pour supprimer un outil personnalisé, cliquez sur le bouton de suppression avec l'icône en forme de croix rouge (❌).

Mode de clonage du disque de l'Agent d'administration

Le clonage du disque dur d'un appareil " étalon " est une méthode répandue pour l'installation d'un logiciel sur de nouveaux appareils. Si l'Agent d'administration sur le disque dur de l'appareil " étalon " fonction en mode normal pendant le clonage, le problème suivant survient :

Après le déploiement de l'image de disque étalon dotée de l'Agent d'administration sur de nouveaux appareils, ces derniers apparaissent sous la même icône dans la Console d'administration. Ce problème survient parce que lors de la copie sur les nouveaux appareils, les données internes identiques sont conservées. Ces données permettent au Serveur d'administration d'associer l'appareil à l'icône dans la Console d'administration.

Pour éviter les problèmes liés à l'affichage incorrect des nouveaux appareils dans la Console d'administration après la copie, vous pouvez utiliser le *mode spécial de clonage de disque de l'Agent d'administration*. Utilisez ce mode si vous déployez une application (avec l'Agent d'administration) sur de nouveaux appareils via le clonage du disque.

En mode de clonage du disque, l'Agent d'administration fonctionne, mais il ne se connecte pas au Serveur d'administration. Une fois sorti du mode de clonage, l'Agent d'administration supprime les données internes qui faisaient que le Serveur d'administration associait plusieurs appareils à une icône dans la Console d'administration. A l'issue de la copie de l'image de l'appareil " étalon ", les nouveaux appareils apparaissent normalement dans la Console d'administration (avec leur propre icône).

Scénarios d'utilisation du mode de clonage du disque de l'Agent d'administration

1. L'administrateur installe l'Agent d'administration sur l'appareil " étalon ".
2. L'administrateur vérifie la connexion de l'Agent d'administration au Serveur d'administration à l'aide de l'utilitaire klnagchk.
3. L'Administrateur active le mode de clonage du disque de l'Agent d'administration.
4. L'administrateur installe sur l'appareil l'application, les correctifs et redémarre l'appareil autant de fois que nécessaire.

5. L'administrateur clone le disque de l'appareil " étalon " sur n'importe quelle quantité d'appareils.
6. Les conditions suivantes doivent être remplies pour chaque copie clonée :
    a. Le nom de l'appareil est modifié.
    b. L'appareil a redémarré.
    c. Le mode de clonage du disque est désactivé.

Activation et désactivation du mode de clonage du disque à l'aide de l'utilitaire klmover

Pour activer ou désactiver le mode de clonage du disque de l'Agent d'administration, procédez comme suit :

1. Lancez l'utilitaire klmover sur l'appareil doté de l'Agent d'administration qu'il faut cloner.
   L'utilitaire klmover se trouve dans le dossier d'installation de l'Agent d'administration.
2. Pour activer le mode de clonage du disque, saisissez la commande suivante à l'invite de commande Windows :
   `klmover -cloningmode 1`
   L'Agent d'administration passe au mode de clonage du disque.
3. Pour connaître l'état actuel du mode de clonage du disque, saisissez la commande suivante dans l'invite de commande :
   `klmover -cloningmode`
   La fenêtre de l'utilitaire affiche les informations qui indiquent sur le mode de clonage du disque est activé ou non.
4. Pour désactiver le mode de clonage du disque, saisissez la commande suivante dans la ligne de commande de l'utilitaire :
   `klmover -cloningmode 0`

Préparation d'un appareil étalon sur lequel l'Agent d'administration est installé pour créer une image du système d'exploitation

Vous voudrez peut-être créer une image du système d'exploitation d'un appareil étalon sur lequel l'Agent d'administration est installé, puis déployer l'image sur les appareils en réseau. Dans ce cas, vous créez une image du système d'exploitation d'un appareil étalon sur lequel l'Agent d'administration n'a pas encore été lancé. Si vous lancez l'Agent d'administration sur un appareil étalon avant de créer une image du système d'exploitation, l'identification par le Serveur d'administration des appareils déployés à partir d'une image du système d'exploitation de l'appareil de référence sera problématique.

Pour préparer l'appareil étalon à la création d'une image du système d'exploitation :

1. Assurez-vous que le système d'exploitation Windows est installé sur l'appareil étalon et installez les autres logiciels dont vous avez besoin sur cet appareil.
2. Sur l'appareil étalon, dans les paramètres de connexions réseau Windows, déconnectez l'appareil de référence du réseau sur lequel Kaspersky Security Center est installé.

3. Sur l'appareil étalon, démarrez l'installation locale de l'Agent d'administration à l'aide du fichier setup.exe.

   L'Assistant d'installation de l'Agent d'administration de l'Agent d'administration de Kaspersky Security Center démarre. Suivez les instructions de l'assistant.

4. Sur la page **Serveur d'administration** de l'Assistant, indiquez l'adresse IP du Serveur d'administration.

   Si vous ne connaissez pas l'adresse exacte du Serveur d'administration, saisissez localhost. Vous pouvez modifier l'adresse IP ultérieurement en utilisant l'utilitaire klmover avec la clé `-address`.

5. Sur la page **Lancer l'application** de l'Assistant, désactivez l'option **Lancer l'application dans le processus d'installation**.

6. Lorsque l'installation de l'Agent d'administration est terminée, ne redémarrez pas l'appareil avant de créer une image du système d'exploitation.

   Si vous redémarrez l'appareil, vous devrez répéter tout le processus de préparation d'un appareil étalon pour la création d'une image du système d'exploitation.

7. Sur l'appareil étalon, dans la ligne de commande, lancez l'utilitaire sysprep et exécutez la commande suivante : `sysprep.exe /generalize /oobe /shutdown`.

L'appareil étalon est prêt pour la création d'une image du système d'exploitation.

Configuration des paramètres de réception des messages du Contrôle de l'intégrité des fichiers

Les applications administrées, comme Kaspersky Security for Windows Server ou Kaspersky Security for Virtualization Light Agent, envoient des messages de Contrôle de l'intégrité des fichiers à Kaspersky Security Center. Kaspersky Security Center permet aussi de suivre la constance des zones critiques importantes des systèmes (par exemple, les serveurs Web, guichets automatiques) et de réagir rapidement aux violations de l'intégrité de ces systèmes. À cet effet, vous pouvez recevoir des messages du module Contrôle de l'intégrité des fichiers. Le module Contrôle de l'intégrité des fichiers permet de suivre non seulement le système de fichiers de l'appareil mais aussi les branches du registre, l'état du pare-feu et l'état de l'équipement connecté.

Vous devez configurer Kaspersky Security Center pour recevoir les messages du module Contrôle de l'intégrité des fichiers sans utiliser des applications Kaspersky Security for Windows Server ou Kaspersky Security for Virtualization Light Agent.

Pour configurer les paramètres de réception des messages du module Contrôle de l'intégrité des fichiers, procédez comme suit :

1. Ouvrez le registre système de l'appareil sur lequel le Serveur d'administration est installé, par exemple, à l'aide de la commande regedit dans le menu **Démarrer** → **Exécuter**.

2. Rendez-vous dans la section :

   - Pour les systèmes 32 bits :

     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags

   - Pour les systèmes 64 bits :

     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1093\1.0.0.0\ServerF

3. Créez les clés :

   - Créez la clé KLSRV_EVP_FIM_PERIOD_SEC pour indiquer la période de calcul du nombre d'événements traités. Définissez les paramètres suivants :

     a. Indiquez le nom de la clé KLSRV_EVP_FIM_PERIOD_SEC.

     b. Définissez le type de clé DWORD.

     c. Précisez la plage de valeurs de l'intervalle de temps entre 43200 et 172800 secondes. Par défaut l'intervalle d'analyse est égal à 86400 secondes.

   - Créez la clé KLSRV_EVP_FIM_LIMIT pour restreindre la quantité d'événements acceptés pour l'intervalle de temps indiqué. Définissez les paramètres suivants :

     a. Indiquez le nom de la clé KLSRV_EVP_FIM_LIMIT.

     b. Définissez le type de clé DWORD.

     c. Précisez la plage de valeurs des événements acceptés entre 2000 et 50000. Le nombre d'événements par défaut est égal à 20000.

   - Créez la clé KLSRV_EVP_FIM_PERIOD_ACCURACY_SEC pour le calcul des événements avec une précision allant jusqu'à l'intervalle de temps défini. Définissez les paramètres suivants :

     a. Indiquez le nom de la clé KLSRV_EVP_FIM_PERIOD_ACCURACY_SEC.

     b. Définissez le type de clé DWORD.

     c. Précisez la plage de valeurs entre 120 et 600 secondes. Par défaut l'intervalle d'analyse est égal à 300 secondes.

   - Créez la clé KLSRV_EVP_FIM_OVERFLOW_LATENCY_SEC pour qu'après la valeur de temps indiquée, l'application contrôle que le nombre d'événements traités sur l'intervalle de temps soit inférieur à restriction définie. L'analyse est exécutée une fois la restriction de la réception des événements atteinte. Si la condition est remplie, l'enregistrement des événements dans la base de données reprend. Définissez les paramètres suivants :

     a. Indiquez le nom de la clé KLSRV_EVP_FIM_OVERFLOW_LATENCY_SEC.

     b. Définissez le type de clé DWORD.

     c. Précisez la plage de valeurs entre 600 et 3600 secondes. Par défaut l'intervalle d'analyse est égal à 1800 secondes.

   Si les clés ne sont pas créées, les valeurs par défaut sont utilisées.

4. Relancez le service du Serveur d'administration.

Les restrictions de réception des événements du module Contrôle de l'intégrité des fichiers seront configurées. Vous pouvez consulter les résultats du fonctionnement du module Contrôle de l'intégrité du système dans les rapports **Top 10 des règles du Contrôle de l'intégrité des fichiers/Contrôle de l'intégrité du système qui ont été le plus souvent déclenchées sur les appareils** et **Top 10 des appareils dont les règles du Contrôle de l'intégrité des fichiers/Contrôle de l'intégrité du système sont le plus souvent déclenchées**.

Maintenance du Serveur d'administration

La maintenance du Serveur d'administration permet de libérer de l'espace dans le dossier du Serveur d'administration et de réduire le volume de la base de données en supprimant des objets qui ne sont plus nécessaires. Cette mesure vous permet d'améliorer les performances et la fiabilité de fonctionnement de l'application. Il est recommandé d'effectuer la maintenance du Serveur d'administration au moins une fois par semaine.

La maintenance du Serveur d'administration s'effectue à l'aide de la tâche correspondante. Pendant la maintenance du Serveur d'administration, l'application exécute les opérations suivantes :

- Supprime les dossiers et les fichiers inutiles du dossier de stockage.
- Supprime les enregistrements inutiles des tableaux (également appelés " dangling pointers ", ou " pointeurs pendouillants ").
- Purge le cache.
- Maintient la base de données (si vous utilisez le serveur SQL ou PostgreSQL comme SGBD) :
  - Elle recherche les erreurs dans la base de données (disponible uniquement pour le serveur SQL).
  - Elle réorganise les indices de la base de données.
  - Elle met à jour les statistiques de la base de données.
  - Elle comprime la base de données (si nécessaire).

Pour créer la tâche Maintenance du Serveur d'administration, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le nœud du Serveur d'administration pour lequel une tâche *Maintenance du Serveur d'administration* doit être créée.
2. Sélectionnez le dossier **Tâches**.
3. Dans l'espace de travail du dossier **Tâches**, cliquez sur le bouton **Nouvelle tâche**.

   Ceci permet de lancer l'Assistant de création d'une tâche.
4. Dans la fenêtre **Sélection du type de tâche** de l'assistant, sélectionnez **Maintenance du Serveur d'administration** comme type de tâche, puis cliquez sur **Suivant**.
5. Si, pendant la maintenance, la base de données du Serveur d'administration doit être comprimée, dans la fenêtre **Paramètres** de l'Assistant, cochez la case **Rétrécir la base de données**.
6. Suivez les étapes ultérieures de l'assistant.

La tâche créée est affichée dans la liste de tâches de l'espace de travail du dossier **Tâches**. Une seule tâche *Maintenance du Serveur d'administration* peut être exécutée pour un même Serveur d'administration. Si une tâche *Maintenance du Serveur d'administration* pour un Serveur d'administration est déjà créée, aucune nouvelle tâche *Maintenance du Serveur d'administration* ne peut être créée.

Accès aux serveurs DNS publics

Si l'accès aux serveurs Kaspersky via le système DNS n'est pas possible, Kaspersky Security Center peut utiliser les serveurs DNS publics suivants, dans l'ordre suivant :

1. DNS public de Google (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. Navigation simplifiée (185.228.168.168)

Les requêtes adressées à ces serveurs DNS peuvent contenir des adresses de domaine et l'adresse IP publique du Serveur d'administration, car l'application établit une connexion TCP/UDP avec le serveur DNS. Si Kaspersky Security Center utilise un serveur DNS public, le traitement des données est régi par la politique de confidentialité du service concerné.

Pour configurer l'utilisation du DNS public à l'aide de l'utilitaire klscflag :

1. Exécutez l'invite de commande Windows en utilisant les droits d'administrateur, puis remplacez votre répertoire actuel par celui contenant l'utilitaire klscflag. L'utilitaire klsclag se trouve dans le dossier dans lequel le Serveur d'administration est installé. Chemin d'installation par défaut est <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.
2. Pour désactiver l'utilisation du DNS public, exécutez la commande suivante :

   ```
   klscflag -fset -pv ".core/.independent" -s Transport -n ForceUseSystemDNS -t d -v 1
   ```

3. Pour activer l'utilisation du DNS public, exécutez la commande suivante :

   ```
   klscflag -fset -pv ".core/.independent" -s Transport -n ForceUseSystemDNS -t d -v 0
   ```

Fenêtre Moyen de notification des utilisateurs

La fenêtre **Mode de notification des utilisateurs** permet de configurer les notifications utilisateur concernant l'installation du certificat sur l'appareil mobile :

- **Afficher le code QR dans l'assistant**. En cas de sélection de cette option, le lien vers le paquet d'installation sera affiché à la dernière étape de l'Assistant de connexion d'un nouvel appareil mobile.
- **Envoyer le code QR à l'utilisateur**. Si vous choisissez cette option, vous pouvez configurer les notifications de l'utilisateur sur la connexion d'un appareil.

Le groupe de paramètres **Par email** permet de configurer les notifications de l'utilisateur relatives à l'installation d'un nouveau certificat sur son appareil mobile via des messages électroniques. Ce mode de notification est disponible uniquement si un serveur SMTP a été configuré.

Le groupe de paramètres **Par SMS** permet de configurer les notifications de l'utilisateur sur l'installation d'un certificat sur son appareil mobile via des messages SMS. Ce mode de notification est disponible uniquement si la notification par SMS a été configurée.

Cliquez sur le lien **Modifier le message** dans les groupes de paramètres **Par email** et **Par SMS** pour afficher et modifier le message de notification si nécessaire.

Fenêtre Sélection d'appareils

Choisissez une sélection dans la liste **Sélection d'appareils**. La liste contient les sélections prédéfinies et les sélections créées par l'utilisateur.

Vous pouvez afficher les détails des sélections d'appareils dans l'espace de travail de la section **Sélections d'appareils**.

Fenêtre Définition du nom de l'objet créé

Dans la fenêtre, indiquez le nom de l'objet créé. Le nom ne peut pas contenir plus de 100 symboles et contenir de symboles spéciaux ("*<>?\:|).

Section Catégories d'applications

Dans cette section, vous pouvez configurer la diffusion des informations sur les catégories d'applications vers les appareils clients.

&Transfert complet des données (pour les Agents d'administration version 10 Service Pack 2 ou version antérieure)

Si cette option a été sélectionnée, en cas de modification des catégories d'applications sur les appareils clients, toutes les données de la catégorie sont transmises aux appareils clients. Cette option de transmission de données est utilisée pour les Agents d'administration de la version Service Pack 2 et versions inférieures.

&Transfert des données uniquement modifiées (pour les Agents d'administration version 10 Service Pack 2 ou ultérieure)

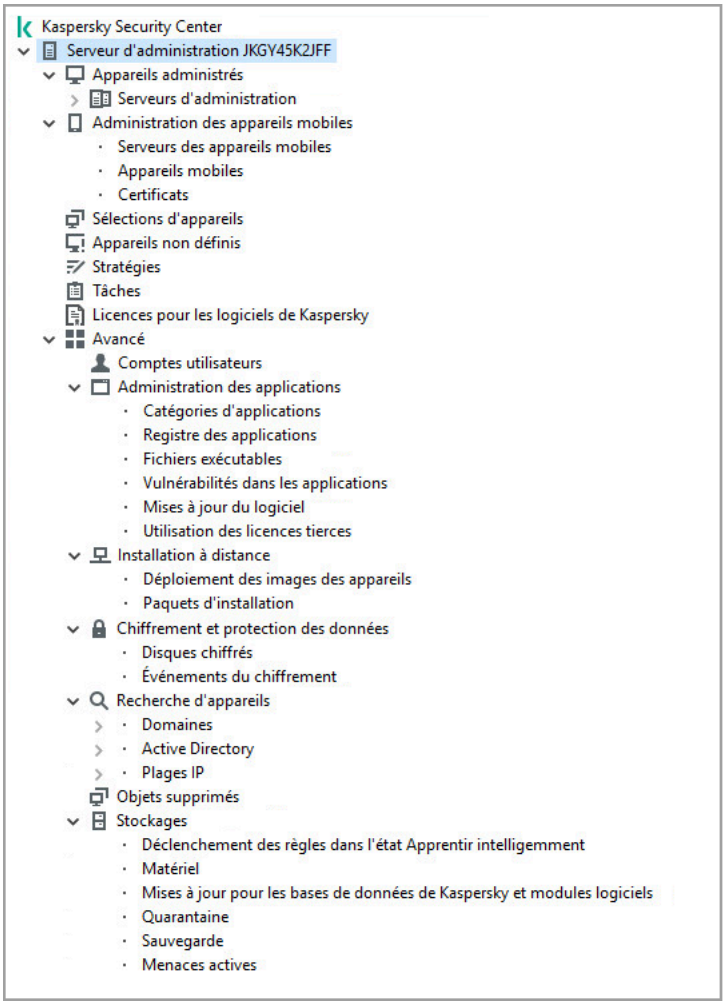
Si cette option a été sélectionnée, en cas de modification des catégories d'applications, toutes les données de catégorie ne sont pas transmises aux appareils clients, seulement les données qui ont été modifiées. Cette option de transmission de données est utilisée pour les Agents d'administration de la version Service Pack 2 et versions supérieures.

Particularités d'utilisation de l'interface d'administration

Cette section contient la description des modes d'utilisation dans la fenêtre principale de Kaspersky Security Center.

Arborescence de la console

L'arborescence de la console (voir la figure ci-dessous) est conçue pour afficher la hiérarchie des Serveurs d'administration sur le réseau d'entreprise, la structure des groupes d'administration, et d'autres objets de l'application, tels que les **Stockages** ou les dossiers **Administration des applications**. L'étendue des noms de Kaspersky Security Center peut inclure plusieurs sections avec les noms des serveurs qui correspondent aux Serveurs d'administration installés et inclus dans la structure du réseau.



Arborescence de la console

Entrée Serveur d'administration

La section **Serveur d'administration : <Device name>** est un conteneur et reflète la structure du Serveur d'administration indiqué.

Le nœud **Serveur d'administration** contient dans son espace de travail des informations récapitulatives sur l'état actuel de l'application et des appareils administrés par le Serveur d'administration. Les informations sur l'espace de travail se trouvent dans les onglets suivants :

- **Surveillance**. Affiche des informations sur le fonctionnement de l'application et l'état actuel des appareils clients en mode temps réel. Les messages importants destinés à l'administrateur (par exemple sur des vulnérabilités, sur des erreurs ou sur la détection de virus) sont mis en couleur. Les liens de l'onglet **Surveillance** permettent d'effectuer des tâches typiques d'administrateur (par exemple, installer et configurer l'application de sécurité sur les appareils clients), ainsi que d'accéder à d'autres dossiers de l'arborescence de la console.

- **Statistiques**. Contient un ensemble de diagrammes regroupés par thèmes (état de la protection, statistiques antivirus, mises à jour, etc.). Des diagrammes visuels présentent des informations à jour sur le fonctionnement de l'application et l'état des appareils clients.

- **Rapports**. Contient des modèles de rapports constitués par l'application. Dans l'onglet, vous pouvez constituer des rapports à partir des modèles prévus et créer vos propres modèles de rapports.

- **Événements**. Contient des écritures d'événements enregistrés pendant le fonctionnement de l'application. Pour faciliter la lecture et le tri, les enregistrements sont répartis selon des sélections thématiques. Dans l'onglet, vous pouvez examiner les sélections d'événements créées automatiquement et créer vos propres sélections.

Dossiers du nœud Serveur d'administration

Le nœud **Serveur d'administration – <Device name>** inclut les dossiers suivants :

- **Appareils administrés**. Le dossier est conçu pour conserver, refléter, configurer et modifier la structure des groupes d'administration, les stratégies de groupe et les tâches de groupe.

- **Administration des appareils mobiles**. Ce dossier est conçu pour l'administration des appareils mobiles. Le dossier **Administration des appareils mobiles** contient aussi les dossiers joints suivants :

  - **Serveurs des appareils mobiles**. Destiné à l'administration des Serveurs MDM iOS.

  - **Appareils mobiles**. Conçu pour l'administration des appareils mobiles KES et MDM iOS.

  - **Certificats**. Conçu pour la gestion des certificats des appareils mobiles.

- **Sélections d'appareils**. Le dossier est conçu pour une sélection rapide d'appareils correspondant à des critères définis (une sélection d'appareils), parmi tous les appareils administrés. Par exemple, vous pouvez sélectionner rapidement les appareils sur lesquels l'application de sécurité n'est pas installée et accéder à ces appareils (voir leurs listes). Avec les appareils sélectionnés, vous pouvez effectuer des actions, par exemple, leur affecter des tâches. Vous pouvez utiliser les sélections fournies et créer vos propres sélections (d'utilisateur).

- **Appareils non définis**. Ce dossier contient la liste des appareils qui ne font partie d'aucun groupe d'administration. Vous pouvez effectuer des actions avec des appareils non définis, par exemple, les déplacer vers des groupes d'administration et installer des applications sur ces appareils.

- **Stratégies**. Ce dossier est conçu pour la consultation et la création de stratégies.

- **Tâches**. Ce dossier est conçu pour la consultation et la création de tâches.

- **Licences pour les logiciels de Kaspersky**. Contient une liste des clés de licence disponibles pour les applications de Kaspersky. Dans l'espace de travail de ce dossier, vous pouvez ajouter de nouvelles clés de licence au stockage des clés de licence, déployer des clés de licence sur les appareils administrés et afficher le rapport sur les clés de licence utilisées.

- **Avancé**. Ce dossier contient un ensemble de dossiers joints correspondant à différents groupes de fonctionnalités de l'application.

Dossier Avancé. Déplacement des dossiers dans l'arborescence de la console

Le dossier **Avancé** contient les dossiers suivants :

- **Comptes utilisateurs**. Ce dossier contient une liste de comptes utilisateurs du réseau.

- **Administration des applications**. Le dossier est conçu pour administrer les applications installées sur les appareils du réseau. Le dossier **Administration des applications** contient aussi les dossiers joints suivants :

  - **Catégories d'applications**. Conçu pour travailler avec les catégories d'applications définies par l'utilisateur.

  - **Registre des applications**. Contient la liste des applications sur les appareils avec l'Agent d'administration installé.

  - **Fichiers exécutables**. Contient la liste des fichiers exécutables enregistrés sur les appareils clients avec l'Agent d'administration installé.

  - **Vulnérabilités dans les applications**. Contient la liste des vulnérabilités dans les applications sur les appareils avec l'Agent d'administration installé.

  - **Mises à jour du logiciel**. Contient la liste des mises à jour des applications, mises à jour reçues par le Serveur d'administration qui peuvent être déployées sur les appareils.

  - **Utilisation des licences tierces**. Comporte une liste des groupes des applications sous licence. Vous pouvez utiliser des groupes des applications sous licence pour surveiller l'utilisation des licences pour les logiciels tiers (applications non développées par Kaspersky) et les éventuelles violations des limites de licence.

- **Installation à distance**. Le dossier est conçu pour administrer l'installation à distance des systèmes d'exploitation et des applications. Le dossier **Installation à distance** contient aussi les dossiers joints suivants :

  - **Déploiement des images des appareils**. Conçu pour déployer les images des systèmes d'exploitation sur les appareils.

  - **Paquets d'installation**. Contient la liste des paquets d'installation qui peuvent être utilisés pour l'installation à distance des applications sur les appareils.

- **Chiffrement et protection des données**. Le dossier est conçu pour administrer le processus de chiffrement des données sur les disques durs et les disques amovibles.

- **Sondage du réseau**. Le dossier est conçu pour afficher le réseau où le Serveur d'administration est installé. Le Serveur d'administration reçoit des informations sur la structure du réseau et de ses appareils via des sondages réguliers du réseau Windows, des sous-réseaux IP et d'Active Directory® sur le réseau d'entreprise. Les résultats des sondages s'affichent dans les espaces de travail des dossiers suivants : **Domaines**, **Plages IP** et **Active Directory**.

- **Stockages**. Le dossier permet de manipuler les objets utilisés pour la surveillance de l'état des appareils et les entretenir. Le dossier **Stockages** contient aussi les dossiers joints suivants :

  - **Détection adaptative des anomalies**. Contient une liste des détections effectuées par les règles de Kaspersky Endpoint Security fonctionnant en mode apprentissage intelligent sur les appareils clients.

  - **Mises à jour logicielles et correctifs de Kaspersky**. Contient la liste des mises à jour reçues par le Serveur d'administration qui peuvent être déployées sur les appareils.

  - **Matériel**. Contient la liste du matériel connecté au réseau de l'entreprise.

  - **Quarantaine**. Contient la liste des objets placés par les applications antivirus dans les dossiers de quarantaine des appareils.

  - **Sauvegarde**. Contient une liste de copies de sauvegarde des fichiers qui ont été supprimés ou modifiés lors de la désinfection sur les appareils.

  - **Fichiers non traités**. Contient la liste des fichiers pour lesquels les applications antivirus ont décidé de la désinfection ultérieure.

Vous pouvez modifier l'ensemble de dossiers placés dans le dossier **Avancé**. Ces dossiers utilisés activement peuvent être déplacés du dossier **Avancé** vers un niveau supérieur. Les dossiers utilisés rarement peuvent être placés dans le dossier **Avancé**.

*Pour déplacer un sous-dossier imbriqué du dossier **Avancé**, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le sous-dossier à déplacer du dossier **Avancé**.

2. Dans le menu contextuel du sous-dossier, sélectionnez le point **Affichage → Déplacer depuis le dossier Avancé**.

> Vous pouvez également extraire un sous-dossier du dossier **Avancé** dans l'espace de travail de ce même dossier **Avancé**, par le lien **Déplacer depuis le dossier Avancé** dans le groupe avec le nom du sous-dossier.

*Pour déplacer un sous-dossier vers le dossier **Avancé**, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le sous-dossier à déplacer vers le dossier **Avancé**.

2. Dans le menu contextuel du sous-dossier, sélectionnez le point **Affichage → Déplacer vers le dossier Avancé**.

Comment mettre à jour les données dans l'espace de travail

> Dans Kaspersky Security Center, les données de l'espace de travail (par exemple états des appareils, statistiques, rapports) ne sont pas mises à jour automatiquement.

Pour mettre à jour les données dans l'espace de travail, exécutez une des actions suivantes :

- Appuyez sur la touche **F5**.
- Dans le menu contextuel de l'objet dans l'arborescence de la console, sélectionnez l'option **Actualiser**.
- Cliquez sur l'icône d'actualisation ( ) dans l'espace de travail.

Comment se déplacer dans l'arborescence de la console

Pour se déplacer dans l'arborescence de la console vous pouvez utiliser les touches suivantes, situées dans la barre d'outils :

- : passage à un pas en arrière.
- : passage à un pas en avant.
- : passage à un niveau plus haut.

Aussi vous pouvez utiliser une chaîne de navigation, située dans l'espace de travail en haut à droite. La chaîne de navigation contient le chemin complet vers ce dossier de l'arborescence de la console où vous êtes situés en ce moment. Tous les éléments de la chaîne, à part le dernier, sont les liens vers les objets de l'arborescence de la console.

Comment ouvrir la fenêtre des propriétés de l'objet dans l'espace de travail

Les propriétés de la plupart des objets de la Console d'administration peuvent être modifiées dans la fenêtre des propriétés de l'objet.

Pour ouvrir la fenêtre des propriétés de l'objet situé dans l'espace de travail, exécutez une des actions suivantes :

- Dans le menu contextuel de l'objet, sélectionnez l'option **Propriétés**.
- Sélectionnez l'objet et cliquez une combinaison des touches **ALT**+**ENTER**.

Comment sélectionner le groupe des objets dans l'espace de travail

Vous pouvez sélectionner le groupe des objets dans l'espace de travail. La sélection du groupe des objets peut être utilisée, par exemple, pour créer un ensemble d'appareils et former ensuite les tâches qui y sont liées.

Pour sélectionner la plage des objets, procédez comme suit :

1. Sélectionnez le premier objet et appuyez sur la touche **SHIFT**.
2. En appuyant sur la touche **SHIFT**, sélectionnez le dernier objet de la plage.

La plage sera sélectionnée.

Pour unir les objets séparés dans le groupe, procédez comme suit :

1. Sélectionnez le premier objet dans le groupe et appuyez sur la touche **CTRL**.
2. En appuyant sur la touche **CTRL**, sélectionnez les autres objets du groupe.

Les objets seront unis dans le groupe.

Comment modifier l'ensemble des colonnes dans l'espace de travail

La Console d'administration permet de modifier l'ensemble des colonnes, reflétées dans l'espace de travail.

Afin de modifier l'ensemble des colonnes dans l'espace de travail, procédez comme suit :

1. Sélectionnez l'objet de l'arborescence de la console, pour lequel vous voulez modifier l'ensemble des colonnes.
2. Dans l'espace de travail du dossier, ouvrez la fenêtre de configuration de l'ensemble des colonnes en cliquant sur le lien **Ajouter ou supprimer des colonnes**.
3. Dans la fenêtre **Ajouter ou supprimer des colonnes**, spécifiez l'ensemble de colonnes à afficher.

Aide

Cette section reprend dans les tableaux le récapitulatif sur le menu contextuel des objets de la Console d'administration, ainsi que sur les états d'objets de l'arborescence de la console et de l'espace de travail.

Commandes du menu contextuel

Cette section contient la liste des objets de la Console d'administration et l'ensemble d'options du menu contextuel y correspondant (cf. tableau ci-après).

Éléments du menu contextuel des entrées de la Console d'administration

Objet	Option du menu	Désignation de l'option du menu
Points généraux du menu contextuel	**Recherche**	Ouvrir la fenêtre de recherche d'appareils.
	Actualiser	Actualiser l'affichage de l'objet sélectionné.
	Exporter la liste	Exporter la liste courante dans le fichier.
	Propriétés	Ouvrir la fenêtre des propriétés de l'objet sélectionné.
	Consulter → Ajouter ou supprimer des colonnes	Ajouter ou supprimer des colonnes dans le tableau d'objets dans l'espace de travail.
	Consulter → Grandes icônes	Afficher les objets dans l'espace de travail comme des grandes icônes.
	Consulter → Petites icônes	Afficher les objets dans l'espace de travail comme des petites icônes.
	Consulter → Liste	Afficher les objets dans l'espace de travail comme une liste.
	Consulter → Tableau	Afficher les objets dans l'espace de travail comme un tableau.
	Consulter → Configurer	Configurer l'affichage des éléments de la Console d'administration.
Kaspersky Security Center	**Nouveau → Serveur d'administration**	Ajouter un Serveur d'administration à l'arborescence de la console.
<Administration Server name>	**&Se connecter au Serveur d'administration**	Connectez-vous au Serveur d'administration.
	S&e déconnecter du Serveur d'administration	Se déconnecte du Serveur d'administration.
Appareils administrés	**Installer une application**	L'assistant de l'installation à distance démarre.
	Consulter → Configuration de l'interface	Configurer l'affichage des éléments de l'interface.
	Supprimer	Supprimer le Serveur d'administration de l'arborescence de la console.
	Installer une application	Lancement en cours de l'Assistant de l'installation à distance pour le groupe d'administration.
	RAZ compteur de virus	Remettre à zéro les compteurs de virus pour les appareils qui font partie du groupe d'administration.
	Consulter le rapport sur les menaces	Créer un rapport sur les menaces et l'activité virale des appareils qui appartiennent au groupe d'administration.
	Nouveau → Groupe	Créer le groupe d'administration.
	Toutes les tâches → Nouvelle structure de groupe	Créer la structure des groupes d'administration sur la base de la structure des domaines ou d'Active Directory.
	Toutes les tâches → Afficher un message	Lancement en cours l'Assistant de création du message pour les utilisateurs des appareils qui font partie du groupe d'administration.
Appareils administrés → Serveurs d'administration	**Nouveau → &Serveur d'administration secondaire**	Démarrage de l'Assistant d'ajout de Serveur d'administration secondaire.
	Nouveau → S&erveur d'administration virtuel	Démarrage de l'Assistant de création du Serveur d'administration virtuel.
Administration des appareils mobiles → Appareils mobiles	**Nouveau → Appareil mobile**	Connecter le nouvel appareil mobile de l'utilisateur.
Administration des appareils mobiles → Certificats	**Nouveau → Certificat**	Créer un certificat.
	Créer → Appareil mobile	Connecter le nouvel appareil mobile de l'utilisateur.

Objet	Option du menu	Désignation de l'option du menu
Sélections d'appareils	**Nouveau → Nouvelle sélection**	Créer une sélection d'appareils.
	Toutes les tâches → Importer	Importer une sélection depuis un fichier.
Licences pour les logiciels de Kaspersky	**&Ajouter un code d'activation ou un fichier clé**	Ajoute la clé de licence dans le stockage du Serveur d'administration.
	A&ctiver l'application	Démarrage de l'Assistant de création de la tâche d'activation de l'application.
	Rapport sur les clés de licence utilisées	Crée et affiche un rapport sur les clés de licence sur les appareils clients.
Gestion des applications → Catégories d'applications	**Nouveau → Catégorie**	Créer une catégorie d'applications.
Gestion des applications → Registre des applications	**Filtrer**	Configurer le filtre pour la liste des applications.
	Applications contrôlées	Configurer la publication des événements sur l'installation des applications.
	Supprimer les applications non installées	Supprimer de la liste les informations sur les applications qui ne sont pas déjà installées sur les appareils de réseau.
Gestion des applications → Mises à jour du logiciel	**Accepter les Contrats de licence utilisateur final des mises à jour**	Accepter le Contrat de Licence Utilisateur Final des mises à jour logicielles.
Gestion des applications → Utilisation des licences tierces	**Nouveau → Groupe des applications sous licence**	Créer un groupe des applications sous licence.
Installation à distance → Paquets d'installation	**Afficher les versions actuelles des applications**	Afficher la liste des versions actuelles des applications Kaspersky exposées sur les serveurs Web.
	Nouveau → &Paquet d'installation	Créer un paquet d'installation.
	Toutes les tâches → Mettre à jour les bases	Actualiser les bases des applications dans les paquets d'installation.
	Toutes les tâches → Afficher la liste générale des paquets autonomes	Consulter la liste des paquets d'installation autonomes créés pour les paquets d'installation.
Recherche d'appareils → Domaines	**Toutes les tâches → Activité des appareils**	Configurer les paramètres de la réaction du Serveur d'administration à la recherche d'activité d'appareils dans le réseau.
Recherche d'appareils → Plages IP	**Nouveau → Plage IP**	Créer une plage IP.
Stockages → Mises à jour pour les bases de données de Kaspersky et modules logiciels	**Télécharger les mises à jour**	Ouvre la fenêtre des propriétés de la tâche de téléchargement des mises à jour dans le stockage du Serveur d'administration.
	Paramètres de téléchargement des mises à jour	Configure la tâche de téléchargement des mises à jour dans le stockage du Serveur d'administration.
	Rapport sur les bases antivirus utilisées	Créer et importer le rapport de versions des bases.
	Toutes les tâches → Purger le stockage des mises à jour	Purger le stockage des mises à jour sur le Serveur d'administration.
Stockages → Matériel	**Nouveau → Appareil**	Créer un appareil réseau.

Liste des appareils administrés. Valeur des colonnes

Le tableau ci-dessous reprend les noms et les descriptions des colonnes de la liste des appareils administrés.

Valeur des colonnes de la liste des appareils administrés

Nom de la colonne	Valeur
Nom	Nom NetBios de l'appareil client. La description des icônes de nom d'appareil figure dans l'appendice.
Type de système d'exploitation	Type de système d'exploitation de l'appareil client.
Domaine Windows	Nom du domaine Windows auquel appartient l'appareil client.
L'Agent d'administration est installé	Résultat de l'installation de l'Agent d'administration sur l'appareil client : *Oui*, *Non*, *Inconnu*.
L'Agent d'administration est en cours d'exécution	Résultat de l'exécution de l'Agent d'administration (*Oui*, *Non*, *Inconnu*).
Protection en temps réel	L'application de sécurité est installée : *Oui*, *Non*, *Inconnu*.
Dernière connexion au Serveur d'administration	Temps écoulé depuis la connexion de l'appareil client au Serveur d'administration.
Dernière mise à jour des bases antivirus	Période écoulée depuis la dernière mise à jour des appareils administrés.
État	État actuel de l'appareil client : *OK, Critique ou Avertissement*.

Nom de la colonne	Valeur
Description de l'état	Conditions de la modification de l'état de l'appareil client en *Critique* ou *Avertissement*. L'état de l'appareil devient *Avertissement* ou *Critique* dans les conditions suivantes : • L'application de sécurité n'est pas installée. • Trop de virus ont été détectés. • Le niveau de la Protection en temps réel diffère de celui défini par l'Administrateur. • La recherche d'applications malveillantes n'a pas été exécutée depuis longtemps. • Les bases sont dépassées. • Ne s'est pas connecté depuis longtemps. • Des menaces actives sont détectées. • Redémarrage requis. La raison du redémarrage de l'appareil peut être l'une des suivantes : ◦ Raison de redémarrage inconnue. ◦ L'application ne peut s'exécuter avant le redémarrage. ◦ Le redémarrage est requis pour terminer la mise à jour. L'application est exécutée. ◦ Le redémarrage est requis pour le lancement de la mise à jour. ◦ Le redémarrage est requis pour la fin de l'analyse ou la désinfection. ◦ Le redémarrage est requis pour terminer l'installation/la désinstallation à distance. ◦ Fin de chiffrement des données sur le disque. Vous pouvez définir les raisons lors de la configuration de la commutation des états des appareils. • Des applications incompatibles sont installées. • Vulnérabilités détectées dans les applications. • La vérification de mises à jour Windows Update n'a pas eu lieu depuis longtemps. • État de chiffrement non valide. • Les paramètres de l'appareil mobile ne correspondent pas à la stratégie. • Problèmes de sécurité non traités détectés. • État de l'appareil défini par l'application. • Espace disque épuisé sur l'appareil. • La licence expire bientôt. L'état de l'appareil devient uniquement *Critique* pour les raisons suivantes : • La licence a expiré. • L'appareil n'est plus administré. • La protection est désactivée. • L'application de sécurité n'est pas en cours d'exécution. Les applications administrées de Kaspersky installées sur les appareils clients peuvent compléter la liste de descriptions des états. Kaspersky Security Center peut recevoir la description de l'état de l'appareil client de la part des applications administrées Kaspersky installées sur cet appareil. Si l'état attribué à l'appareil par une application administrée ne coïncide pas avec l'état attribué par Kaspersky Security Center, la Console d'administration affiche l'état le plus critique pour la sécurité de l'appareil. Par exemple, si une des applications administrées a attribué à l'appareil l'état *Critique* et que Kaspersky Security Center a attribué l'état *Avertissement*, la Console d'administration affiche l'état *Critique* pour cet appareil et la description de l'état attribué par l'application administrée.
Informations mises à jour	Temps écoulé depuis la dernière synchronisation réussie de l'appareil client avec le Serveur d'administration (c'est-à-dire depuis la dernière analyse du réseau).
Nom DNS	Nom du domaine DNS de l'appareil client.
Domaine DNS	Suffixe DNS principal.
Adresse IP	Adresse IP de l'appareil client. Il est conseillé d'utiliser une adresse IPv4.
Heure de la dernière connexion	Période de visibilité de l'appareil client dans le réseau.
Dernière analyse complète	Date et heure de la dernière analyse de l'appareil client effectuée à l'aide de l'application de sécurité à la demande de l'utilisateur.
Nombre total de détections de menaces	Nombre de menaces détectées.

Nom de la colonne	Valeur
État de la protection en temps réel	État de la protection en temps réel : *En cours de démarrage, En cours d'exécution, En cours d'exécution (protection maximale), En cours d'exécution (vitesse maximale), En cours d'exécution (paramètres recommandés), En cours d'exécution (paramètres personnalisés), Arrêté(e), Suspendu(e), Échec*.
Adresse IP de la connexion	Adresse IP de la connexion au Serveur d'administration de Kaspersky Security Center.
Version de l'Agent d'administration	Version de l'Agent d'administration.
Version de l'application	Version de l'application de sécurité installée sur l'appareil client.
Date de publication des bases antivirus	Version des bases antivirus.
Dernier démarrage du système	Date et heure du dernier démarrage de l'appareil client.
Redémarrage requis	Le redémarrage de l'appareil client est requis.
Point de distribution	Nom de l'appareil qui remplit le rôle de point de distribution pour cet appareil client.
Description	Description de l'appareil client obtenue après une analyse du réseau.
État de chiffrement	État du chiffrement des données de l'appareil client.
État WUA	État de l'Agent de mises à jour Windows de l'appareil client. La valeur *Oui* désigne les appareils clients qui reçoivent les mises à jour via Windows Update depuis le Serveur d'administration. La valeur *Non* désigne les appareils clients qui reçoivent les mises à jour via Windows Update depuis d'autres sources.
Taille de bit du système d'exploitation	Capacité du système d'exploitation de l'appareil client.
État de la protection contre les spams	État du module de protection anti-spam : *En cours d'exécution, En cours de démarrage, Arrêté(e), Suspendu(e), Échec, Inconnu*
État de la protection contre les fuites de données	État du module de Protection contre les fuites de données : *En cours d'exécution, En cours de démarrage, Arrêté(e), Suspendu(e), Échec, Inconnu*
État de la protection des serveurs de collaboration	État du module de filtrage du contenu : *En cours d'exécution, En cours de démarrage, Arrêté(e), Suspendu(e), Échec, Inconnu*
État de Endpoint Protection des serveurs de messagerie	État du module de protection antivirus de Serveur de messagerie : *En cours d'exécution, En cours de démarrage, Arrêté(e), Suspendu(e), Échec, Inconnu*
État de Endpoint Sensor	État du module Endpoint Detection and Response (KATA) : *En cours d'exécution, En cours de démarrage, Arrêté(e), Suspendu(e), Échec, Inconnu*
Date de création	Moment où l'icône <Device name> a été créée. Cet attribut est utilisé pour comparer divers événements entre eux.
Nom du Serveur d'administration virtuel ou secondaire	Nom du Serveur d'administration virtuel ou secondaire. Cette colonne n'est disponible que dans les listes contenant des appareils de différents Serveurs d'administration.
Groupe parent	Nom du groupe d'administration où se trouve l'icône <Device name>. Cette colonne n'est disponible que dans les listes contenant des appareils de différents Serveurs d'administration.
Administré par un autre Serveur d'administration	Le paramètre peut prendre l'une de ces valeurs : • Vrai, si lors de l'installation à distance des applications de sécurité sur l'appareil, il s'avère que l'appareil est administré par un Serveur d'administration différent. • Faux, dans le cas inverse.

Nom de la colonne	Valeur
Build du système d'exploitation	Le numéro de version du système d'exploitation. Vous pouvez indiquer si le système d'exploitation sélectionné doit avoir un numéro de version égal, antérieur ou supérieur. Vous pouvez également configurer la recherche de tous les numéros de version à l'exception du numéro indiqué.
ID de version du système d'exploitation	L'identifiant de version du système d'exploitation. Vous pouvez indiquer si le système d'exploitation sélectionné doit avoir un ID de version égal, antérieur ou supérieur. Vous pouvez également configurer la recherche de tous les ID de version à l'exception du numéro indiqué.

États des appareils, des tâches et des stratégies

Le tableau ci-après reprend la liste des icônes qui apparaissent dans l'arborescence de la console et dans l'espace de travail de la Console d'administration à côté des noms des appareils, des tâches et des stratégies. Ces icônes définissent l'état des objets.

États des appareils, des tâches et des stratégies

Icône	État
	Appareil avec un système d'exploitation pour postes de travail détecté dans le réseau mais n'appartenant à aucun groupe d'administration.
	Appareil doté d'un système d'exploitation pour postes de travail appartenant à un groupe d'administration avec l'état *OK*.
	Appareil avec un système d'exploitation pour postes de travail appartenant à un groupe d'administration et correspondant à l'état *Avertissement*.
	Appareil avec un système d'exploitation pour poste de travail appartenant à un groupe d'administration et correspondant à l'état *Critique*.
	Appareil avec un système d'exploitation pour postes de travail appartenant à un groupe d'administration dont la connexion au Serveur d'administration est perdue.
	Appareil avec un système d'exploitation pour serveurs détecté dans le réseau mais n'appartenant à aucun groupe d'administration.
	Appareil doté d'un système d'exploitation pour serveurs appartenant à un groupe d'administration et correspondant à l'état *OK*.
	Appareil avec un système d'exploitation pour serveurs appartenant à un groupe d'administration et correspondant à l'état *Avertissement*.
	Appareil avec un système d'exploitation pour serveurs appartenant à un groupe d'administration et correspondant à l'état *Critique*.
	Appareil avec un système d'exploitation pour serveurs appartenant à un groupe d'administration dont la connexion au Serveur d'administration est perdue.
	Appareil mobile détecté sur le réseau et ne faisant partie d'aucun groupe d'administration.
	Appareil mobile faisant partie d'un groupe d'administration avec l'état *OK*.
	Appareil mobile faisant partie d'un groupe d'administration avec l'état *Avertissement*.
	Appareil mobile faisant partie d'un groupe d'administration avec l'état *Critique*.
	Appareil mobile faisant partie d'un groupe d'administration et dont la connexion au Serveur d'administration a été perdue.
	Appareil protégé au niveau UEFI détecté sur le réseau, mais n'appartenant à aucun groupe d'administration. Appareil protégé au niveau UEFI sur le réseau.
	Appareil protégé au niveau UEFI détecté sur le réseau, mais n'appartenant à aucun groupe d'administration. Appareil protégé au niveau UEFI absent du réseau.
	Appareil protégé au niveau UEFI appartenant à un groupe d'administration et correspondant à l'état *OK*. Appareil protégé au niveau UEFI sur le réseau.

	Appareil protégé au niveau UEFI appartenant à un groupe d'administration et correspondant à l'état *OK*. Appareil protégé au niveau UEFI absent du réseau.
	Appareil protégé au niveau UEFI appartenant à un groupe d'administration et correspondant à l'état *Avertissement*. Appareil protégé au niveau UEFI sur le réseau.
	Appareil protégé au niveau UEFI appartenant à un groupe d'administration et correspondant à l'état *Avertissement*. Appareil protégé au niveau UEFI absent du réseau.
	Appareil protégé au niveau UEFI appartenant à un groupe d'administration et correspondant à l'état *Critique*. Appareil protégé au niveau UEFI sur le réseau.
	Appareil protégé au niveau UEFI appartenant à un groupe d'administration et correspondant à l'état *Critique*. Appareil protégé au niveau UEFI absent du réseau.
	Stratégie active.
	Stratégie inactive.
	Stratégie active héritée du groupe créé sur le Serveur d'administration principal.
	Stratégie active héritée depuis le groupe à un niveau supérieur de la hiérarchie.
	Tâche (de groupe, du Serveur d'administration ou pour un ensemble d'appareils) à l'état *En attente d'exécution* ou *Terminée avec succès*.
	Tâche (tâche de groupe, tâche du Serveur d'administration ou tâche pour un ensemble d'appareils) avec l'état *En cours d'exécution*.
	Tâche (tâche de groupe, tâche du Serveur d'administration ou tâche pour un ensemble d'appareils) dans l'état *Échec*.
	Tâche héritée du groupe créé sur le Serveur d'administration principal.
	Tâche héritée depuis le groupe à un niveau supérieur de la hiérarchie.

Icônes des états des fichiers dans la Console d'administration

Pour simplifier l'utilisation des fichiers dans la Console d'administration de Kaspersky Security Center, des icônes s'affichent en regard des noms de fichiers (cf. le tableau ci-après). Les icônes signalent les états attribués aux fichiers par les applications administrées de Kaspersky sur les appareils clients. Les icônes s'affichent dans l'espace de travail des dossiers **Quarantaine**, **Sauvegarde** et **Menaces actives**.

Les états sont attribués aux objets par l'application Kaspersky Endpoint Security installée sur l'appareil client où se trouve l'objet.

Correspondance des icônes aux états des fichiers

Icône	État
	Fichier avec l'état *Infecté*.
	Fichier avec l'état *Avertissement* ou *Probablement infecté*.
	Fichier avec l'état *Ajouté par l'utilisateur*.
	Fichier avec l'état *Faux positif*.
	Fichier avec l'état *Désinfecté*.
	Fichier avec l'état *Supprimé*.
	Fichier dans le dossier **Quarantaine** avec l'état *Non infecté*, *Protégé par un mot de passe* ou *Doit être envoyé à Kaspersky*. S'il n'y a pas de description de l'état en regard de l'icône, cela signifie que l'application administrée de Kaspersky sur l'appareil client a transmis à Kaspersky Security Center un état inconnu.

	Fichier dans le dossier **Sauvegarde** avec l'état *Non infecté, Protégé par un mot de passe* ou *Doit être envoyé à Kaspersky*. S'il n'y a pas de description de l'état en regard de l'icône, cela signifie que l'application administrée de Kaspersky sur l'appareil client a transmis à Kaspersky Security Center un état inconnu.
	Fichier dans le dossier **Menaces actives** avec le statut *Non infecté, Protégé par un mot de passe* or *Doit être envoyé à Kaspersky*. S'il n'y a pas de description de l'état en regard de l'icône, cela signifie que l'application administrée de Kaspersky sur l'appareil client a transmis à Kaspersky Security Center un état inconnu.

Recherche et exportation de données

Cette section fournit des informations sur les méthodes de recherche et d'exportation des données.

Recherche d'appareils

Kaspersky Security Center permet de rechercher les appareils sur la base des critères définis. Vous pouvez enregistrer les résultats de la recherche dans un fichier de texte.

La fonction de recherche permet de trouver les appareils suivants :

- Les appareils clients dans les groupes d'administration du Serveur d'administration et de ses Serveurs secondaires.
- Les appareils non définis administrés par un Serveur d'administration et ses Serveurs secondaires.

Pour rechercher les appareils clients du groupe d'administration, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez le dossier du groupe d'administration.
2. Dans le menu contextuel du dossier du groupe d'administration, sélectionnez l'option **Recherche**.
3. Sous les onglets de la fenêtre **Recherche**, indiquez les critères à appliquer à la recherche des appareils clients, et cliquez sur le bouton **Rechercher**.

   Les appareils qui correspondent aux critères de recherche définis s'afficheront dans le tableau, dans la partie inférieure de la fenêtre **Recherche**.

Pour rechercher les appareils non définis, procédez comme suit :

1. Dans l'arborescence de la console sélectionnez le dossier **Appareils non définis**.
2. Sélectionnez **Recherche** dans le menu contextuel du dossier **Appareils non définis**.
3. Sous les onglets de la fenêtre **Recherche**, indiquez les critères à appliquer à la recherche des appareils clients, et cliquez sur le bouton **Rechercher**.

   Les appareils qui correspondent aux critères de recherche définis s'afficheront dans le tableau, dans la partie inférieure de la fenêtre **Recherche**.

Pour rechercher les appareils qui appartiennent ou non au groupe d'administration, procédez comme suit :

1. Dans l'arborescence de la console, sélectionnez l'entrée **Serveur d'administration %s** .
2. Dans le menu contextuel de l'entrée, sélectionnez l'option **Recherche**.
3. Sous les onglets de la fenêtre **Recherche**, indiquez les critères à appliquer à la recherche des appareils clients, et cliquez sur le bouton **Rechercher**.

   Les appareils qui correspondent aux critères de recherche définis s'afficheront dans le tableau, dans la partie inférieure de la fenêtre **Recherche**.

La fenêtre **Recherche** vous permet également de rechercher les groupes d'administration et les Serveurs d'administration secondaires à l'aide de la liste déroulante située dans le coin en haut à droite de la fenêtre. La fonctionnalité de recherche des groupes d'administration et des Serveurs d'administration secondaires n'est pas disponible si vous ouvrez la fenêtre **Recherche** à partir du dossier **Appareils non définis**.

Pour rechercher les appareils, vous pouvez utiliser des expressions régulières dans les champs de la fenêtre **Recherche**.

La recherche de texte intégral dans la fenêtre **Recherche** est disponible :

- Sur l'onglet **Réseau**, dans le champ **Description**
- Sur l'onglet **Matériel**, dans les champs **Appareil**, **Éditeur** et **Description**

Paramètres de recherche des appareils

Les paramètres d'analyse des appareils administrés sont présentés ci-après. Les résultats de recherche s'affichent dans le tableau dans la partie inférieure de la fenêtre.

Réseau

L'onglet **Réseau** permet de configurer les critères de recherche d'appareils sur la base de leurs données de réseau :

- **Nom de l'appareil ou adresse IP**

  Nom de réseau Windows (nom NetBIOS) de l'appareil ou adresse IPv4 ou IPv6.

- **Domaine Windows**

  Les appareils faisant partie du domaine Windows indiqué seront affichés.

- **Groupe d'administration**

  Les appareils faisant partie du groupe d'administration seront affichés.

- Description

Texte apparaissant dans la fenêtre des propriétés de l'appareil : dans le champ **Description** de la section **Général**.

Pour décrire le texte dans le champ **Description**, vous pouvez utiliser les caractères suivants :

- A l'intérieur d'un seul mot :
  - *****. Remplace n'importe quelle ligne quel que soit le nombre de caractères.

  Exemple :

  Pour décrire les mots **Serveur**, **Serveurs** ou de serveur, il est possible d'utiliser la ligne **Serveur***.
  - **?.** Remplace un n'importe quel caractère.

  Exemple :

  Pour décrire les mots **Fenêtre** ou **Fenêtres**, il est possible d'utiliser la ligne **Fenêtr?**.

  Caractère ***** ou **?** ne peut pas être utilisé en tant que premier caractère dans la description du texte.
- Pour lier plusieurs mots :
  - Espace. Affiche l'ensemble des appareils dont la description contient l'un des mots de la liste.

  Exemple :

  Pour décrire la phrase contenant le mot **Secondaire** ou **Virtuel**, il est possible d'utiliser la ligne **Secondaire Virtuel**.
  - **+**. Avant le mot signifie la présence obligatoire du mot dans le texte.

  Exemple :

  Pour décrire la phrase contenant le mot **Secondaire**, et le mot **Virtuel**, il est possible de saisir la demande **+Secondaire+Virtuel**.
  - **-**. Avant le mot signifie l'absence obligatoire du mot dans le texte.

  Exemple :

  Pour décrire la phrase avec le mot **Secondaire** et sans le mot **Virtuel**, il est possible de saisir la demande **+Secondaire-Virtuel**.
  - **"<le texte>"**. Le fragment du texte entre guillemets doit être entièrement présent dans le texte.

  Exemple :

  Pour décrire la phrase contenant le groupe de mots **Serveur secondaire**, il est possible de saisir la demande **"Serveur secondaire"**.

- **Plage IP**

  Si l'option est activée, vous pouvez saisir les adresses IP de début et de fin de la plage IP à laquelle les appareils concernés doivent appartenir.

  Cette option est Inactif par défaut.

- **Administré par un autre Serveur d'administration**

  Sélectionnez l'une des valeurs ci-dessous :

  - **Oui**. Seuls les appareils clients administrés par d'autres Serveurs d'administration sont pris en compte.
  - **Non**. Seuls les appareils clients administrés par le même Serveur d'administration sont pris en compte.
  - **La valeur n'est pas sélectionnée**. Les critères ne sont pas appliqués.

Tags

L'onglet **Tags** permet de configurer la recherche d'appareils sur la base de mots clés (tags) ajoutés au préalable aux descriptions des appareils administrés :

- **Appliquer si au moins un tag sélectionné coïncide**

  Si l'option est activée, les appareils dont la description contient au moins l'un des tags sélectionnés figureront dans les résultats de la recherche.

  Si l'option est désactivée, seuls les appareils dont la description contient l'ensemble des tags sélectionnés figureront dans les résultats de la recherche.

  Cette option est Inactif par défaut.

- **Le tag doit être inclus**

  Si vous avez choisi cette option, les résultats de la recherche reprennent les appareils dont la description contient le tag sélectionné. Dans le cadre de la recherche d'appareils, vous pouvez utiliser le caractère * qui remplace n'importe quelle chaîne quel que soit le nombre de caractères.

  Cette option est sélectionnée par défaut.

- **Le tag doit être exclus**

  Si vous avez choisi cette option, les résultats de la recherche reprennent les appareils dont la description ne contient pas le tag sélectionné. Dans le cadre de la recherche d'appareils, vous pouvez utiliser le caractère * qui remplace n'importe quelle chaîne quel que soit le nombre de caractères.

Active Directory

Sur l'onglet **Active Directory**, vous pouvez spécifier que les appareils doivent être recherchés dans l'unité d'organisation (OU) ou le groupe Active Directory. Vous pouvez également inclure des appareils de toutes les unités d'organisation enfants de l'unité d'organisation Active Directory spécifiée dans la sélection. Pour sélectionner des appareils, définissez les paramètres suivants :

- **L'appareil se trouve dans une unité &organisationnelle Active Directory**

  Si l'option est activée, la sélection inclura les appareils de l'unité d'organisation Active Directory indiquée dans le champ de saisie.

  Cette option est Inactif par défaut.

- **Inclure les unités organisationnelles enfants**

  Si l'option est activée, la sélection inclut les appareils appartenant aux unités organisationnelles enfants de l'unité organisationnelle de domaine spécifiée.

  Cette option est Inactif par défaut.

- **L'appareil est un membre du &groupe Active Directory**

  Si l'option est activée, la sélection inclut les appareils issus du groupe Active Directory indiqué dans le champ de saisie.

  Cette option est Inactif par défaut.

Activité réseau

L'onglet **Activité réseau** permet d'indiquer les critères de recherche d'appareils sur la base de leur activité réseau :

- L'appareil est un point de distribution

  La liste déroulante permet de sélectionner les critères d'inclusion des appareils dans la sélection dans le cadre d'une recherche :

  - **Oui**. La sélection contient les appareils qui ne sont pas des points de distribution.
  - **Non**. Les appareils qui sont les points de distribution ne seront pas inclus dans la sélection.
  - **La valeur n'est pas sélectionnée**. Les critères ne sont pas appliqués.

- Maintenir la connexion au Serveur d'administration

  La liste déroulante permet de sélectionner les critères d'inclusion des appareils dans la sélection dans le cadre d'une recherche :

  - **Activé**. La sélection comportera des appareils sur lesquels la case **Maintenir la connexion au Serveur d'administration** est cochée.
  - **Désactivé**. La sélection comprendra des appareils sur lesquels la case **Maintenir la connexion au Serveur d'administration** est décochée.
  - **La valeur n'est pas sélectionnée**. Les critères ne sont pas appliqués.

- Changement du profil de connexion

  La liste déroulante permet de sélectionner les critères d'inclusion des appareils dans la sélection dans le cadre d'une recherche :

  - **Oui**. La sélection inclura les appareils connectés au Serveur d'administration suite au changement du profil de connexion.
  - **Non**. La sélection n'inclura pas les appareils connectés au Serveur d'administration suite au changement du profil de connexion.
  - **La valeur n'est pas sélectionnée**. Les critères ne sont pas appliqués.

- Dernière connexion au Serveur d'administration

  Cette case permet de définir les critères de recherche d'appareils selon la date et l'heure de la dernière connexion au Serveur d'administration.

  Si la case est cochée, le champ de saisie permet d'indiquer les valeurs de l'intervalle de temps (date et heure), durant lequel la dernière connexion de l'Agent d'administration installé sur l'appareil client avec le Serveur d'administration a été effectuée. La sélection contient les appareils qui s'inscrivent dans l'intervalle défini.

  Si la case est décochée, le critère ne sera pas appliqué.

  Celle-ci est décochée par défaut.

- Nouveaux appareils détectés lors d'un sondage du réseau

  Recherche de nouveaux appareils détectés lors du sondage du réseau au cours des derniers jours.

  Si l'option est activée, la sélection inclut seulement les nouveaux appareils détectés lors de la recherche d'appareils au cours du nombre de jours défini dans le champ **Période de détection (jours)**.

  Si l'option est désactivée, la sélection inclut tous les appareils détectés lors de la recherche d'appareils.

  Cette option est Inactif par défaut.

- Appareil visible

  La liste déroulante permet de sélectionner les critères d'inclusion des appareils dans la sélection dans le cadre d'une recherche :

  - **Oui**. L'application est reprise dans la sélection d'appareils visibles sur le réseau à l'heure actuelle.
  - **Non**. L'application est reprise dans la sélection d'appareils qui ne sont pas visibles sur le réseau à l'heure actuelle.
  - **La valeur n'est pas sélectionnée**. Les critères ne sont pas appliqués.

Application

L'onglet **Application** permet de définir les critères de recherche d'appareils sur la base de l'application administrée sélectionnée :

- Nom de l'application

  Liste déroulante qui permet de sélectionner les critères d'inclusion des appareils dans la sélection dans le cadre d'une recherche selon le nom de l'application de Kaspersky.

  La liste ne fournit que le nom des applications disposant de plug-ins d'administration installés sur le poste de travail de l'administrateur.

  Si l'application n'est pas sélectionnée, les critères ne sont pas appliqués.

- Version de l'application

  Champ qui permet de saisir les critères d'inclusion des appareils dans la sélection lors de la recherche par numéro de version de l'application de Kaspersky.

  Si le numéro de version n'est pas indiqué, les critères ne sont pas appliqués.

- Nom de la mise à jour critique

  Champ de saisie qui permet de saisir les critères d'inclusion des appareils dans la sélection lors de la recherche du paquet de mise à jour installé pour l'application par nom ou numéro.

  Si le champ n'est pas rempli, les critères ne sont pas appliqués.

- **Dernière mise à jour des modules**

  Cette option permet de définir les critères de recherche d'appareils selon l'heure de la dernière mise à jour des modules des applications installées sur les appareils.

  Si la case est cochée, le champ de saisie permet d'indiquer les valeurs de l'intervalle de temps (date et heure), durant lequel la dernière mise à jour des modules des applications installées sur les appareils a été effectuée.

  Si la case est décochée, le critère ne sera pas appliqué.

  Celle-ci est décochée par défaut.

- **L'appareil est administré par Kaspersky Security Center**

  La liste déroulante permet d'inclure les appareils qui sont administrés via Kaspersky Security Center dans la sélection d'appareils :

  - **Oui**. L'application ajoute les appareils administrés via Kaspersky Security Center à la sélection d'appareils.
  - **Non**. L'application inclut les appareils dans la sélection s'ils ne sont pas administrés via Kaspersky Security Center.
  - **La valeur n'est pas sélectionnée**. Les critères ne sont pas appliqués.

- **L'application de sécurité est installée**

  La liste déroulante permet d'ajouter à la sélection d'appareils ceux sur lesquels l'application de sécurité est installée :

  - **Oui**. L'application inclut les appareils sur lesquels l'application de sécurité est installée dans la sélection d'appareils.
  - **Non**. L'application inclut les appareils sur lequel l'application de sécurité n'est pas installée dans la sélection d'appareils.
  - **La valeur n'est pas sélectionnée**. Les critères ne sont pas appliqués.

Système d'exploitation

L'onglet **Système d'exploitation** permet de configurer les critères de recherche d'appareils suivants sur la base de leur type de système d'exploitation :

- **Version du système d'exploitation**

  Si la case est cochée, la liste permet de sélectionner les systèmes d'exploitation. Les appareils avec les systèmes d'exploitation indiqués installés sont inclus dans les résultats de recherche.

- **Taille de bit du système d'exploitation**

  Dans la liste déroulante, vous pouvez sélectionner l'architecture du système d'exploitation qui détermine la manière dont la règle de déplacement est appliquée à l'appareil (**Inconnu**, **x86**, **AMD64** ou **IA64**). Par défaut, aucune option n'est sélectionnée dans la liste, l'architecture du système d'exploitation n'est pas définie.

- **Version du service pack du système d'exploitation**

  Dans ce champ, vous pouvez indiquer la version du paquet du système d'exploitation installé (au format X.Y) en présence de laquelle la règle de déplacement s'applique à l'appareil. Par défaut, la version n'est pas indiquée.

- **Build du système d'exploitation**

  Ce paramètre concerne uniquement les systèmes d'exploitation Windows.

  Le numéro de version du système d'exploitation. Vous pouvez indiquer si le système d'exploitation sélectionné doit avoir un numéro de version égal, antérieur ou supérieur. Vous pouvez également configurer la recherche de tous les numéros de version à l'exception du numéro indiqué.

- **ID de version du système d'exploitation**

  Ce paramètre concerne uniquement les systèmes d'exploitation Windows.

  L'identifiant de version du système d'exploitation. Vous pouvez indiquer si le système d'exploitation sélectionné doit avoir un ID de version égal, antérieur ou supérieur. Vous pouvez également configurer la recherche de tous les ID de version à l'exception du numéro indiqué.

État de l'appareil

L'onglet **État de l'appareil** permet de définir les critères de recherche d'appareils sur la base de l'état de l'appareil fourni par l'application administrée :

- **État de l'appareil**

  Liste déroulante qui permet de sélectionner l'un des états de l'appareil : *OK*, *Critique* ou *Avertissement*.

- **État de la protection en temps réel**

  Liste déroulante vous permettant de sélectionner l'état de la protection en temps réel. Les appareils avec l'état indiqué de la protection en temps réel seront inclus dans la sélection.

- **Description d'état de l'appareil**

  Ce champ permet de cocher les cases en regard des conditions qui, lorsqu'elles sont remplies, affectent l'un des états suivants à l'appareil : *OK, Critique* ou *Avertissement*.

- **État de l'appareil défini par l'application**

  Liste déroulante vous permettant de sélectionner l'état de la protection en temps réel. Les appareils avec l'état indiqué de la protection en temps réel seront inclus dans la sélection.

Modules de protection

L'onglet **Modules de protection** permet de configurer les paramètres de recherche d'appareils clients sur la base de l'état de leur protection.

- **Date de publication des bases**

  Si l'option est activée, la recherche d'appareils clients s'exécute selon la date de publication des bases antivirus. Les champs de saisies permettent d'indiquer l'intervalle de temps sur la base duquel la recherche aura lieu.

  Cette option est Inactif par défaut.

- **Dernière analyse**

  Si l'option est activée, la recherche d'appareils clients s'exécute en fonction de l'heure de la dernière analyse des logiciels malveillants. Les champs de saisie permettent d'indiquer l'intervalle durant lequel la dernière analyse des logiciels malveillants a été exécutée.

  Cette option est Inactif par défaut.

- **Nombre total de détections de menaces**

  Si l'option est activée, la recherche d'appareils clients s'exécute en fonction du nombre de virus sélectionné. Les champs de saisie permettent d'indiquer les valeurs inférieures et supérieures du nombre de virus découverts.

  Cette option est Inactif par défaut.

Registre des applications

L'onglet **Registre des applications** permet de configurer la recherche d'appareils sur la base des applications qui y sont installées :

- **Nom de l'application**

  La liste déroulante qui permet de sélectionner l'application. Les appareils avec l'application indiquée installée seront inclus dans la sélection.

- **Version de l'application**

  Le champ de saisie à indiquer la version de l'application sélectionnée.

- **Éditeur**

  La liste déroulante qui permet de sélectionner l'éditeur de l'application installée sur l'appareil.

- **État de l'application**

  La liste déroulante qui permet de sélectionner l'état de l'application (*Installé*, *Non installé*). Les appareils sur lesquels l'application indiquée est installée ou non sont inclus dans la sélection en fonction de l'état sélectionné.

- **Rechercher selon la mise à jour**

  Si l'option est activée, la recherche sera exécutée selon les informations présentes dans les mises à jour des applications installées sur les appareils concernés. Une fois que vous avez sélectionné la case à cocher, les champs **Nom de l'application**, **Version de l'application** et **État de l'application** se changent respectivement en **Nom de la mise à jour**, **Version de la mise à jour** et **État**.

  Cette option est Inactif par défaut.

- **Nom de l'application de sécurité incompatible**

  La liste déroulante qui permet de sélectionner les applications antivirus des éditeurs tiers. Les appareils avec l'application sélectionnée installée seront inclus dans la sélection pendant la recherche.

- **Tag de l'application**

  La liste déroulante permet de sélectionner le tag de l'application. Tous les appareils sur lesquels sont installés des applications dont la description contient le tag sélectionné, sont repris dans la sélection d'appareils.

Hiérarchie des Serveurs d'administration

Sur l'onglet **Hiérarchie des Serveurs d'administration**, cochez la case **Inclure les données des Serveurs d'administration secondaires (jusqu'au niveau)** si vous souhaitez que les informations stockées sur les Serveurs d'administration secondaires soient prises en compte lors de la recherche d'appareils, et dans le champ de saisie, vous pouvez spécifier le niveau d'imbrication du Serveur d'administration secondaire à partir duquel les informations sont prises en compte lors de la recherche d'appareils. Celle-ci est décochée par défaut.

Machines virtuelles

L'onglet **Machines virtuelles** permet de configurer les paramètres de recherche d'appareils selon qu'il s'agit de machines virtuelles ou d'appareils inclus dans une infrastructure de type Virtual Desktop Infrastructure (VDI) :

- Est une machine virtuelle

  La liste déroulante permet de sélectionner les éléments suivants :

  - **Ignorer**.
  - **Non**. Les appareils recherchés ne doivent pas être des machines virtuelles.
  - **Oui**. Les appareils recherchés doivent être des machines virtuelles.

- Type de machine virtuelle

  La liste déroulante permet de sélectionner le fabricant de la machine virtuelle.

  Cette liste déroulante est disponible si les valeurs **Oui** ou **Ignorer** sont sélectionnées dans la liste déroulante **Est une machine virtuelle**.

- Membre d'une Virtual Desktop Infrastructure

  La liste déroulante permet de sélectionner les éléments suivants :

  - **Ignorer**.
  - **Non**. Les appareils recherchés ne doivent pas faire partie de Virtual Desktop Infrastructure.
  - **Oui**. Les appareils recherchés doivent faire partie de Virtual Desktop Infrastructure (VDI).

Matériel

L'onglet **Matériel** permet de configurer la recherche d'appareils clients en fonction du matériel installé :

- Appareil

  La liste déroulante permet de sélectionner le type d'unité. Tous les appareils avec cette unité sont inclus dans les résultats de la recherche.

  Le champ prend en charge la recherche en texte intégral.

- Éditeur

  La liste déroulante permet de sélectionner le fabricant de la machine virtuelle. Tous les appareils avec cette unité sont inclus dans les résultats de la recherche.

  Le champ prend en charge la recherche en texte intégral.

- **Description**

  Description de l'appareil ou du matériel. Les appareils dont la description figure dans le champ seront inclus dans la sélection.

  La description de l'appareil peut être librement saisie dans la fenêtre des propriétés. Le champ prend en charge la recherche en texte intégral.

- **Numéro d'inventaire**

  Le matériel dont le numéro d'inventaire figure dans le champ sera inclus dans la sélection.

- **Fréquence du processeur, en MHz**

  Plage de fréquence du processeur. Les appareils dont la fréquence du processeur est comprise dans la plage figurant dans les champs de saisie (inclus) seront inclus dans la sélection.

- **Noyaux virtuels**

  Plage de noyaux virtuels du processeur. Les appareils dont le nombre de processeurs est compris dans la plage figurant dans les champs de saisie (inclus) seront inclus dans la sélection.

- **Volume du disque dur (Go)**

  Plage de volumes du disque dur de l'appareil. Les appareils dont le volume du disque dur est compris dans la plage figurant dans les champs de saisie (inclus) seront inclus dans la sélection.

- **Taille de la mémoire RAM (Mo)**

  Plage de valeur du volume de mémoire RAM de l'appareil. Les appareils dont le volume de mémoire RAM est compris dans la plage figurant dans les champs de saisie (inclus) seront inclus dans la sélection.

Vulnérabilités et mises à jour

L'onglet **Vulnérabilités et mises à jour** permet de configurer la recherche d'appareils sur la base de leur source de mise à jour Windows Update :

- **WUA est transféré sur le Serveur d'administration**

  Dans la liste déroulante, vous pouvez sélectionner une des options de recherche suivantes :

  - **Oui**. Si cette option a été sélectionnée, les appareils qui reçoivent les mises à jour Windows Update depuis le Serveur d'administration sont inclus dans les résultats de recherche.
  - **Non**. Si cette option a été sélectionnée, les appareils qui reçoivent les mises à jour Windows Update depuis une autre source sont inclus dans les résultats de recherche.

Utilisateurs

L'onglet **Utilisateurs** permet de configurer les critères de recherche d'appareils sur la base des comptes utilisateur ayant ouvert une session dans le système d'exploitation.

- **Dernier utilisateur ayant accédé au système**

  Si l'option est activée, cliquez sur le bouton **Parcourir** pour définir un compte utilisateur. Les résultats de recherche comprennent les appareils dont le dernier accès au système d'exploitation a été effectué par l'utilisateur indiqué.

- **Utilisateur ayant accédé au moins une fois au système**

  Si l'option est activée, cliquez sur le bouton **Parcourir** pour définir un compte utilisateur. Les résultats de recherche comprennent les appareils sur lesquels l'utilisateur indiqué a déjà accédé au système.

Problèmes ayant une incidence sur l'état dans les applications administrées

L'onglet **Problèmes ayant une incidence sur l'état dans les applications administrées** permet de configurer la recherche sur la base des descriptions de leur état fournies par l'application administrée :

- **Description d'état de l'appareil**

  Vous pouvez cocher les cases pour les descriptions des états de l'application administrée dont la réception entraînera l'inclusion de l'appareil dans la sélection. Quand vous sélectionnez un état repris pour plusieurs applications, vous avez la possibilité de sélectionner cet état dans toutes les listes automatiquement.

État des modules des applications administrées

L'onglet **État des modules des applications administrées** permet de configurer les critères de recherche sur la base des états des composants des applications administrées :

- **État de la protection contre les fuites de données**

  Recherchez des appareils sur la base de l'état de la Protection contre les fuites de données (*Inconnu, Arrêté(e), En cours de démarrage, Suspendu(e), En cours d'exécution, Échec*).

- **État de la protection des serveurs de collaboration**

  Recherchez des appareils sur la base de l'état de la protection de collaboration du serveur (*Inconnu, Arrêté(e), En cours de démarrage, Suspendu(e), En cours d'exécution, Échec*).

- **État de Endpoint Protection des serveurs de messagerie**

  Recherchez des appareils sur la base de l'état de la protection du Serveur de messagerie (*Inconnu, Arrêté(e), En cours de démarrage, Suspendu(e), En cours d'exécution, Échec*).

- **État de Endpoint Sensor**

  Recherchez des appareils sur la base de l'état du module Endpoint Sensor (*Inconnu, Arrêté(e), En cours de démarrage, Suspendu(e), En cours d'exécution, Échec*).

Chiffrement

- **Chiffrement**

  Standard d'algorithme de chiffrement symétrique par bloc Advanced Encryption Standard (AES). La liste déroulante permet de sélectionner la taille de la clé de chiffrement (56, 128, 192 ou 256 bits).

  Les valeurs possibles sont *AES56*, *AES128*, *AES192*, *AES256*.

Segments dans le cloud

L'onglet **Segments dans le cloud** permet de configurer la recherche sur la base de l'appartenance à des segments dans le Cloud spécifiques :

- **L'appareil se trouve dans un segment dans le cloud**

  Si l'option est activée, vous pouvez cliquer sur le bouton **Parcourir** pour indiquer le segment dans lequel rechercher.

  Si l'option **Inclure les objets enfants** est également activée, la recherche est exécutée sur l'ensemble des objets enfants du segment indiqué.

  Seuls les appareils du segment choisi figurent dans les résultats de la recherche.

- **Appareil &découvert à l'aide de l'API**

  La liste déroulante permet de choisir s'vous pouvez détecter un appareil à l'aide des outils de l'API :

  - **AWS**. L'appareil est détecté via l'utilisation de l'API AWS, autrement dit, l'appareil est bel et bien dans l'environnement cloud AWS.
  - **Azure**. L'appareil est détecté via l'utilisation de l'API Azure, autrement dit, l'appareil est bel et bien dans l'environnement cloud Azure.
  - **Google Cloud.** L'appareil est détecté via l'utilisation de l'API Google, autrement dit, l'appareil est bel et bien dans le cloud Google.
  - **Non**. L'appareil n'est pas détecté à l'aide de l'API AWS, Azure ou Google, c'est-à-dire qu'il se trouve soit en dehors de l'environnement Cloud, soit dans l'environnement Cloud, mais il ne peut pas être détecté à l'aide d'une API.
  - **Pas de valeur**. Cette condition ne s'applique pas.

Modules de l'application

Cette section contient la liste des modules des applications dont le plug-in d'administration correspondant est installé dans la Console d'administration.

La section **Modules de l'application** permet de définir les critères d'inclusion des appareils dans une sélection sur la base des états et des numéros de version des modules faisant référence à l'application que vous avez sélectionnée :

- **État**

  Recherchez les appareils selon les états des modules renvoyés par une application au Serveur d'administration. Vous avez le choix entre les états suivants : *Aucune donnée de l'appareil*, *Arrêté*, *En cours de démarrage*, *Suspendu*, *En cours d'exécution*, *Dysfonctionnement* ou *Non installé*. Si le module sélectionné de l'application installée sur un appareil administré possède l'état indiqué, l'appareil est repris dans la sélection d'appareils.

  États envoyés par les applications :

  - *En cours de démarrage* : l'initialisation du module est actuellement en cours.
  - *En cours d'exécution* : le module est activé et fonctionne correctement.
  - *Suspendu* : le module est suspendu, par exemple, après que l'utilisateur a suspendu la protection dans l'application administrée.
  - *Dysfonctionnement* : une erreur s'est produite lors du fonctionnement du module.
  - *Arrêté* : le module est désactivé et ne fonctionne pas pour l'instant.
  - *Non installé* : l'utilisateur n'a pas sélectionné le module en vue de l'installer lors de la configuration de l'installation personnalisée de l'application.

  A la différence des autres états, l'état *Aucune donnée de l'appareil* n'est pas envoyé par les applications. Cette option indique que les applications n'ont aucune information sur l'état du module sélectionné. Cela peut se produire, par exemple, quand le module sélectionné n'appartient à aucune des applications installées sur l'appareil ou quand l'appareil est éteint.

- **Version**

  Recherchez les appareils en fonction du numéro de version du module que vous avez sélectionné dans la liste. Vous pouvez taper un numéro de version, par exemple `3.4.1.0`, puis indiquez si le numéro de version du module sélectionné doit être égal, antérieur ou postérieur. Vous pouvez également configurer la recherche de toutes les versions à l'exception du numéro indiqué.

Utilisation des masques dans les variables chaînes

Pour les variables de chaînes, il est permis d'utiliser les masques. Pour créer les masques, vous pouvez utiliser les expressions régulières suivantes :

- * – n'importe quelle ligne d'une longueur de 0 ou plus de symboles
- ? : n'importe quel symbole
- [<range>] : remplace n'importe quel caractère de la plage ou de l'ensemble indiqué.

  Par exemple : [0–9] : n'importe quel chiffre. [abcdef] : un des caractères a, b, c, d, e ou f.

Utilisation des expressions régulières dans la ligne de recherche

Vous pouvez saisir les expressions régulières suivantes dans la ligne de recherche pour rechercher des mots et des caractères particuliers :

- *. Remplace une succession d'un nombre indéterminé de caractères. Par exemple, pour rechercher les mots informatique, informaticien ou informations, saisissez `Server*` dans la ligne de recherche.
- ?. Remplace un n'importe quel caractère Par exemple, pour rechercher les mots Word ou Ward, saisissez `W?rd` dans la ligne de recherche.

  > Le texte dans la ligne de recherche ne peut pas commencer par ?.

- [<range>]. Remplace n'importe quel symbole de la plage indiquée ou de la multitude. Par exemple, pour rechercher n'importe quel chiffre, saisissez l'expression `[0-9` dans la ligne. Pour rechercher un des caractères a, b, c, d, e, f, saisissez l'expression `[abcdef` dans la ligne.

Vous pouvez saisir les expressions régulières suivantes dans la ligne de recherche dans le cadre d'une recherche en texte intégral :

- Espace. Le résultat est l'ensemble des appareils dont la description contient l'un des mots de la liste. Par exemple, pour rechercher des expressions contenant le mot " Secondaire " ou " Virtuel " (ou les deux), saisissez l'expression `Secondary Virtual` dans le champ de recherche.
- Symbole " plus " (+), AND ou &&. Avant le mot signifie la présence obligatoire du mot dans le texte. Par exemple, pour rechercher des expressions contenant le mot " Secondaire " et le mot " Virtuel ", saisissez une des expressions suivantes dans la ligne de recherche : `+Secondary+Virtual`, `Secondary AND Virtual`, `Secondary && Virtual`.
- OR ou ||. L'utilisation de cet opérateur entre deux mots indique qu'un mot ou l'autre doit figurer dans le texte. Par exemple, pour rechercher des expressions contenant le mot " Secondaire " ou le mot " Virtuel ", saisissez une des expressions suivantes dans le champ de recherche : `Secondary OR Virtual`, `Secondary || Virtual`.

- Symbole " mois " (-). Avant le mot signifie l'absence obligatoire du mot dans le texte. Par exemple, pour rechercher une expression qui doit contenir le mot Secondaire mais pas le mot Virtuel, il faut saisir l'expression `+Secondary-Virtual` dans le champ de recherche.

- `"< le texte >"`. Le fragment du texte entre guillemets doit être entièrement présent dans le texte. Par exemple, pour rechercher une expression contenant la combinaison Serveur secondaire, il faut saisir `"]] Serveur secondaire [["` dans le champ de recherche.

La recherche en texte intégral est disponible dans les groupes de filtrage suivants :

- Dans le groupe de filtrage de la liste des événements en fonction des colonnes **Événement** et **Description**.

- Dans le groupe de filtrage des comptes utilisateur en fonction de la colonne **Nom**.

- Dans le groupe de filtrage du registre des applications, en fonction de la colonne **Nom**, si dans le groupe **Afficher dans la liste**, le critère de filtrage **sans groupe** est sélectionné.

Exportation des listes depuis les fenêtres de dialogue

Dans les fenêtres de dialogue de l'application, vous pouvez exporter les listes des fichiers dans les fichiers de texte.

L'exportation de la liste des objets est possible pour les sections de la fenêtre de dialogue qui contiennent le bouton **Exporter dans un fichier**.

Paramètres des tâches

Cette section reprend tous les paramètres des tâches dans Kaspersky Security Center.

Paramètre de la tâche générale

Cette section contient les paramètres que vous pouvez afficher et configurer pour la plupart de vos tâches. La liste des paramètres disponibles dépend de la tâche que vous configurez.

Paramètres définis lors de la création d'une tâche

Vous pouvez définir les paramètres suivants lors de la création d'une tâche. Certains de ces paramètres peuvent également être modifiés dans les propriétés de la tâche créée.

- Paramètres de redémarrage du système d'exploitation :
  - **Ne pas redémarrer l'appareil**

    Les appareils clients ne redémarrent pas automatiquement après l'opération. Pour arrêter le fonctionnement, il faut redémarrer l'appareil (par exemple, manuellement ou à l'aide d'une tâche d'administration des appareils). Les informations sur la nécessité du redémarrage sont enregistrées dans les résultats de la tâche et dans l'état de l'appareil. Cette option convient aux tâches d' sur les serveurs et autres appareils pour lesquels la continuité des opérations est critique.

  - **Redémarrer l'appareil**

    Dans ce cas, le redémarrage des appareils clients est toujours exécuté automatiquement, si celui-ci est requis pour terminer l'opération. Cette option convient aux tâches d' sur des appareils pour lesquels des interruptions périodiques sont admises (débranchement, redémarrage).

  - **Confirmer l'action auprès de l'utilisateur**

    Le message qui signale que l'appareil client doit être redémarré manuellement s'affiche sur l'écran de l'appareil. Pour cette option, il est possible de configurer des paramètres avancés : le texte du message pour l'utilisateur, la fréquence du message, ainsi que le délai à l'issue duquel le redémarrage sera forcé (sans confirmation de l'utilisateur). Cette option convient le mieux pour les postes de travail sur lesquels les utilisateurs doivent pouvoir sélectionner l'heure de redémarrage qui leur convient le mieux.

    Cette option est sélectionnée par défaut.

  - **Répéter la demande toutes les (min.)**

    Quand cette option est activée, l'application invite l'utilisateur à redémarrer le système d'exploitation selon la fréquence indiquée.

    Cette option est activée par défaut. L'intervalle par défaut est de 5 minutes. La valeur peut être comprise entre 1 et 1 440 minutes.

    Si cette option est désactivée, l'invite est affichée une seule fois.

  - **Redémarrer au bout de (min.)**

    Après avoir averti l'utilisateur, l'application force le redémarrage du système d'exploitation à l'issue de l'intervalle défini.

    Cette option est activée par défaut. Le délai par défaut est de 30 minutes. La valeur peut être comprise entre 1 et 1 440 minutes.

  - **Forcer la fermeture des applications dans les sessions bloquées**

Les applications en cours d'exécution peuvent empêcher le redémarrage de l'appareil client. Par exemple, si un document est en train d'être modifié dans un logiciel de traitement de texte et qu'il n'est pas enregistré, l'application n'autorise pas le redémarrage de l'appareil.

Quand cette option est activée, l'arrêt forcé de ces applications sur un appareil verrouillé doit avoir lieu avant de pouvoir redémarrer l'appareil. Les utilisateurs pourraient perdre toute modification qui n'a pas été enregistrée à ce moment.

Si cette option est désactivée, un appareil verrouillé n'est pas redémarré. L'état de la tâche sur cet appareil indique qu'il faut redémarrer l'appareil. Les utilisateurs doivent quitter manuellement toutes les applications en cours d'exécution sur les appareils verrouillés, puis redémarrer ces appareils.

Cette option est Inactif par défaut.

- Paramètres du calendrier de la tâche :
  - **Paramètre Lancement planifié :**
    - Toutes les N heures

      La tâche s'exécute régulièrement, selon l'intervalle défini en heures, à partir de la date et heure définis.

      La tâche s'exécute par défaut toutes les six heures à partir de la date et de l'heure actuelles du système.

    - Tous les N jours

      La tâche s'exécute régulièrement, selon l'intervalle défini en jours. En outre, vous pouvez spécifier la date et l'heure de la première exécution de la tâche. Ces options supplémentaires deviennent disponibles si elles sont prises en charge par l'application pour laquelle vous créez la tâche.

      La tâche s'exécute par défaut chaque jour, à partir de la date et de l'heure actuelle du système.

    - Toutes les N semaines

      La tâche s'exécute régulièrement, selon l'intervalle défini en semaines, le jour indiqué de la semaine et à l'heure indiquée.

      La tâche s'exécute par défaut chaque lundi à l'heure système actuelle.

    - Toutes les N minutes

      La tâche s'exécute régulièrement, à l'intervalle défini en minutes, à partir de l'heure indiquée le jour de la création de la tâche.

      La tâche s'exécute par défaut toutes les 30 minutes, à partir de l'heure actuelle du système.

    - Chaque jour (passage à l'heure d'été non pris en charge)

La tâche s'exécute régulièrement, selon l'intervalle défini en jours. Cette programmation ne tient pas compte du passage à l'heure d'été. Cela signifie que lorsque les horloges sont avancées ou reculées d'une heure au début ou à la fin de l'été, l'heure de lancement réelle de la tâche ne change pas.

Nous déconseillons d'adopter cette programmation. Elle est requise pour la rétrocompatibilité avec Kaspersky Security Center.

La tâche démarre par défaut chaque jour à l'heure système actuelle.

- **Chaque semaine**

  La tâche s'exécute chaque semaine, le jour défini et à l'heure indiquée.

- **Par jours de la semaine**

  La tâche s'exécute régulièrement les jours définis de la semaine, à l'heure indiquée.

  Par défaut, la tâche s'exécute chaque vendredi à 18h00.

- **Chaque mois**

  La tâche s'exécute régulièrement le jour du mois défini, à l'heure indiquée.

  Si le jour en question ne figure pas dans le mois, la tâche s'exécute le dernier jour.

  La tâche s'exécute par défaut le premier jour de chaque mois, à l'heure système actuelle.

- **Manuel**

  La tâche ne s'exécute pas automatiquement. Vous pouvez uniquement la lancer manuellement.

  Cette option est sélectionnée par défaut.

- **Chaque mois, les jours indiqués des semaines sélectionnées**

  La tâche s'exécute régulièrement les jours du mois définis, à l'heure indiquée.

  Par défaut, aucun jour du mois n'est sélectionné. L'heure de début par défaut est 18:00.

- **Lors du téléchargement des mises à jour dans le stockage**

  La tâche s'exécute après le téléchargement des mises à jour dans le stockage. Par exemple, vous pouvez utiliser cette programmation pour rechercher les vulnérabilités et les mises à jour requises.

- **Lors de la détection d'une attaque de virus**

La tâche s'exécute après un événement *Attaque de virus* de virus. Sélectionnez les types d'application qui vont surveiller les propagations de virus. Les types suivants de Application sont présent :

- Antivirus pour postes de travail et serveurs de fichiers
- Antivirus de protection du périmètre
- Antivirus pour systèmes de messagerie

Tous les types d'application sont cochés par défaut.

Il se peut que vous souhaitiez exécuter différentes tâches en fonction du type d'application de sécurité qui signale une propagation de virus. Dans ce cas, supprimez la sélection des types d'application dont vous n'avez pas besoin.

- Après l'exécution d'une autre tâche

  La tâche actuelle démarre à la fin d'une autre tâche. Cette option ne fonctionne que si les deux tâches sont affectées aux mêmes appareils. Par exemple, vous pouvez exécuter la tâche *Administration des appareils* avec l'option **&Activer l'appareil** et, une fois celle-ci terminée, exécuter la tâche de *recherche de virus* comme tâche de déclenchement.

  Il faut sélectionner la tâche de déclenchement dans le tableau et l'état avec lequel cette tâche doit se terminer (**Terminée avec succès** ou **Échec**).

  Si nécessaire, vous pouvez rechercher, trier et filtrer les tâches dans le tableau comme suit :

  - Saisissez le nom de la tâche dans le champ de recherche pour rechercher une tâche par son nom.
  - Cliquez sur l'icône de tri pour trier les tâches par nom.

    Par défaut, les tâches sont triées par ordre alphabétique croissant.
  - Cliquez sur l'icône du filtre, et dans la fenêtre qui s'ouvre, filtrez les tâches par groupe, puis cliquez sur le bouton **Appliquer**.

- Lancer les tâches non exécutées

  Cette option détermine le comportement d'une tâche si un appareil client n'est pas visible sur le réseau quand la tâche est sur le point de démarrer.

  Si la case est Activé, lors du lancement suivant de l'application de Kaspersky sur cet appareil client, une tentative de lancement de la tâche sera faite. Si la programmation de la tâche est **Manuel**, **Une fois** ou **Immédiatement**, la tâche est immédiatement lancée dès que l'appareil apparaît sur le réseau ou immédiatement après l'inclusion de l'appareil dans la zone d'action de la tâche.

  Si cette option est désactivée, seules les tâches planifiées s'exécutent sur les appareils clients. Pour les planifications **Manuel**, **Une fois** et **Immédiatement**, les tâches s'exécutent uniquement sur les appareils clients qui sont visibles sur le réseau. Par exemple, vous pouvez désactiver cette option pour une tâche qui consomme des ressources que vous voulez exécuter uniquement en dehors des heures de bureau.

  Cette option est Inactif par défaut.

- Adopter un décalage aléatoire automatique pour les lancements de tâche

Si cette option est activée, la tâche est lancée sur les appareils clients de manière aléatoire au cours d'un intervalle défini. C'est ce qu'on appelle un *lancement échelonné d'une tâche*. Un lancement échelonné de tâche permet d'éviter la communication simultanée d'un nombre important d'appareils clients avec le Serveur d'administration lors du lancement de la tâche programmée.

Le temps du lancement aléatoire est automatiquement calculée lors de la création d'une tâche selon le nombre d'appareils clients sur lesquels la tâche est diffusée. Par la suite, la tâche démarre toujours à l'heure de lancement calculée. Toutefois, quand les paramètres de la tâche sont modifiés ou si la tâche est lancée manuellement, la valeur calculée de l'heure de lancement de la tâche est modifiée.

Si la case n'est pas cochée, le lancement de la tâche sur les appareils clients s'opère selon la planification.

- **Décaler aléatoirement le lancement de la tâche dans un intervalle de (min.)**

  Si cette option est activée, la tâche est lancée sur les appareils clients de manière aléatoire au cours de l'intervalle défini. Un lancement échelonné de tâche permet d'éviter la communication simultanée d'un nombre important d'appareils clients avec le Serveur d'administration lors du lancement de la tâche programmée.

  Si la case n'est pas cochée, le lancement de la tâche sur les appareils clients s'opère selon la planification.

  Cette option est Inactif par défaut. Par défaut, la valeur de cet intervalle est de une minute.

- Les appareils auxquels les tâches seront affectées :
  - **Sélectionner les appareils détectés sur le réseau par le Serveur d'administration**

    la tâche est affectée à un ensemble d'appareils. L'ensemble d'appareils peut reprendre aussi bien des appareils de groupes d'administration que des appareils non définis.

    Par exemple, vous pourriez utiliser cette option dans une tâche d'installation d'un Agent d'administration sur des appareils non définis.

  - **Définir les adresses des appareils manuellement ou les importer à partir d'une liste**

    Vous pouvez définir les noms NetBIOS, les noms DNS, les adresses IP, ainsi que les plages d'adresses IP auxquels il convient d'affecter la tâche.

    Vous pourriez utiliser cette option pour exécuter une tâche pour un sous-réseau défini. Par exemple, vous pourriez souhaiter installer une certaine application sur les appareils des comptables ou analyser des appareils dans un sous-réseau qui est probablement infecté.

  - **Attribuer la tâche à une sélection d'appareils**

    La tâche est affectée aux appareils qui appartiennent à une sélection d'appareils. Vous pouvez définir une des sélections existantes.

    Par exemple, vous pourriez souhaiter utiliser cette option pour exécuter une tâche sur des appareils dotés d'une version du système d'exploitation spécifique.

  - **Attribuer la tâche à un groupe d'administration**

    La tâche est affectée aux appareils qui appartiennent à un groupe d'administration. Vous pouvez renseigner un des groupes existants ou en créer un.

    Par exemple, vous pourriez souhaiter utiliser cette option pour exécuter une tâche d'envoi de messages pour les utilisateurs si le message est particulier pour les appareils repris dans un groupe d'administration spécifique.

    Si une tâche est attribuée à un groupe d'administration, l'onglet **Sécurité** ne s'affiche pas dans la fenêtre des propriétés de la tâche, car les tâches de groupe sont soumises aux paramètres de sécurité des groupes auxquels elles s'appliquent.

- Paramètres du compte :
  - **Compte par défaut**

    La tâche sera lancée sous le même compte utilisateur sous lequel l'application, exécutant cette tâche, a été installée et lancée.

    Cette option est sélectionnée par défaut.

  - **Indiquer un compte**

    Remplissez les champs **Compte utilisateur** et **Mot de passe** pour définir les détails d'un compte à partir duquel la tâche est exécutée. Le compte doit disposer de droits suffisants pour cette tâche.

- **Compte utilisateur**

  Le compte utilisateur au nom duquel la tâche sera lancée.

- **Mot de passe**

  Mot de passe du compte utilisateur au nom duquel la tâche sera lancée.

Si l'Agent d'administration n'est pas installé sur votre appareil cible, il faut indiquer le compte à utiliser sur l'appareil cible pour accéder au partage admin$. Le compte que vous définissez est uniquement destiné à copier les données sur votre appareil. Si l'Agent d'administration est installé sur votre appareil cible, les données sont copiées par l'intermédiaire de l'Agent d'administration et vous n'avez pas besoin de préciser de compte lors de la création de la tâche.

Paramètres définis après la création de la tâche

Vous pouvez définir les paramètres suivants uniquement après qu'une tâche a été créée.

- Paramètres de la tâche de groupe :
  - **Distribuer aux sous-groupes**

    Cette option est disponible uniquement dans les paramètres des tâches de groupe.

    Lorsque cette option est activée, la zone d'action de la tâche inclut :

    - Le groupe d'administration que vous avez sélectionné lors de la création de la tâche.
    - Les groupes d'administration subordonnés au groupe d'administration sélectionné à n'importe quel niveau inférieur dans la hiérarchie des groupes.

    Lorsque cette option est désactivée, la zone d'action de la tâche inclut uniquement le groupe d'administration que vous avez sélectionné lors de la création de la tâche.

    Cette option est activée par défaut.

  - **&Envoyer aux Serveurs d'administration secondaire et virtuel**

    Lorsque cette option est activée, la tâche effective sur le Serveur d'administration principal est également appliquée sur les Serveurs d'administration secondaires (y compris virtuels). Si une tâche du même type existe déjà sur le Serveur d'administration secondaire, les deux tâches sont appliquées sur le Serveur d'administration secondaire, celui existant et celui hérité du Serveur d'administration principal.

    Cette option est disponible uniquement lorsque l'option **Distribuer aux sous-groupes** est activée.

    Cette option est Inactif par défaut.

- Paramètres de programmation avancés :
  - **Allumer les appareils en utilisant la fonctionnalité Wake-on-LAN avant le lancement de la tâche (min.)**

    Le système d'exploitation sur l'appareil démarre au délai indiqué avant le lancement de la tâche. Par défaut, la valeur de cet délai de est de une minute.

    Activez cette option si vous souhaitez que la tâche soit exécutée sur tous les appareils clients de la zone d'action de la tâche, y compris pour les appareils éteints alors que la tâche est sur le point de démarrer.

    Si vous souhaitez que l'appareil soit automatiquement éteint une fois la tâche terminée, activez l'option **Arrêter les appareils après la fin de la tâche**. Cette option se trouve dans la même fenêtre.

    Cette option est Inactif par défaut.

  - **Arrêter les appareils après la fin de la tâche**

Par exemple, vous pouvez activer cette option pour une tâche d'installation de mise à jour qui installe les mises à jour sur les appareils client chaque vendredi après la fermeture des bureaux, puis éteint ces appareils pour le week-end.

Cette option est Inactif par défaut.

- **Arrêter la tâche si elle prend plus de (min.)**

  A l'issue du délai défini, la tâche s'arrêt automatiquement, qu'elle soit finie ou non.

  Activez cette option si vous souhaitez interrompre (ou arrêter) les tâches dont l'exécution dure trop longtemps.

  Cette option est Inactif par défaut. La durée d'exécution de la tâche par défaut est de 120 minutes.

- Paramètres des notifications :
  - Groupe **Sauvegarder l'historique de la tâche**:
    - &Sur le Serveur d'administration pendant (jours)

      Les événements de l'application en rapport avec l'exécution de la tâche sur tous les appareils clients de la zone d'action de la tâche sont stockés sur le Serveur d'administration pendant le nombre de jours indiqué. A l'issue de cette période, les informations sont supprimées du Serveur d'administration.

      Cette option est activée par défaut.

    - Conserver dans le journal des événements du SE sur l'&appareil

      Les événements de l'application en rapport avec l'exécution de la tâche sont stockés localement dans le journal des événements Windows de chaque appareil client.

      Cette option est Inactif par défaut.

    - Conserver dans le journal des événements du système d'exploitation du &Serveur d'admin

      Les événements de l'application en rapport avec l'exécution de la tâche sur tous les appareils clients de la zone d'action de la tâche sont stockés centralement dans le journal des événements Windows du système d'exploitation du Serveur d'administration.

      Cette option est Inactif par défaut.

    - Sauvegarder tous les événements

      Quand cette option est sélectionnée, tous les événements liés à la tâche sont enregistrés dans les journaux des événements.

    - Sauvegarder les événements relatifs à la progression de la tâche

      Quand cette option est sélectionnée, seuls les événements liés à l'exécution de la tâche sont enregistrés dans les journaux des événements.

    - Sauvegarder uniquement le résultat de la tâche

      Quand cette option est sélectionnée, seuls les événements liés aux résultats des tâches sont enregistrés dans les journaux des événements.

  - Informer l'administrateur des résultats de l'exécution de la tâche

    Vous pouvez choisir les méthodes selon lesquelles les administrateurs reçoivent des notifications relatives aux résultats de l'exécution de la tâche : par email, par SMS ou via le lancement du fichier exécutable. Pour configurer les notifications, cliquez sur le lien **Paramètres**.

    Par défaut, toutes les méthodes de notification sont désactivées.

  - Notifier uniquement les erreurs

Si cette option est activée, les administrateurs ne sont informés que si l'exécution d'une tâche se termine avec une erreur.

Si cette option est désactivée, les administrateurs sont informés après chaque exécution de la tâche.

Cette option est activée par défaut.

- Paramètres de sécurité
- Paramètres de la zone d'action de la tâche

  Selon la définition de la zone d'action de la tâche, les paramètres suivants sont proposés :

  - Appareils

    Si la zone d'action de la tâche est déterminée par un groupe d'administration, vous pouvez voir ce groupe. Aucune modification n'est disponible ici. Cependant, vous pouvez définir **Exclusions de la zone d'action de la tâche**.

    Si la zone d'action d'une tâche est déterminée par une liste d'appareils, vous pouvez modifier cette liste en ajoutant et en supprimant des appareils.

  - Sélection d'appareils

    Vous pouvez modifier la sélection d'appareils à laquelle la tâche est appliquée.

  - Exclusions de la zone d'action de la tâche

    Vous pouvez définir les groupes d'appareils auxquels la tâche n'est pas appliquée. Les groupes à exclure peuvent uniquement être des sous-groupes du groupe d'administration auquel la tâche est appliquée.

- **Historique des révisions**

Télécharger les mises à jour dans les paramètres de la tâche du stockage du Serveur d'administration

Paramètres définis lors de la création d'une tâche

Vous pouvez définir les paramètres suivants lors de la création d'une tâche. Certains de ces paramètres peuvent également être modifiés dans les propriétés de la tâche créée.

- **Sources des mises à jour**

  Les ressources suivantes peuvent faire office de source des mises à jour pour le Serveur d'administration :

  - Serveurs de mises à jour de Kaspersky

    Serveurs HTTP(S) Kaspersky sur lesquels les applications de Kaspersky récupèrent les mises à jour des bases de données et des modules de l'application. Par défaut, le Serveur d'administration communique avec les serveurs de mise à jour de Kaspersky et télécharge les mises à jour au moyen du protocole HTTPS. Vous pouvez configurer le Serveur d'administration pour qu'il utilise le protocole HTTP au lieu du protocole HTTPS.

    Sélectionné par défaut.

  - Serveur d'administration principal

    Cette ressource s'applique aux tâches créées pour un Serveur d'administration virtuel ou secondaire.

  - Dossier local ou réseau

    Un dossier local ou de réseau qui contient les mises à jour les plus récentes. Un dossier de réseau peut être un serveur FTP ou HTTP ou un dossier partagé SMB. Si un dossier réseau nécessite une authentification, seul le protocole SMB est pris en charge. Lors de la sélection du dossier local, il faut indiquer le dossier sur l'appareil avec le Serveur d'administration installé.

    > Un serveur FTP ou http ou un dossier de réseau utilisé par une source des mises à jour doit contenir une structure de dossiers (avec les mises à jour) qui correspond à la structure créée lors de l'utilisation des serveurs de mise à jour de Kaspersky.

- **Autres paramètres**

  Forcer la mise à jour des Serveurs d'administration secondaires

  Si cette option est activée, le Serveur d'administration lance les tâches de mise à jour sur les Serveurs d'administration secondaires dès que de nouvelles mises à jour sont téléchargées. Les tâches de mise à jour sont lancées en utilisant la source de mise à jour configurée dans les propriétés de la tâche sur les Serveurs d'administration secondaires.

  Si cette option est désactivée, les tâches de mise à jour sur les Serveurs d'administration secondaires sont lancées conformément à leur programmation.

  Cette option est Inactif par défaut.

  Copier les mises à jour récupérées dans des dossiers complémentaires

Après que le Serveur d'administration reçoit les mises à jour, il les copie dans les dossiers indiqués. Utilisez cette option si vous voulez administrer manuellement la distribution des mises à jour sur votre réseau.

Par exemple, vous pourriez vouloir utiliser cette option dans la situation suivante : le réseau de votre organisation comprend plusieurs sous-réseaux indépendants et les appareils sur chacun de ces sous-réseaux n'ont pas accès aux autres sous-réseaux. Toutefois, les appareils dans tous les sous-réseaux ont accès à un dossier partagé central. Dans ce cas, vous installez le Serveur d'administration dans un des sous-réseaux pour télécharger les mises à jour depuis les serveurs de mise à jour de Kaspersky, vous activez cette option, puis vous définissez ce dossier partagé réseau. Dans les tâches de téléchargement des mises à jour dans le stockage pour les autres Serveurs d'administration, définissez le nom du dossier réseau partagé en tant que source des mises à jour.

Cette option est Inactif par défaut.

Ne pas forcer la mise à jour des appareils et des Serveurs d'administration secondaires avant la fin de la copie

Les tâches de téléchargement des mises à jour sur les appareils clients et les Serveurs d'administration secondaires démarrent uniquement après la copie de ces mises à jour depuis le dossier de mise à jour principal vers les dossiers de mise à jour complémentaires.

Cette option doit être activée si les appareils clients et les Serveurs d'administration secondaires téléchargent les mises à jour depuis des dossiers réseau complémentaires.

Cette option est Inactif par défaut.

Paramètres définis après la création de la tâche

Vous pouvez définir les paramètres suivants uniquement après qu'une tâche a été créée.

- Section **Paramètres**, bloc **Contenu des mises à jour**

  Télécharger des fichiers diff

  Cette option active la fonction de téléchargement des fichiers diff.

  Cette option est Inactif par défaut.

- Section **Vérification de la mise à jour**

  Vérifier les mises à jour avant de les déployer

  Le Serveur d'administration télécharge les mises à jour depuis la source, les enregistre dans un stockage provisoire et exécute la tâche définie dans le champ **Tâche d'analyse des mises à jour**. Si la tâche aboutit, les mises à jour sont copiées depuis le stockage local vers un dossier partagé sur le Serveur d'administration, puis elles sont distribuées sur tous les appareils pour lesquels le Serveur d'administration fait office de source des mises à jour (les tâches dont le type de planification est **Lors du téléchargement des mises à jour dans le stockage** sont lancées). La tâche de téléchargement des mises à jour sur les référentiels se termine uniquement après la fin de la tâche d'*analyse des mises à jour*.

  Cette option est Inactif par défaut.

  Tâche d'analyse des mises à jour

  Cette tâche vérifie les mises à jour téléchargées avant leur distribution à l'ensemble des appareils dont la source des mises à jour est le Serveur d'administration.

  Dans ce champ, vous pouvez indiquer la tâche de *vérification des mises à jour* créée précédemment. Sinon, vous pouvez aussi créer une nouvelle tâche d'*analyse des mises à jour*.

Paramètres de la tâche de Téléchargement des mises à jour sur les stockages des points de distribution

Paramètres définis lors de la création d'une tâche

Vous pouvez définir les paramètres suivants lors de la création d'une tâche. Certains de ces paramètres peuvent également être modifiés dans les propriétés de la tâche créée.

- **Sources des mises à jour**

  Les ressources suivantes peuvent faire office de source des mises à jour pour le point de distribution :

  - Serveurs de mise à jour de Kaspersky

    Serveurs HTTP(S) Kaspersky sur lesquels les applications de Kaspersky récupèrent les mises à jour des bases de données et des modules de l'application.

    Par défaut, cette option est sélectionnée.

  - Serveur d'administration principal

    Cette ressource s'applique aux tâches créées pour un Serveur d'administration virtuel ou secondaire.

  - Dossier local ou réseau

    Un dossier local ou de réseau qui contient les mises à jour les plus récentes. Un dossier de réseau peut être un serveur FTP ou HTTP ou un dossier partagé SMB. Si un dossier réseau nécessite une authentification, seul le protocole SMB est pris en charge. Lors de la sélection du dossier local, il faut indiquer le dossier sur l'appareil avec le Serveur d'administration installé.

    > Un serveur FTP ou http ou un dossier de réseau utilisé par une source des mises à jour doit contenir une structure de dossiers (avec les mises à jour) qui correspond à la structure créée lors de l'utilisation des serveurs de mise à jour de Kaspersky.

- **Autres paramètres** → **Dossier de stockage des mises à jour**

  Le chemin d'accès au dossier spécifié pour stocker les mises à jour enregistrées. Vous pouvez copier le chemin du dossier spécifié dans un presse-papiers. Vous ne pouvez pas modifier le chemin d'accès à un dossier spécifié pour une tâche de groupe.

Paramètres définis après la création de la tâche

Vous pouvez définir le paramètre suivant dans la section **Paramètres**, dans le groupe **Contenu des mises à jour**, uniquement après la création d'une tâche.

Télécharger des fichiers diff

Cette option active la fonction de téléchargement des fichiers diff.

Cette option est Inactif par défaut.

La tâche Recherche de vulnérabilités et de mises à jour requises est créée

Paramètres définis lors de la création d'une tâche

Vous pouvez définir les paramètres suivants lors de la création d'une tâche. Certains de ces paramètres peuvent également être modifiés dans les propriétés de la tâche créée.

- **Rechercher les vulnérabilités et les mises à jour indiquées par Microsoft**

  Lors de la recherche de vulnérabilités et de mises à jour, Kaspersky Security Center utilise les informations sur les mises à jour Microsoft applicables à partir de la source des mises à jour Microsoft disponibles à ce moment là.

  Par exemple, pensez à désactiver cette option si vous avez différentes tâches avec différents paramètres pour les mises à jour Microsoft et les mises à jour d'applications tierces.

  Cette option est activée par défaut.

  Les informations sur les mises à jour facultatives de Microsoft Windows Update ne sont pas envoyées au Serveur d'administration.

- **Se connecter au serveur de mise à jour pour mettre à jour les données**

L'Agent de mises à jour Windows sur un appareil administré se connecte à la source des mises à jour Microsoft. Les serveurs suivants peuvent servir de source de mises à jour Microsoft :

- Serveur d'administration de Kaspersky Security Center (voir les paramètres de stratégie de l'Agent d'administration)
- Serveur Windows sur lequel Microsoft Windows Server Update Services (WSUS) est déployé dans le réseau de votre organisation
- Serveurs de mises à jour Microsoft

Si cette option est activée, l'Agent de mises à jour Windows sur un appareil administré se connecte à la source de mise à jour Microsoft pour actualiser les informations relatives aux mises à jour Microsoft Windows applicables.

Si cette option est désactivée, l'Agent de mises à jour Windows sur un appareil administré utilise les informations relatives aux mises à jour Microsoft Windows obtenues antérieurement auprès de la source des mises à jour Microsoft.

La connexion à la source des mises à jour Microsoft peut requérir beaucoup de ressources. Pensez à désactiver cette option si vous définissez une connexion régulière à cette source de mises à jour dans une autre tâche ou dans les propriétés de la stratégie de l'Agent d'administration, dans la section **Mises à jour et vulnérabilités du logiciel**. Si vous ne souhaitez pas désactiver cette option, pour réduire la surcharge, vous pouvez configurer la planification des tâches pour randomiser le délai de démarrage des tâches dans les 360 minutes.

Cette option est activée par défaut.

La combinaison des options suivantes des paramètres de la stratégie de l'Agent d'administration définit le mode d'obtention des mises à jour :

- L'Agent de mises à jour Windows sur un appareil administré se connecte au Serveur de mises à jour pour obtenir les mises à jour uniquement si l'option **Se connecter au serveur de mise à jour pour mettre à jour les données** est activée dans les propriétés de la tâche *Recherche de vulnérabilités et de mises à jour requises* et si l'option **Mode de recherche des mises à jour Windows Update** est définie sur **Actif** dans les paramètres de la stratégie de l'Agent d'administration.
- Si vous n'avez pas besoin de l'Agent d'administration pour établir une connexion à la source des mises à jour Microsoft Windows et télécharger les mises à jour lors de l'exécution de la tâche *Recherche de vulnérabilités*, vous pouvez définir l'option **Mode de recherche des mises à jour Windows Update** sur **Passif**, tandis que l'option **Se connecter au serveur de mise à jour pour mettre à jour les données** doit rester activée. Cela vous permet d'économiser des ressources et d'utiliser les mises à jour de Windows déjà reçues pour vérifier la présence de vulnérabilités. Vous pouvez utiliser le mode passif si vous configurez la réception des mises à jour Microsoft Windows différemment. Si la réception des mises à jour Microsoft Windows n'est pas configurée d'une autre manière, ne définissez pas l'option du **Mode de recherche des mises à jour Windows Update** sur **Passif**, car dans ce cas, les informations sur les mises à jour ne seront jamais reçues.
- Quel que soit l'état de l'option **Se connecter au serveur de mise à jour pour mettre à jour les données** (activé ou désactivé), si l'option **Mode de recherche des mises à jour Windows Update** est définie sur **Désactivé**, Kaspersky Security Center ne demande aucune information sur les mises à jour.

- Rechercher les vulnérabilités et les mises à jour de tiers indiquées par Kaspersky

Si cette option est activée, Kaspersky Security Center recherche des vulnérabilités et les mises à jour requises des produits tiers (applications développées par des éditeurs d'application autres que Kaspersky et Microsoft) dans le Registre Windows et dans les dossiers définis sous **Indiquez les chemins pour la recherche avancée des applications dans le système de fichiers**. La liste complète des produits tiers pris en charge est administrée par Kaspersky.

Si cette option est désactivée, Kaspersky Security Center ne recherche pas les vulnérabilités et les mises à jour requises pour les applications tiers. Par exemple, pensez à désactiver cette option si vous avez différentes tâches avec différents paramètres pour les mises à jour Microsoft Windows et les mises à jour d'applications tierces.

Cette option est activée par défaut.

- **Indiquez les chemins pour la recherche avancée des applications dans le système de fichiers**

  Les dossiers dans lesquels Kaspersky Security Center recherche des produits tiers qui requièrent une correction de la vulnérabilité et l'installation d'une mise à jour. Vous pouvez utiliser des variables système.

  Indiquez les dossiers dans lesquels les applications doivent être installées. Par défaut, la liste contient les dossiers système dans lesquels la majorité des applications sont installées.

- **Activer le diagnostic avancé**

  Quand cette fonction est activée, l'Agent d'administration enregistre des fichiers de trace même si l'écriture de fichiers de trace est désactivée pour l'Agent d'administration dans l'utilitaire de diagnostic à distance Kaspersky Security Center. Les traces sont enregistrées dans deux fichiers en alternance la taille de chacun de ces fichiers est déterminée par la valeur paramètre **Taille maximale (Mo) des fichiers de diagnostic avancé**. Quand les deux fichiers sont remplis, l'Agent d'administration écrit à nouveau dans ceux-ci. Les fichiers avec les traces sont stockés dans le dossier %WINDIR%\Temp. Ces fichiers sont accessibles dans l'utilitaire de diagnostic à distance, vous pouvez les télécharger ou les supprimer à cet endroit.

  Quand cette fonction est désactivée, l'Agent d'administration enregistre les traces conformément aux paramètres définis dans l'utilitaire de diagnostic à distance Kaspersky Security Center. Aucune trace complémentaire n'est écrite.

  Lors de la création d'une tâche, il n'est pas nécessaire d'activer le diagnostic avancé. Par contre, vous pouvez activer cette fonction plus tard si, par exemple, une tâche échoue sur certains appareils et que vous souhaitez obtenir des informations complémentaires lors d'une autre exécution de la tâche.

  Cette option est Inactif par défaut.

- **Taille maximale (Mo) des fichiers de diagnostic avancé**

  La valeur par défaut est de 100 Mo, mais elle peut se situer entre 1 et 2 048 Mo. Il peut arriver qu'un expert du Support Technique de Kaspersky vous demande de modifier la valeur par défaut lorsque les informations reprises dans les fichiers de diagnostic avancés que vous avez envoyés ne suffisent pas pour résoudre le problème.

Paramètres de la tâche Installation des mises à jour requises et correction des vulnérabilités

Paramètres définis lors de la création d'une tâche

Vous pouvez définir les paramètres suivants lors de la création d'une tâche. Certains de ces paramètres peuvent également être modifiés dans les propriétés de la tâche créée.

- **Définissez les règles d'installation des mises à jour**

  Ces règles sont appliquées à l'installation des mises à jour sur les appareils clients. Si les règles ne sont pas définies, la tâche n'a rien à exécuter. Pour en savoir plus sur l'utilisation des règles, consultez le point Règles pour l'installation de la mise à jour.

- **Commencer l'installation au moment du &redémarrage ou de l'arrêt de l'appareil**

  Si cette option est activée, les mises à jour sont installées lors du redémarrage ou de l'arrêt de l'appareil. Dans le cas contraire, les mises à jour sont installées selon la programmation.

  Utilisez cette option si l'installation des mises à jour peut avoir un impact sur les performances de l'appareil.

  Cette option est Inactif par défaut.

- **Installer les modules système général requis**

  Si cette option est activée, l'application, avant d'installer une mise à jour, installe automatiquement tous les composants généraux système (prérequis) requis pour l'installation de la mise à jour. Par exemple, il peut s'agir des mises à jour du système d'exploitation.

  Si cette option est désactivée, vous devrez peut-être installer les prérequis manuellement.

  Cette option est Inactif par défaut.

- **Autoriser l'&installation de la nouvelle version de l'application lors de la mise à jour**

  Si cette option est activée, les mises à jour sont autorisées lorsqu'elles entraînent l'installation d'une nouvelle version d'un logiciel.

  Si cette option est désactivée, le logiciel n'est pas mis à jour. Vous pouvez alors installer les nouvelles versions du logiciel manuellement ou via un autre tâche. Par exemple, vous pouvez utiliser cette option si l'infrastructure de votre entreprise n'est pas prise en charge par une nouvelle version du logiciel ou si vous souhaitez vérifier une mise à jour dans une infrastructure d'essai.

  Cette option est activée par défaut.

  La mise à jour d'une application peut provoquer un dysfonctionnement des applications dépendantes installées sur les appareils clients.

- **Télécharger les mises à jour sur l'appareil sans les &installer**

  Quand cette option est activée, l'application télécharge les mises à jour sur l'appareil, mais ne les installe pas automatiquement. Vous pouvez installer les mises à jour manuellement par la suite.

  Les mises à jour Microsoft sont téléchargées dans le stockage Windows système. Les mises à jour des produits tiers (applications développées par des éditeurs d'application autres que Kaspersky et Microsoft) sont téléchargées dans le dossier indiqué dans le champ **Télécharger les mises à jour sur**.

  Si cette option est désactivée, les mises à jour sont installées automatiquement sur l'appareil.

  Cette option est Inactif par défaut.

  - **Télécharger les mises à jour sur**

    Ce dossier est utilisé dans le cadre du téléchargement des mises à jour de produits tiers (applications développées par des éditeurs de logiciels autres que Kaspersky et Microsoft).

- **Activer le diagnostic avancé**

  Quand cette fonction est activée, l'Agent d'administration enregistre des fichiers de trace même si l'écriture de fichiers de trace est désactivée pour l'Agent d'administration dans l'utilitaire de diagnostic à distance Kaspersky Security Center. Les traces sont enregistrées dans deux fichiers en alternance la taille de chacun de ces fichiers est déterminée par la valeur paramètre **Taille maximale (Mo) des fichiers de diagnostic avancé**. Quand les deux fichiers sont remplis, l'Agent d'administration écrit à nouveau dans ceux-ci. Les fichiers avec les traces sont stockés dans le dossier %WINDIR%\Temp. Ces fichiers sont accessibles dans l'utilitaire de diagnostic à distance, vous pouvez les télécharger ou les supprimer à cet endroit.

  Quand cette fonction est désactivée, l'Agent d'administration enregistre les traces conformément aux paramètres définis dans l'utilitaire de diagnostic à distance Kaspersky Security Center. Aucune trace complémentaire n'est écrite.

  Lors de la création d'une tâche, il n'est pas nécessaire d'activer le diagnostic avancé. Par contre, vous pouvez activer cette fonction plus tard si, par exemple, une tâche échoue sur certains appareils et que vous souhaitez obtenir des informations complémentaires lors d'une autre exécution de la tâche.

  Cette option est Inactif par défaut.

  - **Taille maximale (Mo) des fichiers de diagnostic avancé**

    La valeur par défaut est de 100 Mo, mais elle peut se situer entre 1 et 2 048 Mo. Il peut arriver qu'un expert du Support Technique de Kaspersky vous demande de modifier la valeur par défaut lorsque les informations reprises dans les fichiers de diagnostic avancés que vous avez envoyés ne suffisent pas pour résoudre le problème.

Paramètres définis après la création de la tâche

Vous pouvez spécifier les paramètres dans les sections répertoriées ci-dessous uniquement après la création d'une tâche. Pour obtenir une description complète des paramètres de la tâche, voir Paramètres généraux de la tâche.

- **Général**. Cette section contient des informations générales sur la tâche. Vous pouvez également indiquer à quels appareils la tâche *Installation des mises à jour requises et correction des vulnérabilités* doit s'appliquer :

  - **Distribuer aux sous-groupes**

    Cette option est disponible uniquement dans les paramètres des tâches de groupe.

    Lorsque cette option est activée, la zone d'action de la tâche inclut :

    - Le groupe d'administration que vous avez sélectionné lors de la création de la tâche.
    - Les groupes d'administration subordonnés au groupe d'administration sélectionné à n'importe quel niveau inférieur dans la hiérarchie des groupes.

    Lorsque cette option est désactivée, la zone d'action de la tâche inclut uniquement le groupe d'administration que vous avez sélectionné lors de la création de la tâche.

    Cette option est activée par défaut.

  - **&Envoyer aux Serveurs d'administration secondaire et virtuel**

    Lorsque cette option est activée, la tâche effective sur le Serveur d'administration principal est également appliquée sur les Serveurs d'administration secondaires (y compris virtuels). Si une tâche du même type existe déjà sur le Serveur d'administration secondaire, les deux tâches sont appliquées sur le Serveur d'administration secondaire, celui existant et celui hérité du Serveur d'administration principal.

    Cette option est disponible uniquement lorsque l'option **Distribuer aux sous-groupes** est activée.

    Cette option est Inactif par défaut.

- Mises à jour à installer

  La section **Mises à jour à installer** permet de consulter la liste des mises à jour que la tâche installe. Seules les mises à jour qui correspondent aux paramètres de la tâche appliqués sont affichées.

- Testez l'installation des mises à jour :

  - **Ne pas analyser**. Sélectionnez cette option si vous ne voulez pas exécuter l'installation de contrôle des mises à jour.
  - **Lancer l'analyse sur les &appareils indiqués**. Sélectionnez cette option si vous voulez vérifier l'installation des mises à jour sur certains appareils. Cliquez sur le bouton **Ajouter** et sélectionnez les appareils sur lesquels vous devez exécuter l'installation de contrôle des mises à jour.
  - **Lancer l'analyse sur les appareils dans le &groupe indiqué**. Sélectionnez cette option si vous voulez vérifier l'installation des mises à jour sur le groupe d'appareils. Dans le champ **Définissez le groupe test**, indiquez le groupe d'appareils sur lesquels exécuter l'installation de contrôle.
  - **Lancer l'analyse sur le &pourcentage indiqué des appareils**. Sélectionnez cette option si vous voulez lancer l'analyse des mises à jour sur une partie des appareils. Dans le champ **Le pourcentage des appareils de test du nombre total des appareils cibles**, indiquez le pourcentage des appareils qui requièrent l'exécution de l'installation de contrôle des mises à jour.

Liste globale des sous-réseaux

Cette section fournit des informations sur la liste globale des sous-réseaux que vous pouvez utiliser dans les règles.

Pour stocker les informations relatives aux sous-réseaux de votre réseau, vous pouvez dresser une liste globale des sous-réseaux pour chaque Serveur d'administration que vous utilisez. Cette liste vous aide à associer les paires {adresse IP, masque} et les unités physiques comme les succursales. Vous pouvez utiliser les sous-réseaux de cette liste dans les règles et les paramètres de mise en réseau.

Ajout de sous-réseaux à la liste globale des sous-réseaux

Vous pouvez ajouter des sous-réseaux avec leur description à la liste globale des sous-réseaux.

Pour ajouter un sous-réseau à la liste globale des sous-réseaux :

1. Dans l'arborescence de la console, sélectionnez l'entrée correspondant au Serveur d'administration de laquelle il faut se déconnecter.

2. Dans le menu contextuel Serveur d'administration, sélectionnez l'option **Propriétés**.

3. Dans la fenêtre **Propriétés** qui s'ouvre, dans le volet **Sections**, sélectionnez **Liste des sous-réseaux globaux**.

4. Cliquez sur le bouton **Ajouter**.

   La fenêtre **Nouveau sous-réseau** s'ouvre.

5. Remplissez les champs suivants :

   - **Paramètres généraux**

     L'adresse IP de sous-réseau pour le sous-réseau que vous ajoutez.

   - **Masque de sous-réseau**

     Le masque de sous-réseau pour le sous-réseau que vous ajoutez.

   - **Nom**

     Le nom de la clé. Il doit être unique au sein de la liste globale des sous-réseaux. Si vous saisissez un nom qui existe déjà dans la liste, un suffixe est ajouté, par exemple : ~~1, ~~2.

   - **Description**

     La description peut contenir des informations complémentaires sur la succursale où se trouve ce sous-réseau. Ce texte s'affiche dans toutes les listes où figure ce sous-réseau, par exemple dans la liste des règles de restriction du trafic.

     Ce champ est facultatif.

6. Cliquez sur le bouton **OK**.

Le sous-réseau apparaît dans la liste des sous-réseaux.

Consultation et modification des propriétés d'un sous-réseau dans la liste globale des sous-réseaux

Vous pouvez consulter et modifier les propriétés des sous-réseaux dans la liste globale des sous-réseaux.

Pour voir ou modifier les propriétés d'un sous-réseau dans la liste globale des sous-réseaux :

1. Dans l'arborescence de la console, sélectionnez l'entrée correspondant au Serveur d'administration de laquelle il faut se déconnecter.
2. Dans le menu contextuel Serveur d'administration, sélectionnez l'option **Propriétés**.
3. Dans la fenêtre **Propriétés** qui s'ouvre, dans le volet de gauche **Sections**, sélectionnez **Liste des sous-réseaux globaux**.
4. Dans la liste, sélectionnez le sous-réseau que vous souhaitez.
5. Cliquez sur le bouton **Propriétés**.

   La fenêtre **Nouveau sous-réseau** s'ouvre.
6. Le cas échéant, modifiez les paramètres du sous-réseau.
7. Cliquez sur le bouton **OK**.

Si vous introduisez des modifications, elles seront enregistrées.

Utilisation de l'Agent d'administration pour Windows, Linux et macOS : comparaison

Les fonctions de l'Agent d'administration varient en fonction du système d'exploitation de l'appareil. Les paramètres de la stratégie de l'Agent d'administration et du paquet d'installation varient également en fonction du système d'exploitation. Le tableau ci-dessous compare les fonctionnalités de l'Agent d'administration et les scénarios d'utilisation disponibles pour les systèmes d'exploitation Windows, macOS et Linux.

Comparaison entre fonctionnalités de l'Agent d'administration

Fonctionnalité de l'Agent d'administration	Windows	Linux	macOS
Installation			
Création automatique du paquet d'installation de l'Agent d'administration après l'installation de Kaspersky Security Center	✓	–	–
Mode d'installation forcée, à l'aide des options correspondantes dans la tâche d'installation à distance de Kaspersky Security Center	✓	✓	✓
Programme d'installation Via l'envoi aux utilisateurs des appareils de liens vers les paquets autonomes créés par Kaspersky Security Center	✓	✓	✓
Installation par clonage de l'image du disque dur de l'administrateur avec le système d'exploitation et l'Agent d'administration installé : à l'aide des ressources offertes par Kaspersky Security Center pour manipuler des images de disque	✓	–	–
Installation par clonage d'une image du disque dur de l'administrateur avec le système d'exploitation et l'Agent d'administration à l'aide d'outils tiers	✓	✓	✓
Programme d'installation à l'aide d'outils tiers d'installation à distance d'applications	✓	✓	✓
Programme d'installation Manuellement, en lançant les programmes d'installation sur les appareils	✓	✓	✓
Installation de l'Agent d'administration en mode silencieux	✓	✓	✓
Connexion manuelle de l'appareil client au Serveur d'administration, de l'utilitaire klmover	✓	✓	✓

Fonctionnalité de l'Agent d'administration	Windows	Linux	macOS
Installation automatique des mises à Programme d'installation jour et des correctifs pour les composants de Kaspersky Security Center	✓	✓	—
Diffusion automatique de la clé	✓	✓	✓
Synchronisation forcée	✓	✓	✓
Point de distribution			
Utilisation comme point de distribution	✓	✓	✓
Assignation automatique des points de distribution.	✓	✓ Sans utiliser la reconnaissance de l'emplacement réseau (NLA).	✓ Sans utiliser la reconnaissance de l'emplacement réseau (NLA).
Sondage réseau	✓ • Sondage du réseau Windows • Sondage des plages IP • Sondage du contrôleur de domaine (Microsoft Active Directory)	✓ • Sondage des plages IP • Sondage Zeroconf • Sondage du contrôleur de domaine (Microsoft Active Directory, Samba 4 Active Directory)	—
Activer le service KSN proxy côté point de distribution	✓	✓	—
Téléchargement des mises à jour via les serveurs de mise à jour de Kaspersky dans les stockages des points de distribution qui diffusent les mises à jour sur les appareils administrés	✓	✓	— (si un ou plusieurs appareils exécutant Linux ou macOS sont inclus dans la zone d'action de la tâche Télécharger les mises à jour sur les stockages des points de distribution, la tâche reçoit l'état Échec, même si elle s'est terminée avec succès sur tous les appareils Windows).
Installation push des applications	✓	Restreint : il n'est pas possible d'effectuer une installation push sur les appareils Windows à l'aide de points de distribution Linux.	Restreint : il n'est pas possible d'effectuer une installation push sur les appareils Windows à l'aide des points de distribution macOS.
Utilisation en tant que serveur push	✓	✓	—
Administration des applications tierces			
Installation à distance des applications sur les appareils	✓	—	✓ Consultez l'article suivant : Installation à distance d'applications sur les appareils macOS.
Mises à jour du logiciel	✓	—	—
Configuration des mises à jour du système d'exploitation dans une stratégie d'Agent d'administration	✓	—	—
Consultation des informations relatives aux vulnérabilités dans les applications	✓	—	—
Recherche de vulnérabilités dans les applications	✓	—	—
Inventaire du logiciel installé sur les appareils	✓	✓	—

Fonctionnalité de l'Agent d'administration	Windows	Linux	macOS
Machines virtuelles			
Installation de l'Agent d'administration sur une machine virtuelle	✓	✓	✓
Optimiser les paramètres pour Virtual Desktop Infrastructure (VDI)	✓	✓	✓
Prise en charge des machines virtuelles dynamiques	✓	✓	✓
Autres			
Audit des opérations sur un appareil client distant à l'aide du Partage du bureau Windows	✓	—	—
Surveillance de l'état de la protection antivirus	✓	✓	✓
Administration des redémarrages d'appareils	✓	—	—
Prise en charge de la remise à l'état antérieur du système de fichier	✓	✓	✓
Utilisation de l'agent d'administration comme passerelle de connexion	✓	✓	✓
Gestionnaire de connexion	✓	✓	✓
Agent d'administration passant d'un Serveur d'administration à un autre (automatiquement par emplacement réseau)	✓	—	✓
Vérification de la connexion de l'appareil client avec le Serveur d'administration. L'utilitaire klnagchk	✓	✓	✓
Connexion à distance au bureau de l'appareil client	✓	—	✓ En utilisant le système Virtual Network Computing (VNC).
Téléchargement d'un paquet d'installation autonome via l'Assistant de migration	✓	✓	✓
Sondage Zeroconf	—	✓	—
Affichage des informations sur le matériel des appareils clients	✓	✓ Les informations sur le matériel des appareils Linux envoyées au Serveur d'administration par l'Agent d'administration installé sur ces appareils se limitent aux informations spécifiées dans la description des paramètres des appareils administrés pour la Console d'administration et Kaspersky Security Center Web Console.	✓ Les informations sur le matériel des appareils macOS envoyées au Serveur d'administration par l'Agent d'administration installé sur ces appareils se limitent aux informations spécifiées dans la description des paramètres des appareils administrés pour la Console d'administration et Kaspersky Security Center Web Console.

Kaspersky Security Center Web Console

Kaspersky Security Center Web Console (ci-après Kaspersky Security Center Web Console) est une application Web conçue pour contrôler l'état du système de protection des réseaux d'entreprise se trouvant sous la protection des applications de Kaspersky.

A l'aide de l'application, vous pouvez exécuter les actions suivantes :

- Contrôler l'état du système de sécurité de votre entreprise.
- Installer les applications de Kaspersky sur les appareils de votre réseau et administrer les applications installées.
- Administrer les stratégies créées pour les appareils de votre réseau.
- Administrer les comptes utilisateur.
- Administrer les tâches pour les applications installées sur vos appareils réseau.
- Consulter les rapports sur l'état du système de sécurité.
- Gérer la diffusion des rapports aux personnes intéressées : administrateurs système et autres experts en informatique.

Pour en savoir plus sur la configuration matérielle et logicielle requise, consultez la section Configuration requise pour Web Console.

Kaspersky Security Center Web Console offre une interface Web qui assure votre rapport avec le Serveur d'administration avec l'utilisation du navigateur. Le Serveur d'administration est une application qui sert à administrer les applications de Kaspersky installées sur les appareils de votre réseau. Le Serveur d'administration contacte les appareils de votre réseau via les canaux sécurisés des liaisons (SSL). Quand vous vous connectez à Kaspersky Security Center Web Console à l'aide de votre navigateur, le navigateur établit une connexion avec le Serveur de Kaspersky Security Center 12 Web Console.

Kaspersky Security Center Web Console fonctionne d'une manière suivante :

1. Vous connectez au Kaspersky Security Center Web Console à l'aide du navigateur. Dans sa fenêtre, les pages du portail Web de l'application s'affichent.
2. A l'aide des éléments d'administration du portail Internet, vous sélectionnez la commande à exécuter. Kaspersky Security Center Web Console exécute les actions suivantes :
   - Si vous avez sélectionnez la commande couplée avec l'obtention des informations (par exemple, la consultation de la liste des appareils), Kaspersky Security Center Web Console forme une demande sur l'obtention des informations au Serveur d'administration, puis reçoit de sa part les données nécessaires et les transmet au navigateur pour afficher dans le mode favorable.
   - Si vous avez sélectionné la commande d'administration (par exemple, l'installation à distance de l'application), Kaspersky Security Center Web Console reçoit la commande de la part du navigateur et la transmet au Serveur d'administration. Ensuite, l'application reçoit le résultat d'exécution de la commande de la part du Serveur d'administration et transmet le résultat au navigateur pour afficher dans le mode favorable.

Kaspersky Security Center Web Console est une application multilingue. Vous pouvez modifier la langue de l'interface à tout moment, sans rouvrir l'application. Si vous installez Kaspersky Security Center Web Console avec Kaspersky Security Center, Kaspersky Security Center Web Console a la même langue d'interface que celle du fichier d'installation. Si vous n'installez que Kaspersky Security Center Web Console, l'application a la même langue d'interface que votre système d'exploitation. Si Kaspersky Security Center Web Console ne prend pas en charge la langue du fichier d'installation ou du système d'exploitation, la langue anglaise est définie par défaut.

L'administration des appareils mobiles n'est pas prise en charge dans Kaspersky Security Center Web Console. Toutefois, si vous avez ajouté des appareils mobiles à un groupe d'administration la console d'administration Microsoft, ils s'affichent aussi dans Kaspersky Security Center Web Console.

Diagramme de déploiement du Serveur d'administration de Kaspersky Security Center et de Kaspersky Security Center Web Console

La figure ci-dessous illustre le diagramme de déploiement du Serveur d'administration de Kaspersky Security Center et de Kaspersky Security Center Web Console

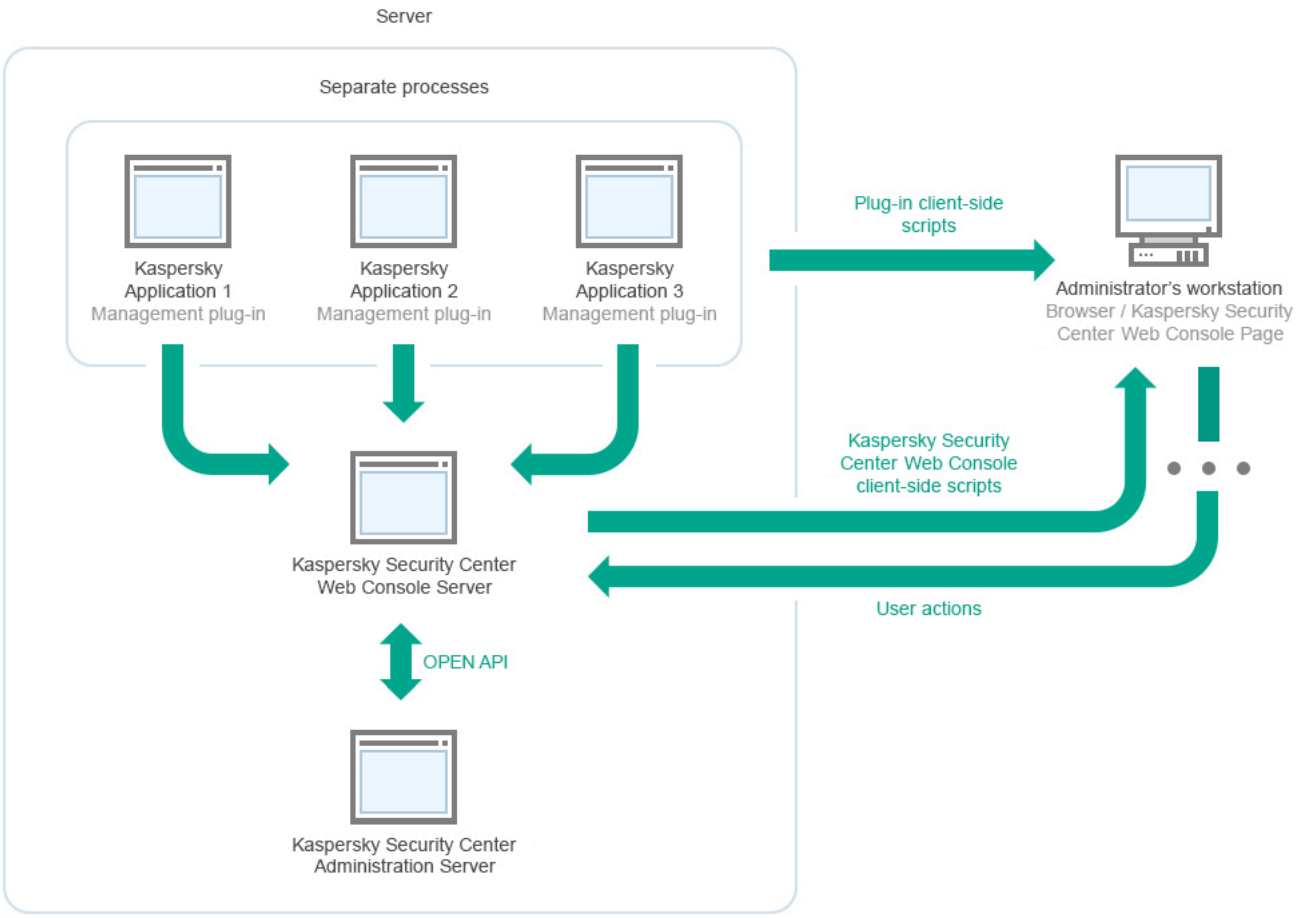


Diagramme de déploiement du Serveur d'administration de Kaspersky Security Center et de Kaspersky Security Center Web Console

Les plug-ins d'administration pour les applications de Kaspersky installées sur les appareils protégés (un plug-in pour chaque application) sont déployés en même temps que le serveur Kaspersky Security Center Web Console.

En tant qu'administrateur, vous accédez à Kaspersky Security Center Web Console via un navigateur Internet sur votre poste de travail.

Quand vous réalisez des opérations spéciales dans Kaspersky Security Center Web Console, le serveur Kaspersky Security Center Web Console communique avec le Serveur d'administration de Kaspersky Security Center via OpenAPI. Le serveur Kaspersky Security Center Web Console sollicite les informations requises au Serveur d'administration de Kaspersky Security Center et affiche les résultats de vos opérations dans Kaspersky Security Center Web Console.

Ports utilisés par Kaspersky Security Center Web Console

Le tableau ci-dessous énumère les ports qui doivent être ouverts sur l'appareil sur lequel Kaspersky Security Center Web Console Server (également appelé Kaspersky Security Center Web Console) est installé.

Ports utilisés par Kaspersky Security Center Web Console

Numéro de port	Nom de service	Protocole	Destination du port	Zone de fonctionnement
2001	Serveur des plug-ins des produits de Kaspersky Security Center	HTTPS	Port de l'API utilisé par les processus du plug-in d'administration pour recevoir les requêtes du « Service d'administration de Kaspersky Security Center Web Console »	Exécution des processus node.exe des plug-ins d'administration
1329, 2003	Service d'administration de Kaspersky Security Center Web Console	HTTPS	Ports de l'API utilisés pour recevoir les requêtes du " Service d'administration de Kaspersky Security Center Web Console " s'exécutant sur le même appareil	Mise à jour des composants de Kaspersky Security Center Web Console
2005	Kaspersky Security Center Web Console	HTTPS	Port de l'API utilisé pour recevoir les requêtes du « Service d'administration de Kaspersky Security Center Web Console » s'exécutant sur le même appareil	Exécution des processus node.exe de Kaspersky Security Center Web Console
3333	Kaspersky OSMP KAS Service	HTTPS	Port de point de terminal d'autorisation OAuth2.0	Gestionnaire des identités et des accès
4004	Kaspersky OSMP Facade Service	HTTPS	Port du fournisseur d'identité OAuth2.0	Gestionnaire des identités et des accès
4444	Kaspersky OSMP KAS Service	HTTPS	Port de terminal d'introspection de jeton OAuth2.0	Gestionnaire des identités et des accès
8200	—	HTTP	Port API utilisé pour générer des certificats au moyen de HashiCorp Vault (pour en savoir plus, consultez le site Internet de HashiCorp Vault)	Installation de Kaspersky Security Center Web Console et mise à jour des composants de Kaspersky Security Center Web Console
4150, 4151, 4152	File d'attente des messages de Kaspersky Security Center Web Console.	HTTPS	Ports API du courtier de messages utilisés pour la communication entre les processus de Kaspersky Security Center Web Console et des plug-ins d'administration	Interaction entre Kaspersky Security Center Web Console et les plug-ins d'administration

Le tableau ci-dessous indique les ports qui ne doivent pas être ouverts sur l'appareil sur lequel Kaspersky Security Center Web Console Server est installé. Cependant, Kaspersky Security Center Web Console utilise ces ports pour le Gestionnaire des identités et des accès.

Ports utilisés par Kaspersky Security Center Web Console pour le Gestionnaire des identités et des accès

Numéro de port	Nom de service	Protocole	Destination du port	Zone de fonctionnement
4445	Kaspersky OSMP KAS Service	HTTPS	Port principal du Gestionnaire des identités et des accès qui reçoit la configuration de Kaspersky Security Center Web Console pour le port du terminal d'autorisation OAuth2.0 (pour plus d'informations sur OAuth 2.0, consultez le site Internet d'OAuth)	Gestionnaire des identités et des accès
2444	Kaspersky OSMP Facade Service	HTTPS	Port pour la configuration du Gestionnaire des identités et des accès	Gestionnaire des identités et des accès
2445	Kaspersky OSMP Facade Service	HTTPS	Port pour la connexion de « Kaspersky OSMP KAS Service à Kaspersky OSMP Facade Service »	Gestionnaire des identités et des accès

Interface de Kaspersky Security Center Web Console

L'administration de Kaspersky Security Center s'opère via l'interface de Kaspersky Security Center Web Console.

La fenêtre de Kaspersky Security Center Web Console contient les éléments suivants :

- Menu principal dans la partie gauche de la fenêtre
- Zone de travail dans la partie droite de la fenêtre

Menu principal

Le menu principal contient les sections suivantes :

- **Serveur d'administration**. Affiche le nom du Serveur d'administration auquel vous êtes actuellement connecté. Cliquez sur l'icône des paramètres ( ) pour ouvrir les propriétés du Serveur d'administration.
- **Surveillance et rapports**. Fournit une vue d'ensemble de votre infrastructure, des états de la protection et des statistiques.
- **Ressources (appareils)**. Contient les outils pour les ressources, ainsi que les tâches et les stratégies d'application de Kaspersky.
- **Utilisateurs et rôles**. Permet d'administrer les utilisateurs et les rôles, de configurer les privilèges des utilisateurs en attribuant des rôles aux utilisateurs et d'associer des profils de stratégie à des rôles.
- **Opérations**. Contient diverses opérations, y compris les licences des applications, l'affichage et la gestion des disques chiffrés et des événements de chiffrement, ainsi que l'administration des applications tierces. Cela vous permet également d'accéder aux stockages d'applications.
- **Découverte et déploiement**. Permet de sonder le réseau à la recherche d'appareils clients et de distribuer les appareils aux groupes d'administration manuellement ou automatiquement. Cette section contient également l'assistant de démarrage rapide de l'application et l'assistant de déploiement de la protection.
- **Place de marché**. Contient des informations sur l'ensemble des solutions d'entreprise de Kaspersky et vous permet de sélectionner celles dont vous avez besoin, puis de procéder à l'achat de ces solutions sur le site de Kaspersky.

- **Paramètres**. Permet de sauvegarder l'état actuel d'un plug-in Web pour pouvoir restaurer l'état enregistré ultérieurement. Contient vos paramètres personnels liés à l'apparence de l'interface, tels que la langue de l'interface ou le thème.

- **Menu de votre compte**. Contient un lien vers l'aide de Kaspersky Security Center. Permet également de vous déconnecter de Kaspersky Security Center, de consulter la version de Kaspersky Security Center Web Console et la liste des plug-ins Internet d'administration installés.

Zone de travail

La zone de travail affiche les informations que vous choisissez d'afficher dans les sections de la fenêtre de l'interface de Kaspersky Security Center Web Console. Il contient également des éléments de contrôle qui permettent de configurer l'affichage des informations.

Épinglage et désépinglage de sections du menu principal

À partir de la section **Épinglé** dans le menu principal, vous pouvez épingler des sections de Kaspersky Security Center Web Console pour les ajouter à vos favoris et y accéder rapidement.

> Si aucun élément n'est épinglé, la section **Épinglé** ne s'affiche pas dans le menu principal.

Vous pouvez épingler des sections qui présentent uniquement des pages. Par exemple, si vous accédez à **Ressources (Appareils)** → **Appareils administrés**, une page avec le tableau des appareils s'ouvre. Vous pouvez donc épingler la section **Appareils administrés**. Si une fenêtre ou aucun élément ne s'affiche après que vous avez sélectionné la section dans le menu principal, vous ne pouvez pas épingler une telle section.

Pour épingler une section, procédez comme suit :

1. Dans le menu principal, placez le curseur de la souris sur la section que vous souhaitez épingler.

   L'icône en forme d'épingle (📌) s'affiche.

2. Cliquez sur l'icône en forme d'épingle (📌).

   La section est épinglée et s'affiche dans la section **Épinglé**.

Vous pouvez également retirer des éléments des favoris en les désépinglant.

Pour désépingler une section, procédez comme suit :

1. Dans le menu principal, accédez à la section **Épinglé**.

2. Passez le curseur de la souris sur la section que vous souhaitez désépingler, puis cliquez sur l'icône de désépinglage (📌).

   La section est retirée des favoris.

Scénario d'installation et de configuration initiale de Kaspersky Security Center Web Console

Ce scénario décrit l'installation du Serveur d'administration de Kaspersky Security Center et de Kaspersky Security Center Web Console. Il explique comment réaliser la configuration initiale du Serveur d'administration via l'Assistant de configuration initiale de l'application et comment installer les applications de Kaspersky sur les appareils administrés à l'aide de l'Assistant de déploiement de la protection.

L'installation et la configuration initiale de Kaspersky Security Center Web Console procède par étapes :

1. **Installation d'un système de gestion de base de données (SGDB)**

   Installez le SGBD que Kaspersky Security Center va utiliser ou utiliser le SGBD existant.

   Pour en savoir plus sur l'installation du SGBD sélectionné, consultez sa documentation.

2. **Installation du Serveur d'administration, de la Console d'administration, de l'Agent d'administration**

   La Console d'administration et la version serveur de l'Agent d'administration sont également installées avec le Serveur d'administration.

   Lors de l'installation du Serveur d'administration de Kaspersky Security Center, indiquez si vous souhaitez installer Kaspersky Security Center Web Console sur le même appareil. Si vous choisissez d'installer les deux composants sur le même appareil, vous ne devez pas installer Kaspersky Security Center Web Console séparément, car celle-ci est automatiquement installée. Si vous souhaitez installer Kaspersky Security Center Web Console sur un autre appareil, installez d'abord le Serveur d'administration de Kaspersky Security Center, puis installez Kaspersky Security Center Web Console.

3. **Installation de Kaspersky Security Center Web Console**

   Si vous choisissez d'installer Kaspersky Security Center Web Console avec le Serveur d'administration de Kaspersky Security Center à l'étape précédente, installez Kaspersky Security Center Web Console séparément. Vous pouvez installer Kaspersky Security Center Web Console sur un autre appareil ou sur le même appareil où le Serveur d'administration est installé.

4. **Configuration initiale**

   Après l'achèvement de l'installation du Serveur d'administration lors de la première connexion au Serveur d'administration, l'Assistant de configuration initiale de l'application est automatiquement lancé. Exécutez la configuration initiale du Serveur d'administration conformément à vos exigences. Lors de la configuration initiale, l'Assistant crée les stratégies indispensables au déploiement de la protection et les tâches selon les paramètres par défaut. Il se peut que ces paramètres ne soient pas parfaits pour les besoins de votre entreprise. Le cas échéant, vous pouvez modifier les paramètres des stratégies et des tâches.

5. **License de Kaspersky Security Center (facultatif)**

   Kaspersky Security Center avec le support des fonctionnalités de base de la Console d'administration ne nécessite pas de licence. Vous avez besoin d'une licence commerciale si vous souhaitez utiliser une ou plusieurs fonctionnalités supplémentaires, dont la gestion des vulnérabilités et des correctifs, l'administration des appareils mobiles et l'intégration aux systèmes SIEM. Vous pouvez ajouter un fichier clé ou un code d'activation pour ces fonctions à l'étape correspondante de l'Assistant de configuration initiale de l'application ou manuellement.

6. **Recherche d'appareils sur le réseau**

Cette étape est gérée par l'Assistant de configuration initiale de l'application. Vous pouvez aussi rechercher les appareils manuellement. Suite à cela, Kaspersky Security Center obtient les adresses et les noms de tous les appareils détectés sur le réseau. Ensuite, vous pouvez installer à l'aide de Kaspersky Security Center des applications de Kaspersky et d'autres éditeurs sur les appareils détectées. Kaspersky Security Center lance la recherche d'appareils régulièrement. Par conséquent, si de nouveaux appareils apparaissent sur le réseau, ils seront détectés automatiquement.

7. **Organisation des appareils dans les groupes d'administration**

   Cette étape est gérée par l'Assistant de configuration initiale de l'application, mais vous pouvez aussi déplacer manuellement les appareils trouvés dans les groupes.

8. **Installation de l'Agent d'administration et des applications de sécurité sur les appareils du réseau**

   Le déploiement de la protection sur le réseau de l'entreprise suppose l'installation de l'Agent d'administration et des applications de sécurité (par exemple, Kaspersky Endpoint Security for Windows) sur les appareils qui ont été détectés par le Serveur d'administration pendant la recherche d'appareils.

   Pour installer les applications à distance, exécutez l'Assistant de déploiement de la protection.

   Les applications de sécurité protègent les appareils contre les virus et d'autres applications qui présentent une menace. L'Agent d'administration assure le lien entre l'appareil et le Serveur d'administration. Les paramètres de l'Agent d'administration sont automatiquement configurés par défaut.

   Avant d'installer l'Agent d'administration et les applications de sécurité sur les appareils du réseau, confirmez la disponibilité de ces appareils (ils sont activés).

9. **Diffusion des clés de licence sur les appareils clients**

   Diffusez les clés de licence sur les appareils client pour activer les applications de sécurité administrées sur ces appareils.

10. **Installation de Kaspersky Security for Mobile (facultatif)**

    Si vous prévoyez d'administrer des appareils mobiles d'entreprise, suivez les instructions fournies dans l'aide de Kaspersky Security for Mobile pour obtenir plus d'informations sur le déploiement de Kaspersky Endpoint Security for Android.

11. **Configuration des stratégies des applications de Kaspersky**

    Pour appliquer différents paramètres d'application à différents appareils, vous pouvez opter pour une administration de la sécurité centrée sur l'appareil et/ou une administration de la sécurité centrée sur l'utilisateur. L'administration de la sécurité centrée sur l'appareil peut être mise en œuvre à l'aide de stratégies et de tâches. Vous pouvez appliquer les tâches uniquement aux appareils qui remplissent certaines conditions. Pour définir les conditions de filtrage des appareils, utilisez des sélections d'appareils et des tags.

12. **Surveillance de l'état de la protection du réseau**

    Vous pouvez surveiller votre réseau à l'aide de widget sur le tableau de bord, créer des rapports depuis les applications de Kaspersky, configurer et afficher des sélections d'événements reçus des applications sur les appareils administrés et consulter les listes de notification.

Installation

Cette section décrit l'installation de Kaspersky Security Center et de Kaspersky Security Center Web Console.

Installation de Kaspersky Security Center (installation standard)

Cette procédure décrit l'installation de Kaspersky Security Center. Avant l'installation, vous devez installer le système de gestion de base de données.

A l'aide de Kaspersky Security Center :

1. Sous un compte disposant de privilèges d'administration, exécutez le fichier exécutable ksc_<numéro de version>_full_<langue de la localisation>.exe.
2. Dans la fenêtre de sélection des applications qui s'ouvre, cliquez sur **Installer Kaspersky Security Center**.

   L'Assistant d'installation du Serveur d'administration de Kaspersky Security Center démarre.
3. À partir de la page d'accueil, poursuivez les étapes de l'Assistant à l'aide du bouton **Suivant**.
4. Si Microsoft .NET Framework n'est pas installé, installez-le.
5. J'accepte les conditions du Contrat de licence et de la Politique de confidentialité.
6. Sélectionnez le type d'installation. À des fins d'évaluation, nous vous recommandons de conserver la valeur **Standard** par défaut.
7. Si vous souhaitez installer Kaspersky Security Center Web Console sur le même appareil, cochez la case **Installer Kaspersky Security Center Web Console**.

   Si vous décochez la case, vous pourrez installer ultérieurement Kaspersky Security Center Web Console séparément sur le même appareil ou sur un autre.
8. Sélectionnez la taille de votre réseau. À des fins d'évaluation, nous vous recommandons de conserver la valeur par défaut **Moins de 100 appareils en réseau**.
9. Sélectionnez le type de serveur de base de données que vous avez installé antérieurement.
10. Définissez les paramètres de connexion pour le serveur de base de données que vous avez installé antérieurement.
11. Définissez les paramètres d'authentification pour le serveur de base de données que vous avez installé antérieurement.
12. Cliquez sur le bouton **Installer** pour lancer l'installation.
13. Une fois l'installation terminée, choisissez si vous voulez lancer la Console d'administration juste après la fermeture de l'assistant.

    Si vous décidez d'ouvrir Kaspersky Security Center Web Console, l'écran de connexion s'ouvre. Vous pourrez alors réaliser la configuration initiale du Serveur d'administration grâce à l'Assistant de configuration initiale de l'application.

    Vous pouvez ouvrir Kaspersky Security Center Web Console uniquement si la solution est déjà installée. Vous ne pouvez pas ouvrir Kaspersky Security Center Web Console si vous n'avez pas installé la solution lors de l'installation de Kaspersky Security Center ou séparément.
14. Dans la fenêtre de la Console d'administration qui s'ouvre, cliquez sur le Serveur d'administration installé.
15. Dans la fenêtre du certificat du Serveur d'administration, cliquez sur le bouton **Oui** pour continuer.

L'Assistant de configuration initiale du Serveur d'administration démarre si vous ne l'aviez pas exécuté dans la Console d'administration basée sur la console de gestion Microsoft.

Dépannage

Si la fenêtre du certificat du Serveur d'administration ne s'ouvre pas et si des erreurs de connexion s'affichent, essayez une des solutions suivantes :

1. Sous Windows, ouvrez **Services** (**Panneau de configuration** → **Outils d'administration** → **Services**). Vérifiez que les services de l'Agent d'administration de Kaspersky Security Center et du Serveur d'administration de Kaspersky Security Center fonctionnent.

2. Dans Windows, ouvrez l'**Observateur d'événements** (**Panneau de configuration** → **Outils d'administration** → **Observateur d'événements**), puis sélectionnez **Journaux des applications et des services** → **Journaux des événements Kaspersky**. Assurez-vous que le journal ne contient pas d'erreurs et qu'il contient des événements comme **Le Serveur d'administration <numéro de version> est en marche**.

Installation de Kaspersky Security Center Web Console

Cette section décrit comment installer le serveur de Kaspersky Security Center Web Console (appelé également Kaspersky Security Center Web Console) séparément. Avant de lancer l'installation, vous devez installer un SGBD et le Serveur d'administration de Kaspersky Security Center. Vous pouvez installer la Kaspersky Security Center Web Console sur le même appareil sur lequel Kaspersky Security Center est installé, ou sur un autre.

Installation de Kaspersky Security Center Web Console :

1. Sous un compte doté de privilèges d'administrateur, lancez le fichier d'installation ksc-web-console-<version number>.<build number>.exe.

   Cette opération démarre l'Assistant de configuration.

2. Choisissez une langue pour l'Assistant de configuration.

3. Dans la fenêtre d'accueil, cliquez sur **Suivant**.

4. Dans la fenêtre **Contrat de licence**, lisez et acceptez les conditions du Contrat de licence utilisateur final. L'installation se poursuit après que vous avez accepté le CLUF. Dans le cas contraire, le bouton **Suivant** n'est pas disponible.

5. Dans la fenêtre **Dossier de destination**, choisissez un dossier où Kaspersky Security Center Web Console sera installé (par défaut, %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center Web Console). Si ce dossier n'existe pas, alors il sera créé automatiquement pendant l'installation.

   Vous pouvez modifier le dossier de destination à l'aide du bouton **Parcourir**.

6. Dans la fenêtre **Paramètres de connexion de Kaspersky Security Center Web Console**, précisez les informations suivantes :

   - L'adresse de Kaspersky Security Center Web Console (par défaut, 127.0.0.1).
   - Le port que Kaspersky Security Center Web Console utilisera pour les connexions entrantes, c'est-à-dire le port qui donne accès à Kaspersky Security Center Web Console à partir d'un navigateur (par défaut, 8080).

   Nous vous recommandons de ne pas modifier l'adresse et le numéro de port.

   Si vous le souhaitez, vous pouvez cliquer sur **Vérifier** pour vous assurer que le port sélectionné est disponible.

   Si vous souhaitez activer l'enregistrement des événements dans le journal concernant les activités de Kaspersky Security Center Web Console, sélectionnez l'option appropriée. Si vous ne sélectionnez pas cette option, les fichiers journaux de Kaspersky Security Center Web Console ne sont pas créés.

7. Dans la fenêtre **Paramètres du compte**, précisez les noms et mot de passe des comptes utilisateur.

   Nous vous recommandons d'utiliser des comptes par défaut.

8. Dans la fenêtre **Certificat client**, sélectionnez l'une des options suivantes :

   - **Créer un certificat**. Cette option est recommandée si vous n'avez pas de certificat de navigateur.
   - **Sélectionner un certificat existant**. Vous pouvez choisir cette option si vous avez déjà un certificat de navigateur. Dans ce cas, indiquez son chemin d'accès.
   - Si vous décidez de générer un nouveau certificat, lorsque vous ouvrez Kaspersky Security Center Web Console, le navigateur peut vous informer que la connexion à Kaspersky Security Center Web Console n'est pas privée et que le certificat de Kaspersky Security Center Web Console n'est pas valide. Cet avertissement apparaît, car le certificat de Kaspersky Security Center Web Console est auto-signé et généré automatiquement par Kaspersky Security Center. Pour supprimer cet avertissement, créez un certificat de confiance dans votre infrastructure et qui répond aux exigences des certificats personnalisés. Ensuite, sélectionnez l'option **Sélectionner un certificat existant** dans la fenêtre **Certificat client**, puis indiquez le chemin d'accès à votre certificat personnalisé.

   Les certificats au format PFX ne sont pas pris en charge par Kaspersky Security Center Web Console. Pour utiliser un tel certificat, vous devez d'abord le convertir au format PEM pris en charge à l'aide d'un utilitaire multiplateforme reposant sur OpenSSL, comme OpenSSL pour Windows.

9. Dans la fenêtre **Serveurs d'administration de confiance**, assurez-vous que votre Serveurs d'administration se trouve sur la liste, et cliquez sur **Suivant** pour accéder à la dernière fenêtre de l'installateur.

   Si vous devez ajouter un nouveau Serveur d'administration à la liste, cliquez sur le bouton **Ajouter**. Dans la fenêtre qui s'ouvre, indiquez les propriétés du nouveau Serveur d'administration de confiance :

   - **Nom du Serveur d'administration**

     Nom du Serveur d'administration qui s'affichera dans la fenêtre de connexion de Kaspersky Security Center Web Console.

   - **Adresse du Serveur d'administration**

     Adresse IP de l'appareil sur lequel vous installez le Serveur d'administration.

   - **Port du Serveur d'administration**

     Le port OpenAPI utilisé par Kaspersky Security Center Web Console pour se connecter au Serveur d'administration (la valeur par défaut est 13299).

   - **Certificat du Serveur d'administration**

     Le fichier du certificat est stocké sur l'appareil sur lequel le Serveur d'administration est installé. Chemin d'accès par défaut au certificat du Serveur d'administration :

     - Pour Windows—%ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert
     - Pour Linux—/var/opt/kaspersky/klnagent_srv/1093/cert/

     Si vous installez Kaspersky Security Center Web Console sur le même appareil où le Serveur d'administration est installé, utilisez l'un des chemins indiqués ci-dessus. Sinon, copiez le fichier de certificat de l'appareil sur lequel le Serveur d'administration est installé sur l'appareil sur lequel vous installez Kaspersky Security Center Web Console, puis indiquez le chemin d'accès local au certificat.

10. Dans la fenêtre **Gestionnaire des identités et des accès (IAM)**, indiquez si vous souhaitez installer le Gestionnaire des identités et des accès (également appelé IAM). Si vous choisissez d'installer le Gestionnaire des identités et des accès, indiquez les numéros de port suivants :

    - **Port administrateur KAS**. Par défaut, le port 4445 est utilisé pour recevoir la configuration de Kaspersky Security Center Web Console pour le port du terminal d'autorisation OAuth2.0.
    - **Port administrateur de façade**. Par défaut, le port 2444 est utilisé dans le cadre de la configuration du Gestionnaire des identités et des accès.
    - **Port d'interaction de façade**. Par défaut, le port 2445 est utilisé dans le cadre de la connexion de Kaspersky OSMP KAS Service à Kaspersky OSMP Facade Service.

    Si vous le souhaitez, vous pouvez modifier les numéros de port par défaut. Vous ne pourrez plus les modifier à l'avenir via Kaspersky Security Center Web Console.

11. Dans la dernière fenêtre de l'installateur, cliquez sur **Installer** pour lancer l'installation.

Une fois l'installation réussite, un raccourci apparaît sur votre bureau, et vous pouvez vous connecter à Kaspersky Security Center Web Console.

L'assistant de configuration initiale du Serveur d'administration démarre si vous ne l'aviez pas exécuté dans la Console d'administration basée sur la console de gestion Microsoft.

Elimination des défaillances

Si Kaspersky Security Center Web Console ne s'affiche pas dans votre navigateur après avoir saisi l'URL, essayez ce qui suit :

1. Confirmez que vous avez indiqué le nom d'hôte ou l'adresse IP corrects de l'appareil sur lequel Kaspersky Security Center Web Console est installé.
2. Confirmez que l'appareil que vous souhaitez utiliser a accès à l'appareil sur lequel Kaspersky Security Center Web Console est installé.
3. Confirmez que les paramètres du pare-feu de l'appareil sur lequel Kaspersky Security Center Web Console est installé acceptent les connexions entrantes via le port 8080 et pour l'application node.exe.
4. Dans Windows, ouvrez **Services**. Confirmez que le service Kaspersky Security Center Web Console est en cours d'exécution.
5. Confirmez que vous pouvez accéder à Kaspersky Security Center via la Console d'administration.
6. Dans Windows, ouvrez l'**Observateur d'événements**, puis sélectionnez **Journaux des applications et des services** → **Journaux des événements Kaspersky**. Confirmez que le journal ne contient aucune erreur.

Installation de Kaspersky Security Center Web Console connecté au Serveur d'administration installé sur les nœuds du cluster de basculement

Cette section décrit comment installer le serveur Kaspersky Security Center Web Console (ci-après Kaspersky Security Center Web Console), qui se connecte au Serveur d'administration installé sur les nœuds du cluster de basculement Kaspersky Security Center ou sur les nœuds du cluster de basculement Windows Server. Avant d'installer Kaspersky Security Center Web Console, installez un SGBD et le Serveur d'administration de Kaspersky Security Center sur les nœuds du cluster de basculement Kaspersky Security Center ou sur les nœuds du cluster de basculement Windows Server.

Si vous utilisez un cluster de basculement Windows Server, il est déconseillé d'installer Kaspersky Security Center Web Console sur un nœud du cluster de basculement. En cas de défaillance du nœud, vous perdrez l'accès au Serveur d'administration.

Pour installer Kaspersky Security Center Web Console qui se connecte au Serveur d'administration installé sur les nœuds du cluster de basculement :

1. Suivez les étapes de l'installation de Kaspersky Security Center Web Console, en commençant par l'étape 1 à l'étape 8.

2. À l'étape 9, dans la fenêtre **Serveurs d'administration de confiance**, cliquez sur le bouton **Ajouter** pour ajouter un cluster de basculement en tant que Serveur d'administration de confiance.

   Dans la fenêtre qui s'ouvre, indiquez les propriétés suivantes :

   - **Nom du Serveur d'administration**

     Nom du cluster qui s'affichera dans la fenêtre de connexion de Kaspersky Security Center Web Console.

   - **Adresse du Serveur d'administration**

     Selon le type de cluster de basculement, indiquez l'adresse du cluster :

     - **Cluster de basculement Kaspersky Security Center**. Indiquez l'adresse IP de la carte réseau secondaire comme adresse du cluster si vous avez créé la carte lors de la préparation des nœuds du cluster. Dans le cas contraire, indiquez l'adresse IP du répartiteur de charge tiers que vous utilisez.

     - **Cluster de basculement Windows Server**. Spécifiez l'adresse de cluster que vous avez obtenue lors de la création du cluster de basculement Windows Server.

   - **Port du Serveur d'administration**

     Le port OpenAPI utilisé par Kaspersky Security Center Web Console pour se connecter au Serveur d'administration (la valeur par défaut est 13299).

   - **Certificat du Serveur d'administration**

     Le certificat du Serveur d'administration se trouve dans le stockage de données partagé du cluster de basculement Kaspersky Security Center ou du cluster de basculement Windows Server. Chemin d'accès par défaut au fichier du certificat : <dossier de données partagé>\1093\cert\klserver.cer. Copiez le fichier de certificat du stockage de données partagé sur l'appareil sur lequel vous installez Kaspersky Security Center Web Console. Indiquez le chemin d'accès local au certificat du Serveur d'administration.

3. Continuez avec l'installation standard de Kaspersky Security Center Web Console.

Une fois l'installation terminée, un raccourci apparaît sur votre bureau et vous pouvez vous connecter à Kaspersky Security Center Web Console.

Mise à niveau de Kaspersky Security Center Web Console

Si vous souhaitez utiliser une version plus récente de Kaspersky Security Center Web Console sans supprimer votre instance actuellement installée, vous pouvez utiliser la procédure de mise à niveau standard fournie dans le programme d'installation de Kaspersky Security Center Web Console.

Pour mettre à jour Kaspersky Security Center Web Console, procédez comme suit :

1. Sous un compte doté de droits d'administrateur, lancez le fichier d'installation ksc-web-console-<version number>.<build number>.exe, où <build number> représente une version de Kaspersky Security Center Web Console dont le numéro est supérieur à celui de votre instance actuellement installée.

2. Dans la fenêtre de l'Assistant d'installation qui s'ouvre, sélectionnez une langue, puis cliquez sur **OK**.

3. Dans la fenêtre de bienvenue, sélectionnez l'option **Mettre à jour**, puis cliquez sur **Suivant**.

4. Dans la fenêtre **Contrat de licence**, lisez et acceptez les conditions du Contrat de licence utilisateur final. L'installation se poursuit après que vous avez accepté le CLUF. Dans le cas contraire, le bouton **Suivant** n'est pas disponible.

5. Parcourez les étapes de l'Assistant d'installation jusqu'à ce que vous ayez terminé l'installation. Lors de la progression, vous pouvez également modifier les paramètres de Kaspersky Security Center Web Console que vous avez définis lors de l'installation précédente. Lorsque vous arrivez à l'étape **Tout est prêt pour modifier Kaspersky Security Center Web Console**, cliquez sur le bouton **Mettre à jour**. Attendez que les nouveaux paramètres soient appliqués et, à l'étape suivante de l'Assistant d'installation, cliquez sur **Terminer**. Vous pouvez également cliquer sur le lien **Lancer Kaspersky Security Center Web Console dans le navigateur** pour démarrer immédiatement l'instance mise à niveau de Kaspersky Security Center Web Console.

   La modification des paramètres de Kaspersky Security Center Web Console pendant la mise à jour n'est disponible que dans la version 12.2 de Kaspersky Security Center Web Console ou dans une version ultérieure.

   Votre instance de Kaspersky Security Center Web Console est mise à niveau.

Certificats pour travailler avec Kaspersky Security Center Web Console

Cette section décrit comment émettre et remplacer les certificats de Kaspersky Security Center Web Console et comment renouveler un certificat pour le Serveur d'administration si le Serveur interagit avec Kaspersky Security Center Web Console.

Réémission du certificat pour Kaspersky Security Center Web Console

La plupart des navigateurs imposent une limite à la durée de validité d'un certificat. Pour respecter cette limite, la durée de validité du certificat de Kaspersky Security Center Web Console est limitée à 397 jours. Vous pouvez remplacer un certificat existant reçu d'un centre de certification (CA) en émettant manuellement un nouveau certificat auto-signé. Vous pouvez également réémettre votre certificat expiré de Kaspersky Security Center Web Console.

La réémission automatique du certificat pour Kaspersky Security Center Web Console n'est pas prise en charge. Vous devez manuellement réémettre le certificat expiré.

Si vous utilisez déjà un certificat auto-signé, vous pouvez également le réémettre en mettant à niveau Kaspersky Security Center Web Console via la procédure standard du programme d'installation (option **Mettre à jour**).

Lorsque vous ouvrez Web Console, le navigateur peut vous informer que la connexion à Web Console n'est pas privée et que le certificat de Web Console n'est pas valide. Cet avertissement apparaît car le certificat de la Console Web est auto-signé et généré automatiquement par Kaspersky Security Center. Pour supprimer ou empêcher cet avertissement, vous pouvez effectuer une des actions suivantes :

- Spécifiez un certificat personnalisé lorsque vous le réémettez (option recommandée). Créez un certificat de confiance dans votre infrastructure et qui répond aux exigences des certificats personnalisés.
- Ajoutez le certificat de Web Console à la liste des certificats de navigateur de confiance après avoir réémis le certificat. Nous vous recommandons d'utiliser cette option uniquement si vous ne pouvez pas créer de certificat personnalisé.

Pour émettre un nouveau certificat lors de la première installation de Kaspersky Security Center Web Console, procédez comme suit :

1. Exécutez l'installation de routine de Kaspersky Security Center Web Console.
2. Lorsque vous arrivez à l'étape **Certificat client** de l'Assistant d'installation, sélectionnez l'option **Créer un certificat**, puis cliquez sur le bouton **Suivant**.
3. Parcourez les étapes restantes de l'Assistant d'installation jusqu'à ce que vous ayez terminé l'installation.

   Un nouveau certificat pour Kaspersky Security Center Web Console est émis avec une durée de validité de 397 jours.

Pour réémettre le certificat expiré de Kaspersky Security Center Web Console, procédez comme suit :

1. Sous un compte doté de droits d'administrateur, exécutez le fichier d'installation ksc-web-console-<version number>.<build number>.exe.
2. Dans la fenêtre de l'Assistant d'installation qui s'ouvre, sélectionnez une langue, puis cliquez sur **OK**.
3. Dans la fenêtre de bienvenue, sélectionnez l'option **Réémettre le certificat**, puis cliquez sur **Suivant**.
4. À l'étape suivante, attendez que la reconfiguration de Kaspersky Security Center Web Console soit terminée, puis cliquez sur **Terminer**.

   Le certificat de Kaspersky Security Center Web Console est réémis pour une autre durée de validité de 397 jours.

Si vous utilisez le Gestionnaire des identités et des accès, vous devez également réémettre tous les certificats TLS pour les ports que le Gestionnaire des identités et des accès utilise. Kaspersky Security Center Web Console affiche une notification lorsqu'un certificat expire. Vous devez suivre les instructions de notification.

Remplacement de certificat pour Kaspersky Security Center Web Console

Par défaut, lors de l'installation de Kaspersky Security Center Web Console Server, un certificat de navigateur pour l'application est généré automatiquement. Vous pouvez remplacer le certificat généré automatiquement par un certificat personnalisé.

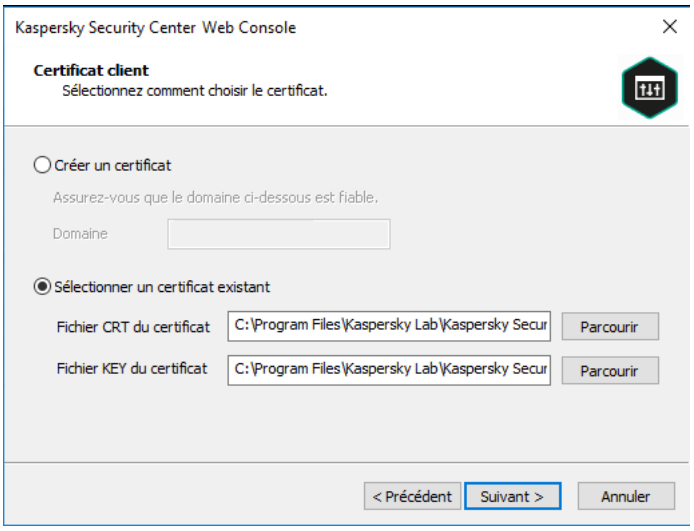
Pour remplacer le certificat de Kaspersky Security Center Web Console Server par un certificat personnalisé :

1. Sur l'appareil où Kaspersky Security Center Web Console Server est installé, exécutez le fichier d'installation ksc-web-console-<version number>.<build number>.exe depuis un compte doté de privilèges d'administrateur.

   Cette opération démarre l'Assistant de configuration.

2. À la première page de l'Assistant, sélectionnez l'option **Mettre à jour**.

3. Sur la page **Certificat client**, sélectionnez l'option **Choisir certificat existant** et spécifiez le chemin d'accès au certificat personnalisé.



Définition du certificat client

4. Sur la dernière page de l'Assistant, cliquez sur **Modifier** pour appliquer les nouveaux paramètres.

5. Une fois la reconfiguration de l'application terminée, cliquez sur le bouton **Terminer**.

Kaspersky Security Center Web Console fonctionne avec le certificat spécifié.

Définition des certificats pour les Serveurs d'administration de confiance dans Kaspersky Security Center Web Console

Le certificat du Serveur d'administration existant est automatiquement remplacé par un nouveau avant sa date d'expiration. Vous pouvez aussi remplacer le certificat du Serveur d'administration existant par un certificat personnalisé. Chaque fois que le certificat est modifié, le nouveau certificat doit être spécifié dans les paramètres de Kaspersky Security Center Web Console. Sinon, Kaspersky Security Center Web Console ne pourra pas se connecter au serveur d'administration.

Pour spécifier un nouveau certificat pour le Serveur d'administration :

1. Sur l'appareil où le Serveur d'administration est installé, copiez le fichier de certificat, par exemple, sur un appareil de stockage de masse.

   Par défaut, le fichier de certificat est stocké dans le dossier suivant :

   - Pour Windows—%ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert
   - Pour Linux—/var/opt/kaspersky/klnagent_srv/1093/cert/

2. Sur le périphérique où Kaspersky Security Center Web Console est installé, placez le fichier de certificat dans un dossier local.

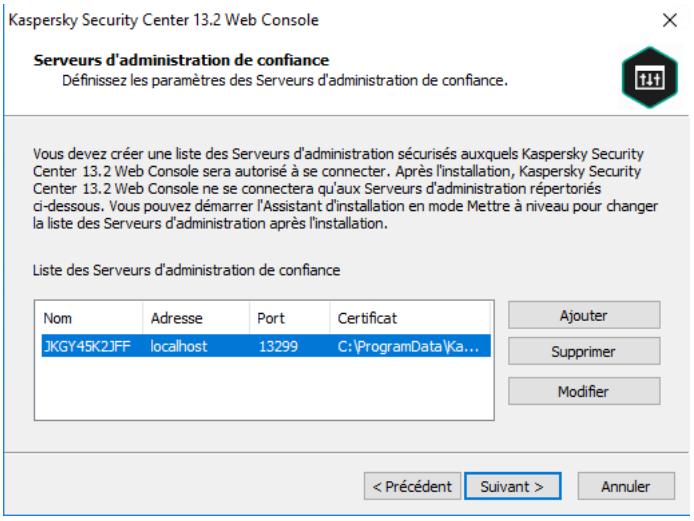
3. Exécutez le fichier d'installation ksc-web-console-<version number>.<build number>.exe sous un compte doté de privilèges d'administrateur.

   Cette opération démarre l'Assistant de configuration.

4. À la première page de l'Assistant, sélectionnez l'option **Mettre à jour**.

   Suivez les instructions de l'assistant.

5. Sur la page **Serveurs d'administration de confiance** de l'assistant, sélectionnez le Serveur d'administration requis et cliquez sur le bouton **Modifier**.



Définition des Serveurs d'administration de confiance

6. Dans la fenêtre **Modifier le Serveur d'administration** qui s'ouvre, cliquez sur le bouton **Parcourir**, indiquez le chemin d'accès au nouveau fichier de certificat, puis cliquez sur le bouton **Mise à jour** pour appliquer les modifications.

7. Sur la page de **Tout est prêt pour modifier Kaspersky Security Center Web Console** de l'assistant, cliquez sur le bouton **Mettre à jour** pour lancer la mise à niveau.

8. Une fois la reconfiguration de l'application terminée, cliquez sur le bouton **Terminer**.

9. Connectez-vous à Kaspersky Security Center Web Console.

Kaspersky Security Center Web Console fonctionne avec le certificat spécifié.

Conversion d'un certificat PFX au format PEM

Pour utiliser un certificat PFX dans Kaspersky Security Center Web Console, vous devez d'abord le convertir au format PEM en utilisant un utilitaire multi-plateforme basé sur OpenSSL.

Pour convertir un certificat PFX au format PEM dans le système d'exploitation Windows :

1. Dans un utilitaire multiplateforme basé sur OpenSSL, exécutez les commandes suivantes :

   ```
   openssl pkcs12 -in <nom du fichier.pfx> -clcerts -nokeys -out server.crt
   ```

   ```
   openssl pkcs12 -in <nom du fichier.pfx> -nocerts -nodes -out key.pem
   ```

   Par conséquent, vous obtenez une clé publique sous forme de fichier .crt et une clé privée sous forme de fichier .pem protégé par une phrase secrète.

2. Assurez-vous que les fichiers .crt et .pem sont générés dans le même dossier où le fichier .pfx est stocké.

3. Si le fichier .crt ou .pem contient les "Bag Attributes", supprimez ces attributs à l'aide d'un éditeur de texte pratique, puis enregistrez le fichier.

4. Redémarrez le service Windows.

5. Kaspersky Security Center Web Console ne prend pas en charge les certificats protégés par une phrase secrète. Par conséquent, exécutez la commande suivante dans un utilitaire multiplateforme basé sur OpenSSL pour supprimer une phrase secrète du fichier .pem :

   ```
   openssl rsa -in key.pem -out key-without-passphrase.pem
   ```

   > N'utilisez pas le même nom pour les fichiers .pem d'entrée et de sortie.

   Par conséquent, le nouveau fichier .pem n'est pas chiffré. Vous n'avez pas besoin d'entrer une phrase secrète pour l'utiliser.

Les fichiers .crt et .pem sont prêts à l'emploi, vous pouvez donc les spécifier dans le programme d'installation de Kaspersky Security Center Web Console.

Pour convertir un certificat PFX au format PEM dans le système d'exploitation Linux :

1. Dans un utilitaire multiplateforme basé sur OpenSSL, exécutez les commandes suivantes :

   ```
   openssl pkcs12 -in <nom du fichier.pfx> -clcerts -nokeys | sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > server.crt
   ```

   ```
   openssl pkcs12 -in <nom du fichier.pfx> -nocerts -nodes | sed -ne '/-BEGIN PRIVATE KEY-/,/-END PRIVATE KEY-/p' > key.pem
   ```

2. Assurez-vous que le fichier de certificat et la clé privée sont générés dans le même répertoire où le fichier .pfx est stocké.

3. Kaspersky Security Center Web Console ne prend pas en charge les certificats protégés par une phrase secrète. Par conséquent, exécutez la commande suivante dans un utilitaire multiplateforme basé sur OpenSSL pour supprimer une phrase secrète du fichier .pem :

   ```
   openssl rsa -in key.pem -out key-without-passphrase.pem
   ```

   > N'utilisez pas le même nom pour les fichiers .pem d'entrée et de sortie.

   Par conséquent, le nouveau fichier .pem n'est pas chiffré. Vous n'avez pas besoin d'entrer une phrase secrète pour l'utiliser.

Les fichiers .crt et .pem sont prêts à l'emploi, vous pouvez donc les spécifier dans le programme d'installation de Kaspersky Security Center Web Console.

Migration depuis Kaspersky Security Center Windows

Cette section décrit la migration des appareils administrés et des objets associés (stratégies, tâches, groupes, tags et autres objets) de Kaspersky Security Center Windows vers :

- Kaspersky Security Center Cloud Console
- Kaspersky Security Center Linux

Migration vers Kaspersky Security Center Cloud Console

Vous pouvez effectuer la migration de Kaspersky Security Center Web Console vers Kaspersky Security Center Cloud Console. Après cela, vous avez accès au Serveur d'administration et au système d'administration de base de données (SGBD), qui sont hébergés dans l'infrastructure de Kaspersky. Vous n'avez pas besoin d'un serveur physique ou d'un SGBD : les deux sont administrés pour vous par les experts de Kaspersky.

Vous pouvez migrer vos appareils administrés exécutant un système d'exploitation Windows, Linux ou macOS sous le contrôle de Kaspersky Security Center Cloud Console. Si votre réseau comprend une hiérarchie de Serveurs d'administration, vous pouvez l'enregistrer dans Kaspersky Security Center Cloud Console. De plus, vous pouvez transférer :

- Tâches et stratégies des applications administrées
- Tâches globales

- Sélections d'appareils personnalisés
- Structure du groupe d'administration et appareils inclus
- Tags attribués aux appareils en migration

Une fois la migration terminée, vous pouvez administrer les appareils à l'aide de Kaspersky Security Center Cloud Console. En même temps, les objets transférés sont conservés et l'Agent d'administration est réinstallé sur tous les appareils administrés.

Pour plus d'informations sur la façon d'effectuer la migration et une liste des prérequis, consultez l'*Aide de Kaspersky Security Center Cloud Console*.

Migration vers Kaspersky Next XDR Expert

Suite à ce scénario, vous pouvez transférer la structure du groupe d'administration, les appareils administrés inclus et les autres objets du groupe (stratégies, tâches, tâches globales, tags et sélections d'appareils) depuis Kaspersky Security Center Windows sous l'administration de Kaspersky Next XDR Expert.

Restrictions :

- La migration est possible uniquement de Kaspersky Security Center 14.2 Windows vers Kaspersky Next XDR Expert à partir de la version 1.0.
- Vous pouvez uniquement exécuter ce scénario à l'aide de Kaspersky Security Center Web Console.

Étapes

La migration se déroule par étapes :

1. **Choisissez une méthode de migration**

   Vous migrez vers Kaspersky Next XDR Expert via l'Assistant de migration. Les étapes de l'Assistant de migration dépendent de la hiérarchie ou non des Serveurs d'administration de Kaspersky Security Center Windows et de Kaspersky Next XDR Expert :

   - Migration à l'aide de la hiérarchie des Serveurs d'administration

     Choisissez cette option si le Serveur d'administration de Kaspersky Security Center Windows est le Serveur d'administration secondaire de Kaspersky Next XDR Expert. Vous gérez le processus de migration et de basculement entre les Serveurs au sein de la console OSMP. Si vous préférez cette option, vous pouvez organiser les Serveurs d'administration dans une hiérarchie pour simplifier la procédure de migration. Pour ce faire, créez la hiérarchie avant de lancer la migration.

   - Migration à l'aide d'un fichier export (archive ZIP)

     Choisissez cette option si les Serveurs d'administration de Kaspersky Security Center Windows et de Kaspersky Next XDR Expert ne sont pas hiérarchisés. Vous gérez la migration à l'aide de deux consoles : une instance pour Kaspersky Security Center Windows et une autre pour la console OSMP. Dans ce cas, vous allez utiliser le fichier d'exportation que vous avez créé et téléchargé lors de l'exportation depuis Kaspersky Security Center Windows et vous allez importer ce fichier dans Kaspersky Next XDR Expert.

2. **Exporter des données depuis Kaspersky Security Center Windows**

   Ouvrez Kaspersky Security Center Windows, puis lancez l'Assistant de migration.

3. **Importer des données dans Kaspersky Next XDR Expert**

   Poursuivez l'Assistant de migration pour importer les données exportées dans Kaspersky Next XDR Expert.

   Si les Serveurs sont hiérarchiques, l'importation démarre automatiquement après un export réussi dans le même Assistant. Si les Serveurs ne sont pas hiérarchiques, vous continuerez l'Assistant de migration après le passage à Kaspersky Next XDR Expert.

4. **Exécuter les actions complémentaires pour transférer manuellement les objets et les paramètres de Kaspersky Security Center Windows vers Kaspersky Next XDR Expert (étape facultative)**

   Vous souhaiterez peut-être également transférer les objets et les paramètres qui ne peuvent pas être transférés via l'Assistant de migration. Par exemple, vous pouvez également effectuer les opérations suivantes :

   - Configurer les tâches globales du Serveur d'administration
   - Configurer les paramètres de la stratégie de l'Agent d'administration
   - Créez des paquets d'installation des applications
   - Créez des Serveurs virtuels
   - Désigner et configurer les points de distribution
   - Configurer les règles de déplacement des appareils
   - Configurer les règles d'exécution pour l'attribution automatique de tags aux appareils
   - Créer les catégories des applications

5. **Déplacez les appareils administrés importés sous la gestion de Kaspersky Next XDR Expert**

   Pour terminer la migration, déplacez les appareils administrés importés sous l'administration de Kaspersky Next XDR Expert. Vous pouvez le faire de l'une des manières suivantes :

   - Par la tâche de groupe de Kaspersky Security Center

     La tâche Modification du Serveur d'administration permet de modifier le Serveur d'administration en fonction des appareils clients.

   - Via l'utilitaire klmover

     Utilisez l'utilitaire klmover et définissez les paramètres de connexion pour le nouveau Serveur d'administration.

   - Par l'installation ou la réinstallation de l'Agent d'administration sur les appareils administrés

     Créez un nouveau paquet d'installation de l'Agent d'administration et définissez les paramètres de connexion pour le nouveau Serveur d'administration dans les propriétés du paquet d'installation. Utilisez le paquet d'installation pour installer l'Agent d'administration sur les appareils administrés importés via la tâche d'installation à distance.

     Vous pouvez également créer et utiliser un paquet d'installation autonome pour installer l'Agent d'administration localement.

6. **Mettre à jour l'Agent d'administration vers la dernière version**

   Nous vous recommandons de mettre à jour l'Agent d'administration vers la même version que la console OSMP.

7. **Assurez-vous que les appareils administrés sont visibles sur le nouveau Serveur d'administration**

   Sur le Serveur d'administration de Kaspersky Next XDR Expert, ouvrez la liste des appareils administrés (**Ressources (Appareils)** → **Appareils administrés**) et vérifiez les valeurs dans les colonnes **Visible**, **L'Agent d'administration est installé** et **Dernière connexion au Serveur d'administration**.

Autres méthodes de migration des données

Outre l'Assistant de migration, vous pouvez également transférer des tâches et des stratégies spécifiques :

- Exportez des tâches depuis Kaspersky Security Center Windows, puis importez les tâches dans Kaspersky Next XDR Expert.
- Exportez les stratégies depuis Kaspersky Security Center Windows, puis importez les stratégies dans Kaspersky Next XDR Expert. Les profils de stratégie associés sont exportés et importés avec les stratégies sélectionnées.

Migration vers Kaspersky Security Center Linux

La migration de Kaspersky Security Center Windows vers Kaspersky Security Center Linux est possible à l'aide de la copie de sauvegarde des données du Serveur d'administration (avec l'utilitaire klbackup) et de l'Assistant de migration.

Le tableau ci-dessous permet de comparer les principales caractéristiques et limites de la migration à l'aide de la copie de sauvegarde des données du Serveur d'administration et de l'Assistant de migration, afin de déterminer l'approche la plus adaptée à votre organisation.

Comparaison des méthodes de migration

Paramètres	Sauvegarde des données du Serveur d'administration	Assistant de migration
Processus de migration	Création d'une sauvegarde complète des données du Serveur d'administration Windows de Kaspersky Security Center et restauration sur un Serveur d'administration de Kaspersky Security Center Linux	Sélection et exportation des données du Serveur d'administration pour la migration, importation de ces données vers le Serveur d'administration de Kaspersky Security Center Linux, et migration des appareils administrés sous la gestion de Kaspersky Security Center
Caractéristiques de la méthode de migration	• Migration de toutes les données du Serveur d'administration • Migration d'un nombre quelconque d'appareils administrés • Permet d'obtenir une copie complète des données du Serveur d'administration de Kaspersky Security Center Windows et de les transférer vers le Serveur d'administration de Kaspersky Security Center Linux	• Migration partielle des données du Serveur d'administration • La sélection des objets à migrer est disponible • Le groupe d'administration ou le sous-groupe à migrer ne peut pas contenir plus de 10 000 appareils • Utilisé pour transférer partiellement les données du Serveur d'administration, y compris uniquement les objets de groupe situés dans le périmètre de migration. Les objets de groupe situés en dehors du périmètre de migration doivent être restaurés manuellement
Zone de migration	Transfert complet des données du Serveur d'administration avec un nombre illimité d'appareils administrés	• Structure des groupes d'administration • Appareils administrés inclus dans les groupes d'administration (**10 000 appareils maximum**) • Tags attribués aux appareils migrés • Tâches globales de l'Agent d'administration et des applications gérées (pas pour le Serveur d'administration) • Tâches de groupe de l'Agent d'administration et des applications administrées • Stratégies des applications administrées • Modèles de rapports • Rôles des utilisateurs • Utilisateurs et groupes de sécurité internes • Catégories d'applications personnalisées avec contenu ajouté manuellement • Sélections d'appareils personnalisés

Zone non migrée	—	• Tâches globales du Serveur d'administration • Événements enregistrés sur le Serveur d'administration • Le stockage des distributifs des applications pour l'installation à distance • Certificat du Serveur d'administration • Clés de licence utilisées par le Serveur d'administration et les applications administrées • Serveurs d'administration virtuels • Paramètres de la stratégie de l'Agent d'administration • Règles de déplacement des appareils • Règles d'exécution pour l'attribution automatique de tags aux appareils • Points de distribution • Paramètres de l'application Kaspersky enregistrés sur le Serveur d'administration
Versions de Kaspersky Security Center prenant en charge les migrations	• Toute version prise en charge de Kaspersky Security Center Windows • Kaspersky Security Center Linux version 15.2 ou ultérieure	• Kaspersky Security Center Windows version 14.2 ou ultérieure • Kaspersky Security Center Linux version 15 ou ultérieure
SGBD entre lesquels la migration est possible	• Microsoft SQL Server → MySQL, MariaDB • Microsoft SQL Server → PostgreSQL, Postgres Pro (uniquement pour la migration de Kaspersky Security Center Windows version 14.2 ou version ultérieure avec le correctif installé vers Kaspersky Security Center Linux version 15.3 ou une version ultérieure) • MySQL → MySQL, MariaDB • MariaDB → MySQL, MariaDB	Migration entre les SGBD pris en charge sans limitations

Migration vers Kaspersky Security Center Linux à l'aide de la sauvegarde des données du Serveur d'administration

Vous pouvez utiliser une sauvegarde des données pour migrer les données du Serveur d'administration de Kaspersky Security Center Windows vers Kaspersky Security Center Linux. Avant la migration, assurez-vous que les fonctionnalités nécessaires de Kaspersky Security Center Windows sont prises en charge dans Kaspersky Security Center Linux.

Restrictions :

- La migration peut être effectuée entre les SGBD suivants :
  - Microsoft SQL Server → MySQL, MariaDB
  - Microsoft SQL Server → PostgreSQL, Postgres Pro
  - MySQL → MySQL, MariaDB
  - MariaDB → MySQL, MariaDB
- La migration des données du Serveur d'administration stockées dans la base de données de Microsoft SQL Server, MySQL ou MariaDB vers MySQL ou MariaDB est prise en charge pour la migration à partir de toute version prise en charge de Kaspersky Security Center Windows vers Kaspersky Security Center Linux 15.2 ou une version ultérieure.

- La migration des données du Serveur d'administration stockés dans la base de données de Microsoft SQL Server vers PostgreSQL ou Postgres Pro est prise en charge pour la migration de Kaspersky Security Center Windows version 14.2 ou une version ultérieure vers Kaspersky Security Center Linux version 15.3 ou une version ultérieure.

  Pour prendre en charge la migration vers PostgreSQL ou Postgres Pro, vous pouvez effectuer une des opérations suivantes :

  - Installez le correctif 15.1.0.20748-pf2 pour le Serveur d'administration de Kaspersky Security Center Windows. Contactez le support technique de Kaspersky pour obtenir ce correctif.
  - Mise à jour de Kaspersky Security Center Windows vers la version 15.1.0.22239.

- Si vous utilisez MySQL ou MariaDB comme SGBD pour Kaspersky Security Center Windows et pour Kaspersky Security Center Linux, le paramètre `lower_case_table_names` doit correspondre pour le SGBD actuel et le nouveau.

  Avant de créer une sauvegarde des données, vérifiez le paramètre `lower_case_table_names`. Ainsi, lors de l'installation de MySQL ou MariaDB pour Kaspersky Security Center Linux, vous devez définir ce paramètre sur la même valeur que celle de ce paramètre pour Windows.

Étapes

La migration à l'aide de la sauvegarde des données du Serveur d'administration se déroule par étapes :

1. **En vérifiant que vous disposez du compte utilisateur interne administrateur à partir duquel vous pouvez vous connecter au Serveur d'administration**

   Le compte de l'administrateur sera utilisé pour se connecter au Serveur d'administration de Kaspersky Security Center Linux. Si vous ne disposez pas de ce compte et que vous êtes connecté uniquement sous un compte Windows local ou sous un compte de domaine, vous ne pourrez pas vous connecter au Serveur d'administration de Kaspersky Security Center Linux après la restauration de la sauvegarde. Le Serveur d'administration de Kaspersky Security Center Linux ne prend pas en charge la connexion à l'aide du compte Windows local. Il est possible de se connecter sous le compte de domaine, mais cela peut nécessiter une configuration supplémentaire du Serveur d'administration.

   Si vous ne disposez pas du compte d'administrateur, vous devrez créer ce compte après avoir restauré la copie de sauvegarde à l'aide de l'utilitaire kladduser.

2. **Création d'une copie de sauvegarde à jour des données du Serveur d'administration de Kaspersky Security Center Windows**

   En fonction du type de SGBD utilisé pour Kaspersky Security Center Windows et Kaspersky Security Center Linux, exécutez une des actions suivantes :

   - Pour la migration de MySQL ou MariaDB vers MySQL ou MariaDB : créez une copie de sauvegarde à l'aide de l'utilitaire klbackup ou une tâche de sauvegarde des données sur l'appareil sur lequel le Serveur d'administration est installé.
   - Pour la migration de Microsoft SQL Server vers MySQL ou MariaDB : créez une copie de sauvegarde à l'aide de l'utilitaire klbackup en activant l'option **Migrer au format MySQL/MariaDB**.
   - Pour la migration de Microsoft SQL Server vers PostgreSQL ou Postgres Pro :

     1. Faites une demande auprès du Support technique de Kaspersky et installez le correctif 15.1.0.20748-pf2 pour le Serveur d'administration afin de prendre en charge la migration vers PostgreSQL et Postgres Pro.

        Vous pouvez également mettre à jour Kaspersky Security Center Windows vers la version 15.1.0.22239.

     2. Créez une copie de sauvegarde à l'aide de l'utilitaire klbackup.

Si vous exécutez l'utilitaire klbackup via la ligne de commande, utilisez l'indicateur `-migrate postgres`.

Si vous utilisez l'interface klbackup, activez l'option **Migrer vers le format Postgres**.

Après avoir créé une copie de sauvegarde, déconnectez du réseau le Serveur d'administration de Kaspersky Security Center Windows.

3 Préparation d'un nouvel appareil en vue de l'installation de Kaspersky Security Center Linux

À cette étape du scénario, procédez comme suit :

1. Sélectionnez un nouvel appareil sur lequel installer le Serveur d'administration. Cet appareil doit répondre à la configuration matérielle et logicielle requise. Vérifiez également que les ports utilisés sur le Serveur d'administration sont disponibles.

2. Attribuez la même adresse au nouvel appareil.

   Le nouveau Serveur d'administration peut recevoir le nom NetBIOS, le FQDN et l'adresse IP statique. Cela dépend de l'adresse du Serveur d'administration qui a été définie dans le paquet d'installation de l'Agent d'administration lors du déploiement des Agents d'administration. Vous pouvez également utiliser l'adresse de connexion qui détermine le Serveur d'administration auquel l'Agent d'administration se connecte (vous pouvez obtenir cette adresse sur les appareils administrés à l'aide de l'utilitaire klnagchk).

4 Installation et configuration du SGBD

À cette étape du scénario, procédez comme suit :

1. Sélectionnez le type de SGBD qui offre des performances optimales. Tenez compte du nombre d'appareils en réseau, de la topologie du réseau et de la charge de travail sur le réseau. Vous pouvez choisir parmi l'un des SGBDs pris en charge.

2. Installez le SGBD selon le type de SGBD sélectionné lors de la création de la sauvegarde. Pour en savoir plus sur l'installation du SGBD sélectionné, consultez sa documentation.

   La nouvelle version de la base de données ne doit pas être antérieure à la version actuelle.

3. Configurez le SGBD pour qu'il fonctionne avec Kaspersky Security Center Linux.

5 Installation de Kaspersky Security Center Linux

Installez Kaspersky Security Center Linux sur le nouvel appareil.

Le compte utilisateur interne de l'administrateur créé lors de l'installation, ainsi que les autres objets (groupes, stratégies, tâches, utilisateurs) créés avant que vous ne restauriez les données du Serveur d'administration à partir de la sauvegarde, seront perdus après la restauration. Ces objets seront remplacés par des objets contenus dans la sauvegarde.

6 Restauration des données du Serveur d'administration à partir de la copie de sauvegarde

À cette étape du scénario, procédez comme suit :

1. Restaurez les données du Serveur d'administration sur le nouvel appareil à l'aide de l'utilitaire klbackup.

2. Si vous ne disposiez pas du compte utilisateur interne de l'administrateur sous lequel vous étiez connecté au Serveur d'administration de Kaspersky Security Center Windows et que vous utilisiez un compte Windows local ou un compte de domaine, créez un compte d'administrateur en utilisant l'utilitaire kladduser comme suit :

   ```
   /opt/kaspersky/ksc64/sbin/kladduser -n ksc -p <password>
   ```

   où le paramètre `<password>` remplit les conditions suivantes :

- Le mot de passe utilisateur ne doit pas comporter moins de 8 ni plus de 256 caractères.
- Le mot de passe doit compter des caractères d'au moins trois des groupes ci-dessous :
  - Lettres majuscules (A-Z)
  - Lettre minuscules (a-z)
  - Chiffres (0-9)
  - Caractères spéciaux (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)

7. **Installation de Kaspersky Security Center Web Console et configuration du Serveur d'administration**

   À cette étape du scénario, procédez comme suit :

   1. Installez Kaspersky Security Center Web Console.

      Si Kaspersky Security Center Web Console a été installé précédemment. Réinstallez-le avec le même fichier de réponses.

      Connectez-vous à Kaspersky Security Center Web Console sous le compte utilisateur interne de l'administrateur.

      Le processus d'initialisation des données dure généralement jusqu'à 15 minutes après la restauration des données du Serveur d'administration. Toutefois, cette durée dépend de la performance du matériel et de la taille des données du Serveur d'administration. Pendant ce temps, Kaspersky Security Center Web Console peut ne pas réussir à se connecter et afficher alors les erreurs.

   2. Vérifiez le fonctionnement des principales fonctions du Serveur d'administration lorsque l'initialisation des données dans la base de données est terminée. Vérifiez que le Serveur d'administration se synchronise avec les appareils gérés et que les données du Serveur d'administration sont récupérées.

   3. Interrogez les contrôleurs de domaine pour récupérer les informations sur la structure du domaine, les comptes utilisateurs, les groupes de sécurité et les noms DNS des appareils inclus dans les domaines.

   4. Si nécessaire, désinstallez le Serveur d'administration et le serveur de base de données de l'appareil précédent.

      Il ne doit pas y avoir plusieurs Serveurs d'administration sur le même réseau avec la même adresse de connexion et le même certificat de Serveur d'administration.

L'administrateur a accès aux données du Serveur d'administration et aux appareils administrés qui se trouvaient dans Kaspersky Security Center Windows, en tenant compte des fonctionnalités prises en charge dans Kaspersky Security Center Linux.

Migration vers Kaspersky Security Center Linux à l'aide de l'Assistant de migration

Suite à ce scénario, vous pouvez transférer la structure du groupe d'administration, les appareils administrés inclus et les autres objets du groupe (stratégies, tâches, tâches globales, tags et sélections d'appareils) depuis Kaspersky Security Center Windows sous l'administration de Kaspersky Security Center Linux. Avant la migration, assurez-vous que les fonctionnalités nécessaires de Kaspersky Security Center Windows sont prises en charge dans Kaspersky Security Center Linux.

Restrictions :

- La migration est possible uniquement à partir de Kaspersky Security Center Windows version 14.2 ou version ultérieure vers Kaspersky Security Center Linux version 15 ou version ultérieure.
- Vous pouvez uniquement exécuter ce scénario à l'aide de Kaspersky Security Center Web Console.

Étapes

La migration se déroule par étapes :

1. **Choisissez une méthode de migration**

   Vous migrez vers Kaspersky Security Center Linux via l'Assistant de migration. Les étapes de l'Assistant de migration dépendent de la hiérarchie ou non des Serveurs d'administration de Kaspersky Security Center Windows et de Kaspersky Security Center Linux :

   - Migration à l'aide de la hiérarchie des Serveurs d'administration

     Choisissez cette option si le Serveur d'administration de Kaspersky Security Center Windows est le Serveur d'administration secondaire de Kaspersky Security Center Linux. Vous administrez le processus de migration et basculez entre les serveurs au sein d'une seule instance de Kaspersky Security Center Web Console. Si vous préférez cette option, vous pouvez organiser les Serveurs d'administration dans une hiérarchie pour simplifier la procédure de migration. Pour ce faire, créez la hiérarchie avant de lancer la migration.

   - Migration à l'aide d'un fichier export (archive ZIP)

     Choisissez cette option si les Serveurs d'administration de Kaspersky Security Center Windows et de Kaspersky Security Center Linux ne sont pas hiérarchisés. Vous gérez le processus de migration avec deux instances de Kaspersky Security Center Web Console : une instance pour Kaspersky Security Center Windows et une autre pour Kaspersky Security Center Linux. Dans ce cas, vous allez utiliser le fichier d'exportation que vous avez créé et téléchargé lors de l'exportation depuis Kaspersky Security Center Windows et vous allez importer ce fichier dans Kaspersky Security Center Linux.

2. **Sauvegarder le certificat et la clé privée du Serveur d'administration de Kaspersky Security Center Windows (étape facultative)**

   Vous pouvez placer les appareils administrés sous la gestion du Serveur d'administration de Kaspersky Security Center Linux en restaurant le certificat et la clé privée du Serveur d'administration à partir d'une copie de sauvegarde. Dans ce cas, sauvegardez le certificat et la clé privée du Serveur d'administration de Kaspersky Security Center Windows. Ensuite, à l'étape 6, restaurez le certificat et la clé privée.

3. **Exporter des données depuis Kaspersky Security Center Windows**

   Ouvrez Kaspersky Security Center Windows, puis lancez l'Assistant de migration.

4. **Importer des données dans Kaspersky Security Center Linux**

   Poursuivez l'Assistant de migration pour importer les données exportées dans Kaspersky Security Center Linux. Si les Serveurs sont hiérarchiques, l'importation démarre automatiquement après un export réussi dans le même Assistant. Si les Serveurs ne sont pas hiérarchiques, vous continuerez l'Assistant de migration après le passage à Kaspersky Security Center Linux.

5. **Exécuter les actions complémentaires pour transférer manuellement les objets et les paramètres de Kaspersky Security Center Windows vers Kaspersky Security Center Linux (étape facultative)**

   Vous souhaiterez peut-être également transférer les objets et les paramètres qui ne peuvent pas être transférés via l'Assistant de migration. Par exemple, vous pouvez également effectuer les opérations suivantes :

   - Transférer les clés de licence utilisées par le Serveur d'administration et les applications administrées

- Configurer les tâches globales du Serveur d'administration
- Configurer les paramètres de la stratégie de l'Agent d'administration
- Créez des paquets d'installation des applications
- Créez des Serveurs virtuels
- Désigner et configurer les points de distribution
- Configurer les règles de déplacement des appareils
- Configurer les règles d'exécution pour l'attribution automatique de tags aux appareils
- Créer les catégories des applications

6. **Déplacez les appareils administrés par Kaspersky Security Center Linux administré**

   Pour terminer la migration, déplacez les appareils administrés importés sous l'administration de Kaspersky Security Center Linux. Vous pouvez le faire de l'une des manières suivantes :

   - Via l'utilitaire klmover

     Utilisez l'utilitaire klmover et définissez les paramètres de connexion pour le nouveau Serveur d'administration.

   - Via la tâche *Modification du Serveur d'administration*

     Créez une tâche *Modification du Serveur d'administration*, et définissez les appareils administrés importés, le nouveau Serveur d'administration et d'autres paramètres de la tâche. Exécutez ensuite la tâche pour placer les appareils administrés sous la gestion du Serveur d'administration de Kaspersky Security Center Linux.

   - Par la suppression (si déjà installé) et la poursuite de l'installation de l'Agent d'administration sur les appareils administrés

     Créez un nouveau paquet d'installation de l'Agent d'administration et définissez les paramètres de connexion pour le nouveau Serveur d'administration dans les propriétés du paquet d'installation. Supprimez l'Agent d'administration sur les appareils administrés importés, puis utilisez le paquet d'installation pour installer l'Agent d'administration sur les appareils administrés importés via une tâche d'installation à distance. Vous pouvez également créer et utiliser un paquet d'installation autonome pour installer l'Agent d'administration localement. Pour plus d'informations, consultez Basculer les appareils administrés sous l'administration de Kaspersky Security Center Linux.

   - Par la restauration du certificat et de la clé privée du Serveur d'administration à partir d'une copie de sauvegarde (uniquement pour la migration vers Kaspersky Security Center Linux 15.1 ou une version ultérieure)

     Attribuez la même adresse réseau à l'appareil équipé du Serveur d'administration de Kaspersky Security Center Linux que sur le Serveur d'administration de Kaspersky Security Center Windows. Lancez l'utilitaire klbackup avec le paramètre `-cert_only` pour restaurer le certificat du Serveur d'administration et la clé privée à partir de la copie de sauvegarde que vous avez enregistrée à l'étape 2. Dans la ligne de commande, exécutez la commande suivante : `/opt/kaspersky/ksc64/sbin/klbackup -path <chemin d'accès à la copie de sauvegarde du certificat du Serveur d'administration> -restore -cert_only`. Pour plus d'informations, consultez la section Utilisation de l'utilitaire klbackup pour basculer des appareils gérés sous l'administration d'un autre Serveur d'administration.

7. **Mettre à jour l'Agent d'administration vers la dernière version**

   Nous vous recommandons de mettre à jour l'Agent d'administration pour Linux vers la même version que Kaspersky Security Center.

8. **Assurez-vous que les appareils administrés sont visibles sur le nouveau Serveur d'administration**

Sur le Serveur d'administration de Kaspersky Security Center Linux, ouvrez la liste des appareils administrés (**Ressources (Appareils)** → **Appareils administrés**) et vérifiez les valeurs dans les colonnes **Visible**, **L'Agent d'administration est installé** et **Dernière connexion au Serveur d'administration**.

Autres méthodes de migration des données

Outre l'Assistant de migration, vous pouvez également transférer des tâches et des stratégies spécifiques :

- Exportez des tâches depuis Kaspersky Security Center Windows, puis importez les tâches dans Kaspersky Security Center Linux.
- Exportez des stratégies spécifiques depuis Kaspersky Security Center Windows, puis importez les stratégies dans Kaspersky Security Center Linux. Les profils de stratégie associés sont exportés et importés avec les stratégies sélectionnées.

Exportation des objets du groupe depuis Kaspersky Security Center Windows

Structure des groupes d'administration des migrations, y compris les appareils administrés et autres groupes d'objets du Kaspersky Security Center Windows vers Kaspersky Security Center Linux, vous devez d'abord sélectionner les données à exporter et créer un fichier d'exportation. Le fichier d'exportation contient les informations sur tous les objets de groupe que vous souhaitez migrer. Le fichier d'exportation sera utilisé pour une importation ultérieure dans Kaspersky Security Center Linux.

Vous pouvez exporter les objets suivants :

- Tâches et stratégies des applications administrées
- Tâches globales
- Sélections d'appareils personnalisés
- Structure du groupe d'administration et appareils inclus
- Tags attribués aux appareils en migration

Avant de commencer à exporter, lisez les informations générales sur la migration vers Kaspersky Security Center Linux. Choisissez la méthode de migration, en utilisant ou sans la hiérarchie des Serveurs d'administration de Kaspersky Security Center Windows et Kaspersky Security Center Linux.

Pour exporter des appareils administrés et des objets de groupe associés via l'Assistant de migration, procédez comme suit :

1. Selon que les Serveurs d'administration de Kaspersky Security Center Windows et de Kaspersky Security Center Linux sont hiérarchisés ou non, effectuez l'une des opérations suivantes :
   - Si les Serveurs sont organisés selon une hiérarchie, ouvrez Kaspersky Security Center Web Console, puis basculez vers le Serveur de Kaspersky Security Center Windows.
   - Si les Serveurs ne sont pas hiérarchisés, ouvrez Kaspersky Security Center Web Console connecté à Kaspersky Security Center Windows.
2. Dans le menu principal, accédez à **Opérations** → **Migration**.

3. Pour lancer l'Assistant et suivre les étapes, sélectionnez l'emplacement où vous souhaitez transférer les données et les paramètres.

   - Si vous souhaitez transférer vos données et vos paramètres vers Kaspersky Security Center Cloud Console, sélectionnez l'option **Migrer vers Kaspersky Security Center Cloud Console**.

   - Si vous souhaitez transférer vos données et vos paramètres vers Kaspersky Security Center Linux ou Kaspersky Next XDR Expert, sélectionnez l'option **Passer à Kaspersky Security Center Linux ou à Open Single Management Platform**.

4. Sélectionnez le groupe d'administration ou le sous-groupe que vous souhaitez exporter. Assurez-vous que le groupe d'administration ou le sous-groupe sélectionné ne contient pas plus de 10 000 appareils.

5. Sélectionnez les applications administrées dont les tâches et les stratégies seront exportées. Sélectionnez uniquement les applications compatibles avec Kaspersky Security Center Linux. Les objets des applications non compatibles seront exportés, mais ils ne seront pas opérationnels.

6. Utilisez les liens sur la gauche pour choisir les tâches globales, les sélections d'appareils et les rapports à exporter. Le lien **Objets de groupe** permet d'exclure de l'exportation des rôles personnalisés, des utilisateurs internes et des groupes de sécurité, ainsi que des catégories d'applications personnalisées.

Le fichier d'exportation (archive ZIP) est créé. Selon que vous migrez avec prise en charge de la hiérarchie de Serveur d'administration ou non, le fichier d'exportation est enregistré comme suit :

- En cas d'organisation hiérarchique des Serveurs, le fichier d'exportation est enregistré dans le dossier temporaire sur le Serveur de Kaspersky Security Center Web Console.

- Si les Serveurs ne sont pas hiérarchiques, le fichier d'exportation est téléchargé sur votre appareil.

Pour la migration avec prise en charge de la hiérarchie du Serveur d'administration, l'importation démarre automatiquement après un exportation réussie. Pour une migration sans prise en charge de la hiérarchie du Serveur d'administration, vous pouvez importer manuellement le fichier d'exportation enregistré dans Kaspersky Security Center Linux.

Importation du fichier d'exportation Kaspersky Security Center Cloud Linux

Pour transférer des informations relatives aux appareils administrés, aux objets et à leurs paramètres que vous avez exportés à partir de Kaspersky Security Center Windows, vous devez importer celles-ci dans Kaspersky Security Center Linux ou Kaspersky Next XDR Expert.

Pour importer des appareils administrés et des objets associés via l'Assistant de migration, procédez comme suit :

1. Selon que les Serveurs d'administration de Kaspersky Security Center Windows et de Kaspersky Security Center Linux sont hiérarchisés ou non, effectuez l'une des opérations suivantes :

   - Si les Serveurs sont organisés en hiérarchie, passez à l'étape suivante de l'Assistant de migration une fois l'exportation terminée. L'importation démarre automatiquement après une exportation réussie dans cet Assistant (voir l'étape 2 de cette instruction).

   - Si les Serveurs ne sont pas hiérarchisés :

     a. Ouvrez Kaspersky Security Center Web Console connectée à Kaspersky Security Center Linux ou Kaspersky Next XDR Expert.

     b. Dans le menu principal, accédez à **Opérations** → **Migration**.

     c. Sélectionnez le fichier d'exportation (archive ZIP) que vous avez créé et téléchargé lors de l'exportation depuis Kaspersky Security Center Windows. Le téléchargement du fichier d'exportation démarre.

2. Une fois le fichier d'exportation téléchargé avec succès, vous pouvez continuer l'importation. Si vous souhaitez spécifier un autre fichier d'exportation, cliquez sur le lien **Modifier**, puis sélectionnez le fichier requis.

3. L'ensemble de la hiérarchie des groupes d'administration de Kaspersky Security Center Linux est affiché.

   Cochez la case en regard du groupe d'administration cible dans lequel les objets du groupe d'administration exporté (appareils administrés, stratégies, tâches et autres objets du groupe) doivent être restaurés.

4. L'importation des objets de groupe démarre. Il est impossible de réduire l'Assistant de migration et d'effectuer des opérations simultanées lors de l'importation. Attendez que les icônes de rafraîchissement (🔄) à côté de tous les éléments de la liste des objets soient remplacées par des coches vertes (✓) et que l'importation soit terminée.

5. Une fois que l'importation est terminée, la structure exportée des groupes d'administration, y compris les détails des appareils, apparaît sous le groupe d'administration cible que vous avez sélectionné. Si le nom de l'objet que vous restaurez est identique au nom d'un objet existant, un suffixe incrémentiel est ajouté à l'objet restauré.

> Si la tâche migrée reprend les détails du compte à partir duquel la tâche est exécutée sont spécifiées, vous devez ouvrir la tâche et saisir à nouveau le mot de passe une fois l'importation terminée.

Si l'importation s'est terminée avec une erreur, vous pouvez effectuer l'une des opérations suivantes :

- Pour la migration avec prise en charge de la hiérarchie du Serveur d'administration, vous pouvez recommencer l'importation du fichier d'exportation.

- Pour la migration sans prise en charge de la hiérarchie du Serveur d'administration, vous pouvez démarrer l'Assistant de migration pour sélectionner un autre fichier d'exportation, puis l'importer à nouveau.

Vous pouvez vérifier si les objets de groupe inclus dans la portée d'exportation ont été importés avec succès dans Kaspersky Security Center Linux. Pour ce faire, rendez-vous dans la section **Ressources (Appareils)** et assurez-vous que les objets importés apparaissent dans les sous-sections correspondantes.

Notez que les appareils gérés importés sont affichés dans la sous-section **Appareils administrés**, mais ils sont invisibles sur le réseau et l'Agent d'administration n'est pas installé ni exécuté sur eux (la valeur *Non* dans les colonnes **Visible**, **L'Agent d'administration est installé** et **L'Agent d'administration est en cours d'exécution**).

Pour terminer la migration, vous devez faire en sorte que les appareils administrés soient administrés par Kaspersky Security Center Linux.

Basculer les appareils administrés vers l'administration de Kaspersky Security Center Linux

Après une importation réussie des informations sur les appareils administrés, les objets et leurs paramètres vers Kaspersky Security Center Linux, vous devez faire passer les appareils administrés sous l'administration de Kaspersky Security Center Linux pour terminer la migration.

Vous pouvez déplacer les appareils administrés vers Kaspersky Security Center Linux d'une des manières suivantes :

- Via l'utilitaire klmover.
- Via la tâche *Modification du Serveur d'administration*.
- Restauration du certificat et de la clé privée du Serveur d'administration à partir d'une copie de sauvegarde (uniquement pour la migration vers Kaspersky Security Center Linux 15.1 ou une version ultérieure).

  Pour en savoir plus, reportez-vous à l'étape 6 du scénario de migration principal.
- Installation de l'Agent d'administration sur les appareils administrés via la tâche d'installation à distance.

Pour faire passer les appareils administrés sous l'administration de Kaspersky Security Center Linux en installant l'Agent d'administration :

1. Supprimez l'Agent d'administration sur les appareils administrés importés qui passeront sous la gestion de Kaspersky Security Center Linux.
2. Basculez vers le Serveur d'administration de Kaspersky Security Center Windows.
3. Accédez à **Découverte et déploiement** → **Déploiement et attribution** → **Paquets d'installation**, puis ouvrez les propriétés d'un package d'installation existant de l'Agent d'administration.

   Si le paquet d'installation de l'Agent d'administration est absent de la liste des paquets, téléchargez-en un nouveau.

   Vous pouvez également créer et utiliser un paquet d'installation autonome pour installer l'Agent d'administration localement.
4. Sous l'onglet **Paramètres**, sélectionnez la section **Connexion**. Spécifiez les paramètres de connexion du Serveur d'administration de Kaspersky Security Center Linux.
5. Créez une tâche d'installation à distance pour les appareils administrés, puis spécifiez le paquet d'installation de l'Agent d'administration reconfiguré.

   Vous pouvez installer l'Agent d'administration via le Serveur d'administration de Kaspersky Security Center Windows ou via un appareil Windows faisant office de point de distribution. Si vous utilisez le Serveur d'administration, activez l'option **En utilisant les ressources du système d'exploitation via le Serveur d'administration**. Si vous utilisez un point de distribution, activez l'option **En utilisant les ressources du système d'exploitation via les points de distribution**.
6. Lancez la tâche d'installation à distance de l'application.

Une fois la tâche d'installation à distance terminée, accédez au Serveur d'administration de Kaspersky Security Center Linux et assurez-vous que les appareils administrés sont visibles sur le réseau et que l'Agent d'administration est installé et exécuté sur eux (la valeur *Oui* dans les colonnes **Visible**, **L'Agent d'administration est installé**, et **L'Agent d'administration est en cours d'exécution**).

Connexion et déconnexion de Kaspersky Security Center Web Console

Vous pouvez vous connecter à Kaspersky Security Center Web Console après avoir installé le Serveur d'administration et le Serveur de la Web Console. Vous devez connaître l'adresse Internet du Serveur d'administration et le numéro de port indiqué pendant l'installation (par défaut, le numéro de port est 8080). Dans votre navigateur, JavaScript doit être activé.

Vous pouvez vous connecter à Kaspersky Security Center Web Console à l'aide des méthodes suivantes :

- En utilisant l'authentification de domaine

  > Si vous choisissez cette méthode, assurez-vous que le sondage du contrôleur de domaine est activé et que les utilisateurs du domaine sont ajoutés au Serveur d'administration.

- En indiquant le nom d'utilisateur et le mot de passe du domaine
- En indiquant le nom d'utilisateur et le mot de passe de l'administrateur

Connexion à l'aide de l'authentification de domaine

Pour vous connecter à Kaspersky Security Center Web Console à l'aide de l'authentification de domaine :

1. Dans votre navigateur, accédez à l'adresse https://`<Adresse de Kaspersky Security Center Web Console>:<Numéro de port>`

   La page de connexion s'affiche.

2. Si vous avez ajouté plusieurs serveurs de confiance, dans la liste des Serveurs d'administration, sélectionnez 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 n'est pas affiché.

3. Exécutez une des actions suivantes :

   - Cliquez sur le bouton **Utiliser l'authentification du domaine**.
   - Si un ou plusieurs Serveurs d'administration virtuels sont créés sur le Serveur et que vous souhaitez vous connecter à un Serveur virtuel, en utilisant l'authentification de domaine :

     a. Cliquez sur **Afficher les options du Serveur virtuel**.

     b. Saisissez le nom du Serveur d'administration virtuel que vous avez indiqué lors de la création du Serveur virtuel.

     c. Cliquez sur le bouton **Utiliser l'authentification du domaine**.

4. Si la vérification en deux étapes est activée pour votre compte, indiquez le code de sécurité généré par l'application d'authentification sur l'appareil mobile.

   Si nécessaire, vous pouvez revenir à la page de connexion.

Une fois connecté, le tableau de bord s'affiche dans la langue et le thème utilisés pour la dernière fois. Vous pouvez naviguer dans Kaspersky Security Center Web Console et l'utiliser avec Kaspersky Security Center.

Connexion en indiquant le nom d'utilisateur et le mot de passe de l'administrateur

Pour vous connecter à Kaspersky Security Center Web Console à l'aide du nom d'utilisateur et du mot de passe de l'administrateur, procédez comme suit :

1. Dans votre navigateur, accédez à l'adresse https://`<Adresse de Kaspersky Security Center Web Console>:<Numéro de port>`

   La page de connexion s'affiche.

2. Si vous avez ajouté plusieurs serveurs de confiance, dans la liste des Serveurs d'administration, sélectionnez 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 n'est pas affiché.

3. Exécutez une des actions suivantes :

   - Pour se connecter au Serveur d'administration avec un compte utilisateur de domaine, procédez comme suit :

     a. Indiquez le nom d'utilisateur et le mot de passe de l'utilisateur du domaine.

     Vous pouvez saisir le nom d'utilisateur de l'utilisateur du domaine dans l'un des formats suivants :

     - `Username@dns.domain`
     - `NTDOMAIN\Username`

     b. Cliquez sur le bouton **Se connecter**.

     Avant de vous connecter avec un compte d'utilisateur de domaine, interrogez le contrôleur de domaine pour obtenir la liste des utilisateurs du domaine.

   - Pour vous connecter au Serveur d'administration :

     a. Saisissez le nom d'utilisateur et le mot de passe de l'Administrateur local.

     b. Cliquez sur le bouton **Se connecter**.

   - Si un ou plusieurs Serveurs d'administration virtuels sont créés sur le Serveur et que vous souhaitez vous connecter à un Serveur virtuel :

     a. Cliquez sur **Afficher les options du Serveur virtuel**.

     b. Saisissez le nom du Serveur d'administration virtuel que vous avez indiqué lors de la création du Serveur virtuel.

     c. Saisissez le nom utilisateur et le mot de passe de l'administrateur qui dispose des privilèges sur le Serveur d'administration virtuel.

     d. Cliquez sur le bouton **Se connecter**.

4. Si la vérification en deux étapes est activée pour votre compte, indiquez le code de sécurité généré par l'application d'authentification sur l'appareil mobile.

   Si nécessaire, vous pouvez revenir à la page de connexion.

5. Si la modification forcée du mot de passe est activée pour votre compte ou si votre mot de passe a expiré, la fenêtre de modification du mot de passe s'affiche. Définissez un nouveau mot de passe pour vous connecter à Kaspersky Security Center Web Console.

Une fois connecté, le tableau de bord s'affiche dans la langue et le thème utilisés pour la dernière fois. Vous pouvez naviguer dans Kaspersky Security Center Web Console et l'utiliser avec Kaspersky Security Center.

Déconnexion

Pour vous déconnecter de Kaspersky Security Center Web Console,

Dans le menu principal, allez dans les paramètres de votre compte et sélectionnez **Se déconnecter**.

Kaspersky Security Center Web Console se ferme, et la page de connexion s'affiche.

Gestionnaire des identités et des accès dans Kaspersky Security Center Web Console

Cette section fournit des informations sur le Gestionnaire des identités et des accès (également appelé IAM).

À propos du Gestionnaire des identités et des accès

Le *Gestionnaire des identités et des accès* (également appelé IAM) est un module de Kaspersky Security Center Web Console qui vous permet d'utiliser une authentification unique (SSO) entre Kaspersky Security Center Web Console et l'interface Internet de Kaspersky Industrial CyberSecurity for Networks Console. IAM utilise le protocole OAuth 2.0 pour assurer l'autorisation de Kaspersky Industrial CyberSecurity for Networks dans Kaspersky Security Center Web Console.

Dans ce cas, Kaspersky Industrial CyberSecurity for Networks, auquel vous avez accès via Kaspersky Security Center Web Console, est appelé *serveur de ressources*, et Kaspersky Security Center Web Console et l'interface Internet de Kaspersky Industrial CyberSecurity for Networks Console sont appelés *clients OAuth 2.0*. Un serveur de ressources est un programme qui fonctionne avec plusieurs utilisateurs et qui nécessite une autorisation. Le client utilise un *jeton* pour procéder à l'autorisation sur le serveur de ressources. Un jeton est une séquence unique d'octets. Lorsqu'un jeton expire, il est automatiquement réémis. IAM agit comme un serveur d'autorisation unique pour plusieurs clients OAuth 2.0.

Vous pouvez installer IAM lors de l'installation de Kaspersky Security Center Web Console. Vous pouvez l'activer ultérieurement à tout moment dans les paramètres de Kaspersky Security Center Web Console. Si un serveur Kaspersky Industrial CyberSecurity ou une interface Internet de Kaspersky Industrial CyberSecurity est installé sur un appareil administré par le même Serveur d'administration, IAM détecte ce programme, et une notification s'affiche dans Kaspersky Security Center Web Console pour vous en informer. Vous pouvez enregistrer Kaspersky Industrial CyberSecurity for Networks et utiliser la SSO (technologie d'authentification unique) pour Kaspersky Security Center Web Console et l'interface Internet de Kaspersky Industrial CyberSecurity for Networks.

Si vous vous déconnectez de Kaspersky Security Center Web Console, votre session dans l'interface Internet de Kaspersky Industrial CyberSecurity for Networks se terminera et vous devrez vous reconnecter à Kaspersky Security Center Web Console.

Activation du Gestionnaire des identités et des accès : scénario

Prérequis

Avant de commencer, assurez-vous d'avoir accès à Kaspersky Industrial CyberSecurity for Networks version 3.1 ou à toute version ultérieure.

Étapes

L'activation du Gestionnaire des identités et des accès (également appelée IAM) se déroule par étapes :

1. **Vérification des ports requis**

   Assurez-vous que les ports 3333, 4004 et 4444 sont ouverts sur l'appareil sur lequel Kaspersky Security Center Web Console est installé. Ces ports sont nécessaires pour utiliser OAuth 2.0. Si vous le souhaitez, vous pouvez modifier les numéros de port par défaut dans la fenêtre des paramètres de Kaspersky Security Center Web Console.

   Outre les ports 3333, 4004 et 4444, Kaspersky Security Center Web Console utilise également les ports 4445, 2444 et 2445 à des fins diverses.

2. **Installation du Gestionnaire des identités et des accès**

   Pendant l'installation de Kaspersky Security Center Web Console, indiquez que vous souhaitez installer le Gestionnaire des identités et des accès. Si vous ne l'avez pas fait, exécutez de nouveau l'Assistant d'installation de Kaspersky Security Center Web Console.

3. **Configuration du Gestionnaire des identités et des accès**

   Dans la fenêtre des paramètres de Kaspersky Security Center Web Console, assurez-vous que le commutateur **Gestionnaire des identités et des accès (IAM)** est activé. Indiquez également le DNS de l'appareil sur lequel Kaspersky Security Center Web Console est installé : les applications clientes se connecteront à cet appareil.

4. **Spécification des paramètres du jeton**

   Dans la fenêtre des paramètres de Kaspersky Security Center Web Console, indiquez la durée de vie des jetons ainsi que le délai d'expiration de l'autorisation que le Gestionnaire des identités et des accès utilisera. Vous pouvez utiliser les valeurs par défaut ou indiquer vos propres valeurs en fonction de vos besoins.

5. **Octroi de certificats**

   Si vous préférez utiliser les certificats générés par le Serveur d'administration, téléchargez, dans la fenêtre des paramètres de Kaspersky Security Center Web Console, les certificats racine des ports utilisés par IAM et distribuez-les aux postes de travail des utilisateurs de Kaspersky Security Center Web Console. Sinon, les navigateurs des utilisateurs présenteront des messages d'erreur lors de la tentative de connexion à Kaspersky Security Center Web Console.

6. **Enregistrement des serveurs de Kaspersky Industrial CyberSecurity for Networks et des interfaces Web de Kaspersky Industrial CyberSecurity for Networks**

Une fois IAM installé, Kaspersky Security Center Web Console affiche un message indiquant qu'un serveur Industrial CyberSecurity for Networks (ou plusieurs serveurs) et une ou plusieurs interfaces Internet de Kaspersky Industrial CyberSecurity for Networks attendent d'être enregistrés. Cliquez sur ce message pour enregistrer votre serveur (ou plusieurs serveurs) et votre interface Web (ou plusieurs interfaces Web) de Kaspersky Industrial CyberSecurity for Networks.

Résultats

Après avoir terminé ce scénario, vous serez en mesure d'utiliser l'authentification unique et IAM pour Kaspersky Industrial CyberSecurity for Networks et Kaspersky Security Center Web Console.

Configuration du Gestionnaire des identités et des accès dans Kaspersky Security Center Web Console

Pour configurer le Gestionnaire des identités et des accès selon vos besoins, procédez comme suit :

1. Dans le menu principal, accédez à **Paramètres** → **Gestionnaire des identités et des accès**.
2. Dans la section **Gestionnaire des identités et des accès**, assurez-vous que le Gestionnaire des identités et des accès est activé.
3. Cliquez sur le lien **Paramètres** sous la ligne **Nom de réseau de l'appareil du gestionnaire des identités et des accès**.
4. Indiquez le DNS de l'appareil sur lequel vous avez installé le Gestionnaire des identités et des accès. Les applications clientes se connecteront à cet appareil.
5. Si vous le souhaitez, modifiez les paramètres de jeton par défaut, les paramètres de certificat et les numéros de port en cliquant sur le lien **Paramètres** situé sous le groupe de paramètres correspondant.

Le Gestionnaire des identités et des accès est activé et fonctionne selon vos besoins.

Enregistrement de l'application Kaspersky Industrial CyberSecurity for Networks dans Kaspersky Security Center Web Console

Pour commencer à utiliser l'application Kaspersky Industrial CyberSecurity for Networks via Kaspersky Security Center Web Console, vous devez d'abord l'enregistrer dans Kaspersky Security Center Web Console.

Pour enregistrer l'application Kaspersky Industrial CyberSecurity for Networks :

1. Assurez-vous que ce qui suit est fait :

   - Vous avez téléchargé et installé le plug-in Internet de Kaspersky Industrial CyberSecurity for Networks.

     Cependant, vous pouvez le faire plus tard en attendant que le Serveur de Kaspersky Industrial CyberSecurity for Networks Server se synchronise avec le Serveur d'administration.

   - Vous avez terminé le scénario de préparation à l'utilisation de la technologie Single Sign-On (SSO).

   - Les paramètres nécessaires dans l'interface Web de Kaspersky Industrial CyberSecurity for Networks sont spécifiés sur la page de Kaspersky Security Center. Pour plus de détails, veuillez consulter l'Aide en ligne de Kaspersky Industrial CyberSecurity for Networks.

   - Vous êtes connecté à Kaspersky Security Center Web Console sous un compte administrateur.

   - IAM est configuré.

2. Déplacez l'appareil sur lequel Kaspersky Industrial CyberSecurity for Networks Server est installé du groupe Appareils non attribués vers le groupe Appareils administrés :

   a. Dans le menu principal, accédez à **Découverte et déploiement** → **Appareils non définis**.

   b. Cochez la case à côté de l'appareil sur lequel Kaspersky Industrial CyberSecurity for Networks Server est installé.

   c. Cliquez sur le bouton **Déplacer vers le groupe**.

   d. Dans la hiérarchie des groupes d'administration, cochez la case à côté du groupe Appareils administrés.

   e. Cliquez sur le bouton **Déplacer**.

3. Accédez aux propriétés de l'appareil sur lequel Kaspersky Industrial CyberSecurity for Networks Server est installé.

4. Sur la page des propriétés de l'appareil, dans la section **Général**, sélectionnez l'option **Maintenir la connexion au Serveur d'administration**, puis cliquez sur le bouton **Sauvegarder**.

5. Dans la fenêtre des propriétés de l'appareil, sélectionnez la section **Applications**.

6. Dans la section **Applications**, sélectionnez Kaspersky Network Agent.

7. Si l'état actuel de l'application est *Arrêté*, attendez qu'il devienne *En cours d'exécution*.

   Cela peut prend jusqu'à 15 minutes. Si vous n'avez pas encore installé le plug-in Web Kaspersky Industrial CyberSecurity for Networks, vous pouvez le faire maintenant, en attendant.

8. Dans le menu principal, accédez à **Paramètres** → **Gestionnaire des identités et des accès**.

   Dans le champ **Demandes d'enregistrement**, une demande en attente est affichée.

9. Cliquez sur le lien **Paramètres** sous le champ **Demandes d'enregistrement**.

10. Dans la liste des clients enregistrés qui s'ouvre, cochez la case à côté du nom du serveur Kaspersky Industrial CyberSecurity for Networks, qui a l'état *En attente*, puis cliquez sur le bouton **Approuver**.

    Si vous ne souhaitez pas enregistrer Kaspersky Industrial CyberSecurity for Networks Server, vous pouvez cliquer sur le bouton Refuser et revenir ultérieurement à cette liste.

    Après avoir cliqué sur le bouton **Approuver**, l'état passe à *Approuvé*, puis à *Prêt*. Si l'état ne change pas, vous pouvez cliquer sur le bouton Actualiser.

11. Fermez la liste des clients enregistrés et assurez-vous que la valeur dans le champ **Clients enregistrés** a augmenté.

12. Pour ajouter le widget Kaspersky Industrial CyberSecurity for Networks sur le tableau de bord :

    a. Dans le menu principal, accédez à **Surveillance et rapports → Tableau de bord**.

    b. Sur tableau de bord, cliquez sur le bouton **Ajouter ou restaurer un widget web**.

    c. Dans le menu du widget qui s'ouvre, sélectionnez **Autre**.

    d. Sélectionnez le widget Kaspersky Industrial CyberSecurity for Networks.

    Vous pouvez maintenant accéder à l'interface Web de Kaspersky Industrial CyberSecurity for Networks à l'aide du lien dans le widget.

Une fois la procédure d'enregistrement terminée, un nouveau bouton, **Kaspersky Security Center**, apparaît sur la page de connexion de l'interface Web de Kaspersky Industrial CyberSecurity for Networks. Vous pouvez cliquer sur ce bouton pour vous connecter à l'interface Web de Kaspersky Industrial CyberSecurity for Networks avec vos identifiants de Kaspersky Security Center.

Durée de vie des jetons et délai d'expiration de l'autorisation pour le Gestionnaire des identités et des accès

Lors de la configuration du Gestionnaire des identités et des accès (également appelé IAM), vous devez indiquer les paramètres de durée de vie du jeton et de délai d'expiration de l'autorisation. Les paramètres par défaut sont conçus pour refléter à la fois les normes de sécurité et la charge du serveur. Cependant, vous pouvez modifier ces paramètres en fonction des stratégies de votre organisation.

IAM réémet automatiquement un jeton lorsqu'il est sur le point d'expirer.

Le tableau ci-dessous indique les paramètres de durée de vie du jeton par défaut.

Paramètres de durée de vie du jeton

Jeton	Durée de vie par défaut (en secondes)	Description
Jeton d'identité (id_token)	86400	Jeton d'identité utilisé par le client OAuth 2.0 (c'est-à-dire Kaspersky Security Center Web Console ou Kaspersky Industrial CyberSecurity Console). IAM envoie au client le jeton d'identification contenant des informations sur l'utilisateur (c'est-à-dire le profil utilisateur).
Jeton d'accès (access_token)	86400	Jeton d'accès utilisé par le client OAuth 2.0 pour accéder au serveur de ressources au nom du propriétaire de la ressource identifié par IAM.
Jeton d'actualisation (refresh_token)	172800	Le client OAuth 2.0 utilise ce jeton pour réémettre le jeton d'identité et le jeton d'accès.

Le tableau ci-dessous répertorie les délais d'expiration pour auth_code et login_consent_request.

Paramètres du délai d'expiration de l'autorisation

Paramètre	Délai d'expiration par défaut (en secondes)	Description
Code d'autorisation (auth_code)	3600	Délai d'expiration pour l'échange de code pour le jeton. Le client OAuth 2.0 envoie ce code au serveur de ressources et obtient le jeton d'accès en échange.
Délai d'expiration de la demande d'accord de connexion (login_consent_request)	3600	Délai d'expiration pour la délégation des droits d'utilisateur au client OAuth 2.0.

Pour obtenir plus d'informations sur les jetons, consultez le site Web d'OAuth.

Pour configurer le délai d'attente pour les clients qui ne détectent aucune activité de la souris ou du clavier, procédez comme suit :

1. Dans le dossier d'installation de Kaspersky Security Center Web Console, recherchez et ouvrez le fichier config.json. Le fichier contient les paramètres de configuration du délai d'attente pour les clients inactifs.

2. Utilisez le paramètre `clientIdleTimeout` pour indiquer le délai, en millisecondes, après lequel un client inactif affiche une fenêtre contextuelle d'avertissement.

3. Utilisez le paramètre `clientLogoutTimeout` pour indiquer le délai, en millisecondes, après lequel les autorisations IAM pour le client inactif prennent fin. `clientLogoutTimeout` commence un compte à rebours séquentiel après `clientIdleTimeout`.

Téléchargement et distribution des certificats IAM

Par défaut, le Gestionnaire des identités et des accès utilise les certificats générés par le Serveur d'administration pour permettre aux navigateurs d'accéder à Kaspersky Security Center Web Console. Cependant, si vous le souhaitez, vous pouvez utiliser des certificats personnalisés. Quel que soit le certificat que vous utilisez, vous devez vous assurer que tous les postes de travail à partir desquels les utilisateurs de Kaspersky Security Center Web Console accèdent à Kaspersky Security Center Web Console font confiance à ce certificat.

Pour télécharger et distribuer des certificats, procédez comme suit :

1. Dans le menu principal, accédez à **Paramètres** → **Gestionnaire des identités et des accès**.
2. Pour chaque certificat, cliquez sur le lien **Paramètres** sous le groupe de paramètres approprié, puis effectuez l'une des opérations suivantes :
   - Si vous souhaitez utiliser le certificat généré par le Serveur d'administration lors de l'installation de Kaspersky Security Center Web Console, procédez comme suit :
     1. Sélectionnez **Certificat généré par le Serveur d'administration** dans la fenêtre des propriétés du certificat qui s'ouvre.
     2. Cliquez sur le bouton **Télécharger** pour télécharger le certificat.
     3. Distribuez le certificat téléchargé à tous les postes de travail à partir desquels les utilisateurs de Kaspersky Security Center Web Console accèdent à Kaspersky Security Center Web Console.
   - Si vous avez un certificat que vous souhaitez utiliser, procédez comme suit :
     1. Sélectionnez **Certificat TLS personnalisé** dans la fenêtre des propriétés du certificat qui s'ouvre.
     2. Sélectionnez le fichier de certificat et la clé privée.
     3. Cliquez sur le bouton **OK**.
     4. Distribuez le certificat à tous les postes de travail à partir desquels les utilisateurs accèdent à Kaspersky Security Center Web Console ou à Kaspersky Industrial CyberSecurity Console.

Les certificats permettent aux utilisateurs d'accéder à Kaspersky Security Center Web Console et à Kaspersky Industrial CyberSecurity Console.

Vous devez émettre de nouveau tous les certificats en temps voulu. Les certificats générés par le Serveur d'administration doivent être générés de nouveau manuellement. Les certificats générés par le programme d'installation de Kaspersky Security Center Web Console doivent être générés de nouveau en utilisant le programme d'installation.

Désactivation du Gestionnaire des identités et des accès

Si vous le souhaitez, vous pouvez désactiver le Gestionnaire des identités et des accès (également appelé IAM).

Pour désactiver IAM, procédez comme suit :

1. Dans le menu principal, accédez à **Paramètres** → **Intégration**.
2. Dans la section **Gestionnaire des identités et des accès**, désactivez le commutateur **Gestionnaire des identités et des accès**.

Vous pouvez activer IAM à tout moment ultérieurement.

Si vous mettez à jour Kaspersky Security Center Web Console via le programme d'installation et indiquez que vous ne souhaitez pas installer IAM, Kaspersky Security Center Web Console sera mis à niveau, et IAM ne sera pas installé. Toutes les informations sur l'intégration avec Kaspersky Industrial CyberSecurity for Networks seront supprimées de votre appareil ainsi que les fichiers de configuration IAM et les fichiers journaux.

Configuration de l'authentification de domaine à l'aide des protocoles NTLM et Kerberos

Kaspersky Security Center 15.1 vous permet d'utiliser l'authentification de domaine dans OpenAPI en utilisant les protocoles NTLM et Kerberos. L'utilisation de l'authentification de domaine permet à un utilisateur Windows d'activer l'authentification sécurisée dans Kaspersky Security Center Web Console sans avoir à ressaisir le mot de passe sur le réseau d'entreprise (authentification unique).

L'authentification de domaine dans OpenAPI via le protocole Kerberos comporte les restrictions suivantes :

- L'utilisateur de Kaspersky Security Center Web Console doit être authentifié dans Active Directory à l'aide du protocole Kerberos. L'utilisateur doit disposer d'un Ticket Granting Ticket Kerberos valide (également appelé TGT). Un TGT est émis automatiquement lorsque vous vous authentifiez auprès du domaine.

- Vous devez configurer l'authentification Kerberos dans le navigateur. Pour plus de détails, reportez-vous à la documentation du navigateur que vous utilisez.

Si vous souhaitez utiliser l'authentification de domaine à l'aide des protocoles Kerberos, votre réseau doit remplir les conditions suivantes :

- Le Serveur d'administration doit fonctionner sous le nom du compte de domaine.

- Kaspersky Security Center Web Console Server doit être installé sur le même appareil sur lequel le serveur d'administration est installé.

- Vous devez préciser les noms des principaux du service (SPN) suivants pour le compte du Serveur d'administration :

  - "http/<server.fqnd.name>"

  - "http/<server>"

  Ici,<server> est le nom réseau du Serveur d'administration, et <server.fqnd.name> est le nom de domaine pleinement qualifié de l'appareil du Serveur d'administration.

- Lors de la connexion à la Console d'administration ou à Kaspersky Security Center Web Console, l'adresse du Serveur d'administration doit être indiquée exactement comme l'adresse pour laquelle le nom principal du service (SPN) est enregistré. Vous pouvez spécifier soit <server.fqnd.name>, soit <server>.

- Pour une connexion sans mot de passe, le processus du navigateur dans lequel Kaspersky Security Center Web Console est ouvert en tant que navigateur doit être exécuté sous un compte de domaine.

Les protocoles Kerberos et NTLM ne sont pris en charge que dans OpenAPI pour Kaspersky Security Center 15.1. Ils ne sont pas pris en charge dans OpenAPI pour Kaspersky Security Center Linux.

Configuration du Serveur d'administration

Cette section décrit la configuration et les propriétés du Serveur d'administration de Kaspersky Security Center.

Configuration de la connexion de Kaspersky Security Center Web Console au serveur d'administration

Pour définir les ports de connexion du Serveur d'administration, procédez comme suit :

1. Dans le menu principal, cliquez sur l'icône paramètres ( ) en face du nom du Serveur d'administration requis.
   La fenêtre des propriétés du Serveur d'administration s'ouvre.
2. Sous l'onglet **Général**, sélectionnez la section **Ports de connexion**.

L'application affiche les principaux paramètres de connexion du Serveur sélectionné.

Kaspersky Security Center Web Console est connecté au Serveur d'administration via le port SSL TCP 13299. Le même port peut être utilisé par les objets d'automatisation de l'utilitaire klakaut.

Le port TCP 14000 peut être utilisé pour connecter Kaspersky Security Center Web Console, les points de distribution, les Serveurs d'administration secondaires et les objets d'automatisation de l'utilitaire klakaut, ainsi que pour recevoir des données depuis les appareils clients.

En général, le port SSL TCP 13000 peut être utilisé uniquement par l'Agent d'administration, un Serveur d'administration secondaire et le Serveur d'administration principal installé en zone démilitarisée. Dans certains cas, la connexion de Kaspersky Security Center Web Console devra être établie via le port SSL 13000 :

- Si un port SSL unique doit être utilisé aussi bien pour Kaspersky Security Center Web Console que pour les autres activités (la réception des données depuis les appareils clients, la connexion des points de distribution, la connexion des Serveurs d'administration secondaires).
- Si un objet d'automatisation de l'utilitaire klakaut n'est pas connecté au Serveur d'administration directement, mais par le point de distribution situé en zone démilitarisée.

Configuration du journal des événements de connexion au Serveur d'administration

L'historique des connexions et des tentatives de connexion au Serveur d'administration lors de son fonctionnement peut être enregistré dans un fichier journal. Les informations de ce fichier permettent de suivre non seulement les connexions à l'intérieur de votre infrastructure réseau, mais également les tentatives non autorisées d'accès au serveur.

Pour enregistrer les événements de connexion au Serveur d'administration, procédez comme suit :

1. Dans le menu principal, cliquez sur l'icône des paramètres ( ) en regard du nom du Serveur d'administration requis.

   La fenêtre des propriétés du Serveur d'administration s'ouvre.

2. Sous l'onglet **Général**, sélectionnez la section **Ports de connexion**.

3. Activez l'option **Consigner les événements de connexion du Serveur d'administration**.

Tous les autres événements de connexions entrantes vers le Serveur d'administration, résultats d'authentification et erreurs SSL seront enregistrés dans le fichier %ProgramData%\KasperskyLab\adminkit\logs\sc.syslog.

Configuration des paramètres d'accès Internet du Serveur d'administration

Vous devez configurer l'accès à Internet pour utiliser Kaspersky Security Network et télécharger les mises à jour des bases antivirus pour Kaspersky Security Center et les applications Kaspersky administrées.

Pour indiquer les paramètres d'accès Internet du Serveur d'administration :

1. Dans le menu principal, cliquez sur l'icône des paramètres ( ) à côté du nom du Serveur d'administration.

   La fenêtre des propriétés du Serveur d'administration s'ouvre.

2. Sous l'onglet **Général**, sélectionnez la section **Paramètres d'accès au réseau Internet**.

3. Activer l'option **Utiliser un serveur proxy** si vous souhaitez utiliser un serveur proxy pour vous connecter à Internet. Si cette option est activée, les champs de saisie des paramètres sont accessibles. Configurez les paramètres suivants de connexion au serveur proxy :

   - Adresse

     Adresse du serveur proxy pour la connexion de Kaspersky Security Center à Internet.

   - Numéro de port

     Numéro du port via lequel la connexion proxy à Kaspersky Security Center sera établie.

   - Ne pas utiliser le serveur proxy pour les adresses locales

     Le serveur proxy n'est pas utilisé lors de la connexion aux appareils dans le réseau local.

   - Authentification du serveur proxy

     Si la case est cochée, les champs de saisie permettent d'indiquer les identifiants pour l'authentification sur le serveur proxy.

     Ce champ de saisie est accessible si la case **Utiliser un serveur proxy** est cochée.

   - Nom d'utilisateur

     Compte utilisateur sous lequel la connexion au serveur proxy est établie (ce champ est disponible si la case **Authentification du serveur proxy** est cochée).

   - Mot de passe

     Mot de passe défini par l'utilisateur sous le compte duquel la connexion au serveur proxy est établie (ce champ est disponible si la case **Authentification du serveur proxy** est cochée).

     Pour voir le mot de passe saisi, cliquez sur le bouton **Afficher** et maintenez-le enfoncé aussi longtemps que vous en avez besoin.

Vous pouvez également configurer l'accès à Internet à l'aide de l'Assistant de configuration initiale de l'application.

Définition du nombre d'événements maximal dans le stockage d'événements

Dans la section **Stockage d'événements** de la fenêtre de propriétés du Serveur d'administration, vous pouvez configurer les paramètres de stockage des événements dans la base de données du Serveur d'administration en limitant le nombre d'enregistrements sur les événements et la durée de stockage de ces derniers. Quand vous définissez le nombre maximal d'événements, l'application calcule un espace de stockage approximatif requis pour la quantité indiquée. Ce calcul approximatif permet d'évaluer si vous avez assez d'espace libre sur le disque pour éviter un débordement de base de données. Par défaut, la capacité de la base de données du Serveur d'administration est de 400 000 événements. La capacité maximale recommandée de la base de données est de 45 millions d'événements.

L'application vérifie la base de données toutes les 10 minutes. Si le nombre d'événements atteint la valeur maximale indiquée plus 10 000, l'application supprime les événements les plus anciens de manière à ne conserver que le nombre maximal d'événements indiqué.

Quand le Serveur d'administration supprime les anciens événements, il ne peut pas enregistrer les nouveaux événements dans la base de données. Durant cette période, les informations relatives aux événements qui ont été rejetés sont écrites dans le journal des événements Kaspersky. Les nouveaux événements sont placés dans une file d'attente et enregistrés dans la base de données dès que la suppression est terminée.

Pour limiter le nombre d'événements qui peut être stocké dans la base d'événements du Serveur d'administration :

1. Dans le menu principal, cliquez sur l'icône paramètres ( ) en face du nom du Serveur d'administration requis.

   La fenêtre des propriétés du Serveur d'administration s'ouvre.

2. Sous l'onglet **Général**, sélectionnez la section **Stockage d'événements**. Définissez le nombre maximal d'événements stockés dans la base de données.

3. Cliquez sur le bouton **Enregistrer**.

Vous pouvez également réaliser les opérations suivantes :

- Modifiez les paramètres de n'importe quelle tâche pour enregistrer les événements liés à la progression de la tâche ou enregistrer uniquement les résultats de l'exécution de la tâche.

- Réduisez ou désactivez la période de stockage des événements des applications du Serveur d'administration, de l'Agent d'administration et des applications Kaspersky installées sur les appareils administrés.

Ainsi, vous diminuez le nombre d'événements dans la base de données, vous augmentez la vitesse de fonctionnement des scénarios liés à l'analyse du tableau des événements dans la base de données, et vous réduisez le risque que les événements critiques soient ignorés.

Paramètres de connexion des appareils protégés au niveau UEFI

Un *Appareil protégé au niveau UEFI* est un appareil avec une solution ou une application Kaspersky pour UEFI intégrée au niveau du BIOS. La protection intégrée assure la sécurité de l'appareil au début du lancement du système quand la protection des appareils qui ne sont pas dotés de l'application intégrée commence à fonctionner uniquement après le lancement de l'application de sécurité. Kaspersky Security Center prend en charge l'administration de ces appareils.

Pour modifier les paramètres de connexion des appareils protégés au niveau UEFI, procédez comme suit :

1. Dans le menu principal, cliquez sur l'icône des paramètres ( ) en regard du nom du Serveur d'administration requis.

   La fenêtre des propriétés du Serveur d'administration s'ouvre.

2. Sous l'onglet **Général**, sélectionnez la section **Ports supplémentaires**.

3. Modifiez les paramètres pertinents :

   - **Ouvrir le port pour les appareils protégés au niveau UEFI et KasperskyOS**

     Les appareils protégés au niveau UEFI peuvent se connecter au Serveur d'administration.

   - **Port pour les appareils protégés au niveau UEFI et KasperskyOS**

     Vous pouvez modifier le numéro de port si l'option **Ouvrir le port pour les appareils protégés au niveau UEFI et KasperskyOS** est activée. Le numéro de port par défaut est 13294.

4. Cliquez sur le bouton **Enregistrer**.

Les appareils protégés au niveau UEFI peuvent désormais se connecter au Serveur d'administration.

Création d'une hiérarchie des Serveurs d'administration : ajout d'un Serveur d'administration secondaire

Ajout du Serveur d'administration secondaire (effectué sur le futur Serveur d'administration principal)

Vous pouvez ajouter un Serveur d'administration en tant que Serveur d'administration secondaire et définir en même temps une relation hiérarchique de type "serveur principal/serveur secondaire".

Pour ajouter un Serveur d'administration secondaire disponible pour la connexion via Kaspersky Security Center Web Console :

1. Assurez-vous que le port 13000 du futur Serveur d'administration principal peut recevoir les connexions des Serveurs d'administration secondaires.

2. Sur le futur Serveur d'administration principal, cliquez sur l'icône paramètres ( ).

3. Sur la page des propriétés qui s'ouvre, sélectionnez sur l'onglet **Serveurs d'administration**.

4. Cochez la case en regard du nom du groupe d'administration auquel vous souhaitez ajouter le Serveur d'administration.

5. Sur la ligne de menu, cliquez sur **Connecter un Serveur d'administration secondaire**.

   L'Assistant d'ajout de Serveur d'administration secondaire démarre. Parcourez les étapes de l'assistant à l'aide du bouton **Suivant**.

6. Remplissez les champs suivants :

- **Connecter le Serveur d'administration principal au Serveur d'administration secondaire dans la DMZ**

  Sélectionnez cette option si le Serveur d'administration secondaire se trouve dans une zone démilitarisée (DMZ).

  Si cette option est sélectionnée, il faut renseigner le paramètre **Adresse du serveur secondaire**.

  Si cette option est sélectionnée, le Serveur d'administration primaire établit la connexion au Serveur d'administration secondaire. Sinon, le Serveur d'administration secondaire initie la connexion au Serveur d'administration primaire.

- **Nom d'affichage du Serveur d'administration secondaire**

  Le nom sous lequel le Serveur d'administration secondaire sera affiché dans la hiérarchie. Si vous le souhaitez, vous pouvez saisir l'adresse IP en tant que nom ou vous pouvez utiliser un nom comme, par exemple, " Serveur secondaire pour le groupe 1 ".

- **Adresse du Serveur d'administration secondaire (facultative)**

  Spécifiez l'adresse IP ou le nom de domaine du Serveur d'administration secondaire.

  Ce paramètre est obligatoire si l'option **Connecter le Serveur d'administration principal au Serveur d'administration secondaire dans la DMZ** est activée.

- **Port SSL du Serveur d'administration**

  Indiquez le numéro du port SSL sur le Serveur d'administration principal. Le numéro de port par défaut est 13000.

- **Port API du Serveur d'administration**

  Indiquez le numéro de port sur le Serveur d'administration principal de réception des connexions via OpenAPI. Le numéro de port par défaut est 13299.

7. Définissez le certificat pour le Serveur d'administration secondaire. Si vous avez spécifié le paramètre **Adresse du serveur secondaire**, vous pouvez cliquer sur le bouton **Obtenir depuis le Serveur d'administration secondaire** pour obtenir le certificat. Dans le cas contraire, cliquez sur le bouton **Rechercher le fichier de certificat** et localisez le fichier de certificat.

8. Spécifiez les paramètres de connexion :

   - Saisissez l'adresse du futur Serveur d'administration primaire.

   - Si le futur Serveur d'administration secondaire utilise un serveur proxy, saisissez l'adresse du serveur proxy et les informations d'identification de l'utilisateur pour se connecter au serveur proxy.

9. Saisissez les identifiants de l'utilisateur qui dispose des droits d'accès sur le futur Serveur d'administration secondaire.

10. Si la vérification en deux étapes est activée et configurée, renseignez le code de sécurité généré par l'application d'authentification.

    Si la vérification en deux étapes est activée, mais pas configurée pour ce compte, vous pouvez créer la hiérarchie à partir du futur Serveur secondaire (voir les instructions ci-dessous).

Si les paramètres de connexion sont corrects, la connexion avec le futur Serveur secondaire est établie et la hiérarchie " primaire/secondaire " est créée. En cas d'échec de la connexion, vérifiez les paramètres de connexion ou indiquez manuellement le certificat du futur Serveur secondaire.

La connexion entre les Serveurs d'administration primaire et secondaire est établie via le port 13000. Les tâches et les stratégies du Serveur d'administration principal sont reçues et appliquées. Le Serveur d'administration secondaire s'affiche sur le Serveur d'administration principal, dans le groupe d'administration auquel il a été ajouté.

Ajout du Serveur d'administration secondaire (effectué sur le futur Serveur d'administration secondaire)

Si vous n'avez pas pu vous connecter au futur Serveur d'administration secondaire (par exemple, parce qu'il était temporairement déconnecté ou indisponible), vous pouvez néanmoins ajouter un Serveur d'administration secondaire.

Pour ajouter un Serveur d'administration indisponible pour la connexion via Kaspersky Security Center Web Console, à titre de Serveur secondaire, procédez comme suit :

1. Envoyez le fichier du certificat du futur Serveur d'administration principal à l'administrateur système du bureau où se trouve le futur Serveur d'administration secondaire. (Vous pouvez, par exemple, copier le fichier sur un appareil externe tel qu'un disque flash ou l'envoyer par email.)

   Le fichier du certificat se trouve sur le futur Serveur d'administration principal à l'adresse %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert\klserver.cer.

2. Demandez à l'administrateur système en charge du futur Serveur d'administration secondaire de procéder comme suit :

   a. Cliquez sur l'icône des Paramètres ( ).

   b. Sur la page des propriétés qui s'ouvre, accédez à la section **Hiérarchie des Serveurs d'administration** de l'onglet **Général**.

   c. Cochez l'option **Ce Serveur d'administration est secondaire dans la hiérarchie**.

   d. Dans le champ **Adresse du Serveur d'administration principal**, saisissez le nom de réseau du futur Serveur d'administration principal.

   e. Choisissez le fichier précédemment enregistré contenant le certificat du futur Serveur d'administration principal en cliquant sur **Parcourir**.

   f. Si nécessaire, cochez la case **Connecter le Serveur d'administration principal au Serveur d'administration secondaire dans la DMZ**.

   g. Si la connexion au futur Serveur d'administration secondaire se fait via un serveur proxy, sélectionnez l'option **Utiliser un serveur proxy** et précisez les paramètres de connexion.

   h. Cliquez sur **Enregistrer**.

La hiérarchie " principal/secondaire " est établie. Le Serveur d'administration principal commence à accepter la connexion du Serveur d'administration secondaire à l'aide du port 13000. Les tâches et les stratégies du Serveur d'administration principal sont reçues et appliquées. Le Serveur d'administration secondaire s'affiche sur le Serveur d'administration principal, dans le groupe d'administration où il a été ajouté.

Affichage de la liste des Serveurs d'administration secondaires

Pour afficher la liste des Serveurs d'administration secondaires (virtuels inclus) :

Dans le menu principal, cliquez sur le nom du Serveur d'administration, qui est à côté de l'icône des paramètres ( ).

La liste déroulante des Serveurs d'administration secondaires (virtuels inclus) s'affiche.

Vous pouvez aller à l'un de ces serveur d'administration en cliquant sur son nom.

The administration groups are shown, too, but they are grayed and not available for management in this menu.

Si vous êtes connecté à votre Serveur d'administration primaire dans Kaspersky Security Center Web Console et que vous ne pouvez pas vous connecter à un Serveur d'administration virtuel administré par un Serveur d'administration secondaire, vous pouvez utiliser l'une des manières suivantes :

- **Modifiez l'installation existante de Kaspersky Security Center Web Console pour ajouter le Serveur secondaire à la liste des Serveurs d'administration de confiance**. Ensuite, vous pourrez vous connecter au Serveur d'administration virtuel dans Kaspersky Security Center Web Console.

  1. Sur l'appareil où Kaspersky Security Center Web Console est installé, exécutez le fichier d'installation ksc-web-console-<version number>.<build number>.exe depuis un compte doté de privilèges d'administrateur.

     L'Assistant d'installation démarre. Naviguez dans les fenêtres de l'Assistant à l'aide du bouton **Suivant**.

  2. Sélectionnez l'option **Mettre à niveau**.

  3. À l'étape **Type de modification**, sélectionnez l'option **Modifier les paramètres de connexion**.

  4. À l'étape **Serveurs d'administration de confiance**, ajoutez le Serveur d'administration secondaire requis.

  5. À la dernière étape, cliquez sur **Modifier** pour appliquer les nouveaux paramètres.

  6. Une fois la reconfiguration de l'application terminée, cliquez sur le bouton **Terminer**.

- Utilisez Kaspersky Security Center Web Console pour vous connecter directement au Serveur d'administration secondaire sur lequel le Serveur virtuel a été créé. Ensuite, vous pourrez passer au Serveur d'administration virtuel dans Kaspersky Security Center Web Console.

- Utilisez la Console d'administration MMC pour vous connecter directement au Serveur virtuel.

Suppression d'une hiérarchie des Serveurs d'administration

Si vous ne souhaitez plus disposer d'une hiérarchie de Serveurs d'administration, vous pouvez les déconnecter de cette hiérarchie.

Pour supprimer une hiérarchie de Serveurs d'administration :

1. Dans le menu principal, cliquez sur l'icône des paramètres ( ) en regard du nom du Serveur d'administration principal.

2. Sur la page qui s'ouvre, accédez à l'onglet **Serveurs d'administration**.

3. Dans le groupe d'administration où vous voulez supprimer le Serveur d'administration secondaire, sélectionnez le Serveur d'administration secondaire.

4. Dans la ligne du menu, cliquez sur **Supprimer**.

5. Dans la fenêtre qui s'ouvre, cliquez sur **OK** pour confirmer que vous voulez supprimer le Serveur d'administration secondaire.

L'ancien Serveur d'administration principal et l'ancien Serveur d'administration secondaire sont désormais indépendants l'un de l'autre. La hiérarchie n'existe plus.

Maintenance du Serveur d'administration

La maintenance du Serveur d'administration permet de libérer de l'espace dans le dossier du Serveur d'administration et de réduire le volume de la base de données en supprimant des objets qui ne sont plus nécessaires. Cette mesure vous permet d'améliorer les performances et la fiabilité de fonctionnement de l'application. Il est recommandé de procéder à la maintenance du Serveur d'administration au moins une fois par semaine.

La maintenance du Serveur d'administration s'effectue à l'aide de la tâche correspondante. Pendant la maintenance du Serveur d'administration, l'application exécute les opérations suivantes :

- Supprime les dossiers et les fichiers inutiles du dossier de stockage.
- Supprime les enregistrements inutiles des tableaux (également appelés " dangling pointers ", ou " pointeurs pendouillants ").
- Purge le cache.
- Maintient la base de données (si vous utilisez le serveur SQL ou PostgreSQL comme SGBD) :
  - Elle recherche les erreurs dans la base de données (disponible uniquement pour le serveur SQL).
  - Elle réorganise les indices de la base de données.
  - Elle met à jour les statistiques de la base de données.
  - Elle comprime la base de données (si nécessaire).

La tâche Maintenance du Serveur d'administration est créée automatiquement lors de l'installation de Kaspersky Security Center. Si la tâche Maintenance du Serveur d'administration est supprimée, vous pouvez la créer manuellement.

Pour créer la tâche Maintenance du Serveur d'administration, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Tâches**.
2. Cliquez sur le bouton **Ajouter**.

   Ceci permet de lancer l'Assistant de création d'une tâche.
3. Dans la fenêtre de l'Assistant **Paramètres de nouvelle tâche**, sélectionnez **Maintenance du Serveur d'administration** en tant que type de tâche et cliquez sur le bouton **Suivant**.
4. Suivez les étapes ultérieures de l'assistant.

La tâche qui vient d'être créée s'affiche dans la liste des tâches. Une seule tâche Maintenance du Serveur d'administration peut être exécutée pour un même Serveur d'administration. Si une tâche Maintenance du Serveur d'administration pour un Serveur d'administration est déjà créée, aucune nouvelle tâche Maintenance du Serveur d'administration ne peut être créée.

Configuration de l'interface

Vous pouvez configurer l'interface de Kaspersky Security Center Web Console pour afficher et masquer les sections et les éléments d'interface, en fonction des fonctionnalités utilisées.

Pour configurer l'interface de Kaspersky Security Center Web Console conformément à l'ensemble de fonctionnalités actuellement utilisé, procédez comme suit :

1. Dans le menu principal, allez dans les paramètres de votre compte et sélectionnez **Options d'interface**.
2. Dans la fenêtre **Options d'interface** qui s'ouvre, activez ou désactivez les options requises.
3. Cliquez sur **Enregistrer**.

Ensuite, la console affiche les sections du menu principal en fonction des options activées. Par exemple, si vous activez **Afficher les alertes EDR**, la section **Surveillance et rapports** → **Alerte** s'affiche dans le menu principal.

Administration des Serveurs d'administration virtuels

Cette section décrit les actions suivantes pour administrer les Serveurs d'administration virtuels :

- Créer des Serveurs d'administration virtuels
- Activer et désactiver les Serveurs d'administration virtuels
- Désigner un administrateur pour un Serveur d'administration virtuel
- Modifier le Serveur d'administration pour les appareils clients
- Supprimer les Serveurs d'administration virtuels

Création d'un Serveur d'administration virtuel

Vous pouvez créer des Serveurs d'administration virtuels et les ajouter aux groupes d'administration.

Lorsque vous créez un Serveur d'administration virtuel, il hérite de la liste des utilisateurs et de tous les droits d'utilisateur du Serveur d'administration principal. Si un utilisateur dispose de droits d'accès au Serveur primaire, cet utilisateur dispose également de droits d'accès au Serveur virtuel. Après la création, vous configurez indépendamment les droits d'accès aux Serveurs.

Pour créer et ajouter un Serveur d'administration virtuel, procédez comme suit :

1. Dans le menu principal, cliquez sur l'icône des paramètres ( ) en regard du nom du Serveur d'administration requis.
2. Sur la page qui s'ouvre, accédez à l'onglet **Serveurs d'administration**.

3. Choisissez le groupe d'administration auquel vous souhaitez ajouter un Serveur d'administration virtuel. Le Serveur d'administration virtuel va administrer les appareils du groupe sélectionné (y compris les sous-groupes).

4. Dans la ligne du menu, cliquez sur **Nouveau Serveur d'administration virtuel**.

5. Sur la page qui s'ouvre, définissez les propriétés du nouveau Serveur d'administration virtuel :

   - **Nom du Serveur d'administration virtuel**.
   - **Adresse de connexion du Serveur d'administration**

     Vous pouvez définir le nom ou l'adresse IP de votre Serveur d'administration.

6. Dans la liste des utilisateurs, sélectionnez l'administrateur virtuel du Serveur d'administration. Si vous le souhaitez vous pouvez modifier l'un des comptes existants afin de lui attribuer le rôle de l'administrateur ou de créer un nouveau compte utilisateur.

7. Cliquez sur **Enregistrer**.

Le nouveau Serveur d'administration virtuel est créé, ajouté au groupe d'administration et s'affiche sous l'onglet **Serveurs d'administration**.

Si vous êtes connecté à votre Serveur d'administration primaire dans Kaspersky Security Center Web Console et que vous ne pouvez pas vous connecter à un Serveur d'administration virtuel administré par un Serveur d'administration secondaire, vous pouvez utiliser l'une des manières suivantes :

- Modifiez l'installation existante de Kaspersky Security Center Web Console pour ajouter le Serveur secondaire à la liste des Serveurs d'administration de confiance. Ensuite, vous pourrez vous connecter au Serveur d'administration virtuel dans Kaspersky Security Center Web Console.

  1. Sur l'appareil où Kaspersky Security Center Web Console est installé, exécutez le fichier d'installation ksc-web-console-<version number>.<build number>.exe depuis un compte doté de privilèges d'administrateur.

     L'Assistant d'installation démarre. Naviguez dans les fenêtres de l'Assistant à l'aide du bouton **Suivant**.

  2. Sélectionnez l'option **Mettre à niveau**.

  3. À l'étape **Type de modification**, sélectionnez l'option **Modifier les paramètres de connexion**.

  4. À l'étape **Serveurs d'administration de confiance**, ajoutez le Serveur d'administration secondaire requis.

  5. À la dernière étape, cliquez sur **Modifier** pour appliquer les nouveaux paramètres.

  6. Une fois la reconfiguration de l'application terminée, cliquez sur le bouton **Terminer**.

- Utilisez Kaspersky Security Center Web Console pour vous connecter directement au Serveur d'administration secondaire sur lequel le Serveur virtuel a été créé. Ensuite, vous pourrez passer au Serveur d'administration virtuel dans Kaspersky Security Center Web Console.

- Utilisez la Console d'administration MMC pour vous connecter directement au Serveur virtuel.

Activation et désactivation d'un Serveur d'administration virtuel

Lorsque vous créez un nouveau Serveur d'administration virtuel, il est activé par défaut. Vous pouvez le désactiver ou le réactiver à tout moment. Désactiver ou activer un Serveur d'administration virtuel revient à éteindre ou allumer un Serveur d'administration physique.

Pour activer ou désactiver un Serveur d'administration virtuel :

1. Dans le menu principal, cliquez sur l'icône des paramètres ( ) en regard du nom du Serveur d'administration requis.
2. Sur la page qui s'ouvre, accédez à l'onglet **Serveurs d'administration**.
3. Sélectionnez le Serveur d'administration virtuel que vous souhaitez activer ou désactiver.
4. Sur la ligne du menu, cliquez sur le bouton **Activer / désactiver le Serveur d'administration virtuel**.

L'état du Serveur d'administration virtuel passe à activé ou désactivé en fonction de son état précédent. L'état mis à jour est affiché à côté du nom du Serveur d'administration.

Désignation d'un administrateur pour un Serveur d'administration virtuel

Lorsque vous utilisez des Serveurs d'administration virtuels dans votre organisation, vous souhaiterez peut-être désigner un administrateur dédié pour chaque Serveur d'administration virtuel. Par exemple, cela peut être utile lorsque vous créez des Serveurs d'administration virtuels pour administrer des bureaux ou des services distincts de votre organisation, ou si vous êtes un fournisseur MSP et que vous administrez vos clients via des Serveurs d'administration virtuels.

Lorsque vous créez un Serveur d'administration virtuel, il hérite de la liste des utilisateurs et de tous les droits d'utilisateur du Serveur d'administration principal. Si un utilisateur dispose de droits d'accès au Serveur primaire, cet utilisateur dispose également de droits d'accès au Serveur virtuel. Après la création, vous configurez indépendamment les droits d'accès aux Serveurs. Si vous souhaitez désigner un administrateur pour un Serveur d'administration virtuel uniquement, assurez-vous que l'administrateur ne dispose pas de droits d'accès sur le Serveur d'administration primaire.

Vous désignez un administrateur pour un Serveur d'administration virtuel en accordant les droits d'accès d'administrateur au Serveur d'administration virtuel. Vous pouvez accorder les droits d'accès requis de l'une des manières suivantes :

- Configurer manuellement les droits d'accès de l'administrateur
- Attribuer un ou plusieurs rôles d'utilisateur à l'administrateur

Pour se connecter à Kaspersky Security Center Web Console, l'administrateur du Serveur d'administration virtuel renseigne le nom du Serveur d'administration virtuel, le nom d'utilisateur et le mot de passe. Kaspersky Security Center Web Console authentifie l'administrateur et ouvre le Serveur d'administration virtuel pour lequel l'administrateur a des droits d'accès. L'administrateur ne peut pas basculer entre les Serveurs d'administration.

Prérequis

Avant de commencer, assurez-vous que les conditions suivantes sont remplies :

- Le Serveur d'administration virtuel est créé.
- Sur le Serveur d'administration primaire, vous avez créé un compte utilisateur pour l'administrateur que vous souhaitez affecter au Serveur d'administration virtuel.
- Vous disposez du droit **Modifier les ACL d'objet** dans la zone fonctionnelle **Fonctions générales → Autorisations utilisateur**.

Configuration manuelle des droits d'accès

Pour désigner un administrateur pour un Serveur d'administration virtuel, procédez comme suit :

1. Dans le menu principal, basculez vers le Serveur d'administration virtuel requis :
   a. Cliquez sur l'icône en forme de chevron (›) à droite du nom actuel du Serveur d'administration.
   b. Sélectionnez le Serveur d'administration requis.
2. Dans le menu principal, cliquez sur l'icône des paramètres (⚙) à côté du nom du Serveur d'administration.
   La fenêtre des propriétés du Serveur d'administration s'ouvre.
3. Sous l'onglet **Privilèges d'accès**, cliquez sur le bouton **Ajouter**.
   Une liste unifiée des utilisateurs du Serveur d'administration principal et du Serveur d'administration virtuel actuel s'ouvre.
4. Dans la liste des utilisateurs, sélectionnez le compte utilisateur de l'administrateur que vous souhaitez affecter au Serveur d'administration virtuel, puis cliquez sur le bouton **OK**.
   L'application ajoute l'utilisateur sélectionné à la liste des utilisateurs sous l'onglet **Privilèges d'accès**.
5. Cochez la case en regard du nom du compte ajouté, puis cliquez sur le bouton **Privilèges d'accès**.
6. Configurez les privilèges de l'administrateur sur le Serveur d'administration virtuel.
   Pour que l'authentification réussisse, l'administrateur doit disposer au minimum des privilèges suivants :
   - Accorde les droits de **Lire** dans la zone fonctionnelle **Fonctions générales → Fonctionnalité de base**
   - Droits de **Lire** dans la zone fonctionnelle **Fonctions générales → Serveurs d'administration virtuels**

L'application enregistre les droits d'utilisateur modifiés dans le compte administrateur.

Configuration des droits d'accès par l'attribution des rôles d'utilisateur

Vous pouvez également accorder les droits d'accès à un administrateur de Serveur d'administration virtuel via les rôles d'utilisateur. Par exemple, cela peut être utile si vous souhaitez désigner plusieurs administrateurs sur le même Serveur d'administration virtuel. Si tel est le cas, vous pouvez attribuer un ou même plusieurs rôles d'utilisateur aux comptes d'administrateurs au lieu de configurer les mêmes droits d'utilisateur pour plusieurs administrateurs.

Pour désigner un administrateur pour un Serveur d'administration virtuel en attribuant des rôles d'utilisateur, procédez comme suit :

1. Sur le Serveur d'administration principal, créez un rôle d'utilisateur, puis indiquez tous les droits d'accès requis dont un administrateur doit disposer sur le Serveur d'administration virtuel. Vous pouvez créer plusieurs rôles, par exemple, si vous souhaitez séparer l'accès à différents domaines fonctionnels.

2. Dans le menu principal, basculez vers le Serveur d'administration virtuel requis :

   a. Cliquez sur l'icône en forme de chevron (›) à droite du nom actuel du Serveur d'administration.

   b. Sélectionnez le Serveur d'administration requis.

3. Attribuez le nouveau rôle ou plusieurs rôles au compte administrateur.

L'application attribue les nouveaux rôles au compte administrateur.

Configuration des droits d'accès au niveau de l'objet

Outre l'attribution de droits d'accès au niveau du domaine fonctionnel, vous pouvez configurer l'accès à des objets spécifique s sur le Serveur d'administration virtuel, par exemple, à un groupe d'administration ou à une tâche spécifique. Pour ce faire, basculez sur le Serveur d'administration virtuel, puis configurez les droits d'accès dans les propriétés de l'objet.

Modification du Serveur d'administration pour les appareils clients

Vous pouvez modifier le Serveur d'administration, sous lequel les appareils clients se trouvent, par un autre Serveur à l'aide de la tâche *Modification du Serveur d'administration*. Une fois la tâche terminée, les appareils client sélectionnés seront placés sous l'administration du serveur d'administration que vous spécifiez.

> Vous ne pouvez pas utiliser la tâche *Modification du Serveur d'administration* pour les appareils clients connectés au Serveur d'administration via des passerelles de connexion. Pour de tels appareils, vous devez soit reconfigurer l'Agent d'administration, soit réinstaller l'Agent d'administration et indiquer la passerelle de connexion.

Pour modifier le Serveur d'administration, sous lequel les appareils clients se trouvent, par un autre Serveur, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Tâches**.

2. Cliquez sur **Ajouter**.

   Ceci permet de lancer l'assistant de création d'une tâche. Parcourez les étapes de l'assistant à l'aide du bouton **Suivant**.

3. À l'étape **Paramètres de nouvelle tâche** de l'assistant, spécifiez les paramètres suivants :

   a. Dans la liste déroulante **Application**, sélectionnez **Kaspersky Security Center**.

   b. Dans le champ **Type de tâche**, sélectionnez **Modification du Serveur d'administration**.

   c. Dans le champ **Nom de la tâche**, renseignez le nom de la tâche que vous créez.

   Le nom de la tâche ne peut pas contenir plus de 100 symboles et contenir de symboles spéciaux ("*<>?\:|).

   d. Sélectionnez les appareils auxquels les tâches seront affectées :

   - **Attribuer la tâche à un groupe d'administration**

     La tâche est affectée aux appareils qui appartiennent à un groupe d'administration. Vous pouvez renseigner un des groupes existants ou en créer un.

     Par exemple, vous pourriez souhaiter utiliser cette option pour exécuter une tâche d'envoi de messages pour les utilisateurs si le message est particulier pour les appareils repris dans un groupe d'administration spécifique.

     Si une tâche est attribuée à un groupe d'administration, l'onglet **Sécurité** ne s'affiche pas dans la fenêtre des propriétés de la tâche, car les tâches de groupe sont soumises aux paramètres de sécurité des groupes auxquels elles s'appliquent.

   - **Définir les adresses des appareils manuellement ou les importer à partir d'une liste**

     Vous pouvez définir les noms NetBIOS, les noms DNS, les adresses IP, ainsi que les plages d'adresses IP auxquels il convient d'affecter la tâche.

     Vous pourriez utiliser cette option pour exécuter une tâche pour un sous-réseau défini. Par exemple, vous pourriez souhaiter installer une certaine application sur les appareils des comptables ou analyser des appareils dans un sous-réseau qui est probablement infecté.

   - **Attribuer la tâche à une sélection d'appareils**

     La tâche est affectée aux appareils qui appartiennent à une sélection d'appareils. Vous pouvez définir une des sélections existantes.

     Par exemple, vous pourriez souhaiter utiliser cette option pour exécuter une tâche sur des appareils dotés d'une version du système d'exploitation spécifique.

4. À l'étape **Zone de la tâche** de l'assistant, indiquez un groupe d'administration, des appareils avec des adresses spécifiques ou une sélection d'appareils.

5. À cette étape de l'assistant, confirmez que vous acceptez les conditions de modification du Serveur d'administration pour les appareils clients.

6. À cette étape de l'assistant, sélectionnez le Serveur d'administration que vous souhaitez utiliser pour administrer les appareils sélectionnés :

- **Passer à un autre Serveur d'administration principal**

  Pour déplacer les appareils clients vers un autre Serveur d'administration principal, spécifiez les paramètres de connexion au Serveur d'administration suivants :

  1. Dans le champ **Adresse du Serveur d'administration**, spécifiez l'adresse du nouveau Serveur d'administration principal.
  2. Dans le champ **Numéro de port**, spécifiez le numéro de port utilisé pour se connecter au Serveur d'administration.

     Le numéro du port par défaut est 14000.
  3. Dans le champ, **Port SSL**, indiquez le numéro du port SSL sur le Serveur d'administration principal.

     Le numéro du port par défaut est 13000.
  4. Si nécessaire, activez l'option **Utiliser un serveur proxy**.

     Si l'option est désactivée, la connexion directe est utilisée pour connecter l'appareil au Serveur d'administration.

     Si cette option est activée, définissez les paramètres du serveur proxy :

     - **Adresse du serveur proxy**
     - **Port du serveur proxy**

     Si votre serveur proxy nécessite une authentification, dans les champs **Nom d'utilisateur** et **Mot de passe**, indiquez les identifiants du compte sous lequel la connexion au serveur proxy est établie. Nous vous recommandons de spécifier les informations d'identification d'un compte disposant des privilèges minimaux requis uniquement pour l'authentification sur le serveur proxy.
  5. Si nécessaire, téléchargez un nouveau certificat de Serveur d'administration.

- **Passer à un autre Serveur virtuel sur ce Serveur principal**

  Sélectionnez cette option pour déplacer les appareils clients vers le Serveur d'administration virtuel sur le Serveur d'administration principal actuel. Pour ce faire, dans la liste déroulante **Nom du Serveur d'administration virtuel**, sélectionnez le Serveur d'administration virtuel nécessaire.

7. À l'étape **Sélection du compte utilisateur pour exécuter la tâche** de l'assistant, indiquez les paramètres du compte :

   - **Compte par défaut**

     La tâche sera lancée sous le même compte utilisateur sous lequel l'application, exécutant cette tâche, a été installée et lancée.

     Cette option est sélectionnée par défaut.

   - **Indiquer un compte**

     Remplissez les champs **Compte utilisateur** et **Mot de passe** pour définir les détails d'un compte à partir duquel la tâche est exécutée. Le compte doit disposer de droits suffisants pour cette tâche.

     - **Compte utilisateur**

       Le compte utilisateur au nom duquel la tâche sera lancée.

     - **Mot de passe**

       Mot de passe du compte utilisateur au nom duquel la tâche sera lancée.

8. Si vous souhaitez modifier les paramètres de tâche par défaut, à l'étape **Fin de la création de la tâche** de l'assistant, activez l'option **Ouvrir les détails de la tâche à la fin de la création**.

   Si vous n'activez pas cette tâche, la tâche est créée selon les paramètres par défaut. Vous pourrez modifier ces paramètres par défaut plus tard, à tout moment.

9. Cliquez sur le bouton **Terminer**.

   La tâche est créée et s'affiche dans la liste des tâches.

10. Cliquez sur le nom de la tâche créée pour ouvrir la fenêtre de propriétés de la tâche.

11. Si vous souhaitez modifier les paramètres de tâche par défaut, dans la fenêtre des propriétés de la tâche, indiquez les paramètres généraux de la tâche en fonction de vos besoins.

12. Cliquez sur le bouton **Enregistrer**.

    La tâche est créée et configurée.

13. Lancez la tâche créée.

Après la fin de la tâche, les appareils clients, pour lesquels elle a été créée, passent sous l'administration du Serveur d'administration indiqué dans les paramètres de la tâche.

Suppression d'un Serveur d'administration virtuel

Lorsque vous supprimez un Serveur d'administration virtuel, tous les objets créés sur le Serveur d'administration, y compris les stratégies et les tâches, seront également supprimés. Les appareils administrés des groupes d'administration qui étaient administrés par le Serveur d'administration virtuel seront supprimés des groupes d'administration. Pour renvoyer les appareils administrés par Kaspersky Security Center, exécutez l'interrogation du réseau, puis déplacez les appareils trouvés du groupe Appareils non attribués vers les groupes d'administration.

Pour supprimer un Serveur d'administration virtuel :

1. Dans le menu principal, cliquez sur l'icône des paramètres ( ) à côté du nom du Serveur d'administration.
2. Sur la page qui s'ouvre, accédez à l'onglet **Serveurs d'administration**.
3. Sélectionnez le Serveur d'administration virtuel que vous souhaitez supprimer.
4. Dans la ligne du menu, cliquez sur le bouton **Supprimer**.

Le Serveur d'administration virtuel est supprimé.

Activation de la protection du compte contre les modifications non autorisées

Vous pouvez activer une option supplémentaire pour protéger un compte utilisateur contre les modifications non autorisées. Si cette option est activée, la modification des paramètres du compte utilisateur nécessite l'autorisation de l'utilisateur disposant des droits de modification.

Pour activer ou désactiver la protection du compte contre les modifications non autorisées, procédez comme suit :

1. Dans le menu principal, accédez à **Utilisateurs et rôles** → **Utilisateurs**.
2. Cliquez sur le nom du compte utilisateur interne pour lequel vous souhaitez spécifier la protection du compte contre les modifications non autorisées.
3. Dans la fenêtre des paramètres utilisateur qui s'ouvre, sélectionnez l'onglet **Protection du compte**.
4. Sous l'onglet **Protection du compte**, sélectionnez l'option **Demander une authentification pour vérifier l'autorisation de modifier les comptes utilisateurs** si vous souhaitez demander les identifiants à chaque fois que les paramètres de compte sont changés ou modifiés. Dans le cas contraire, sélectionnez l'option **Autoriser les utilisateurs à modifier ce compte sans authentification supplémentaire**.
5. Cliquez sur **Enregistrer**.

La protection du compte contre les modifications non autorisées est activée pour un compte utilisateur.

Copie de sauvegarde et restauration des données du Serveur d'administration

La copie de sauvegarde des données permet de déplacer le Serveur d'administration d'un appareil à un autre sans perte d'informations. Grâce à la sauvegarde, vous pouvez restaurer les données lorsque vous déplacez la base de données du Serveur d'administration vers un autre appareil, ou lors de la mise à niveau vers une version plus récente de Kaspersky Security Center. Vous pouvez également utiliser la sauvegarde des données pour déplacer les données du Serveur d'administration de Kaspersky Security Center Windows sous la gestion de Kaspersky Security Center Linux (le déplacement des données de Kaspersky Security Center Windows n'est pas pris en charge).

Notez que les plug-ins d'administration installés ne sont pas sauvegardés. Après avoir restauré les données du Serveur d'administration à partir d'une copie de sauvegarde, vous devez télécharger et réinstaller les plug-ins pour les applications administrées.

Avant de sauvegarder les données du Serveur d'administration, vérifiez si un Serveur d'administration virtuel est ajouté au groupe d'administration. Si un Serveur d'administration virtuel est ajouté, assurez-vous qu'un administrateur est affecté à ce Serveur d'administration virtuel avant la sauvegarde. Vous ne pouvez pas accorder à l'administrateur des droits d'accès au Serveur d'administration virtuel après la sauvegarde. Notez que si les informations d'identification du compte administrateur sont perdues, vous ne pourrez pas attribuer un nouvel administrateur au serveur d'administrateur virtuel.

Pour sauvegarder ou restaurer un cluster de basculement de Kaspersky Security Center, vous devez interrompre le cluster dans son ensemble à des fins de maintenance, puis le redémarrer une fois la sauvegarde ou la restauration terminée.

Vous pouvez créer une copie de sauvegarde des données du Serveur d'administration à l'aide d'une des options suivantes :

- Créer et lancer la tâche de copie de sauvegarde des données via la Console d'administration.
- Lancez l'utilitaire klbackup sur l'appareil où le Serveur d'administration est installé. Cet utilitaire figure dans le kit de distribution de Kaspersky Security Center. Après l'installation du Serveur d'administration, l'utilitaire se trouve dans la racine du dossier de destination indiqué lors de l'installation de l'application.

La copie de sauvegarde des données du Serveur d'administration enregistre les données suivantes :

- Base de données du Serveur d'administration (stratégies, tâches, paramètres des applications, événements enregistrés sur le Serveur d'administration).
- Les données de configuration de la structure du groupe d'administration et des appareils clients.
- Le stockage des distributifs des applications pour l'installation à distance.
- Le certificat du Serveur d'administration.
- Contenu du dossier *Mises à jour*.

  Par défaut, le chemin du dossier est C:\ProgramData\KasperskyLab\adminkit\1093\.working\share\Updates\

La restauration des données du Serveur d'administration est possible uniquement à l'aide de l'utilitaire klbackup. Vous devez effectuer la restauration sur une instance opérationnelle du Serveur d'administration qui vient d'être installée et dont la version est identique à la version du Serveur pour lequel la copie de sauvegarde avait été créée (ou plus récente).

Création d'une tâche de copie de sauvegarde des données

Les tâches de la copie de sauvegarde sont des tâches du Serveur d'administration et elles sont créées par l'Assistant de configuration initiale de l'application. Si la tâche de copie de sauvegarde, créée par l'Assistant de configuration initiale de l'application, a été supprimée, vous pouvez la créer manuellement.

Pour créer une tâche de copie de sauvegarde des données du Serveur d'administration, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Tâches**.
2. Cliquez sur le bouton **Ajouter**.

   Ceci permet de lancer l'Assistant de création d'une tâche.
3. Dans la fenêtre de l'Assistant **Paramètres de nouvelle tâche**, sélectionnez le type de tâche **Sauvegarde des données du Serveur d'administration**.
4. Suivez les étapes ultérieures de l'assistant.

La tâche **Sauvegarde des données du Serveur d'administration** peut être créée dans un seul exemplaire. Si la tâche de sauvegarde des données du Serveur d'administration a déjà été créée pour le Serveur d'administration, alors elle ne s'affiche pas dans la fenêtre de sélection du type de tâche de l'Assistant de création de la tâche de copie de sauvegarde du Serveur d'administration.

Pour configurer la tâche Sauvegarde des données du Serveur d'administration, procédez comme suit :

1. Dans le menu principal, sélectionnez **Ressources (Appareils)** → **Tâches**, puis sélectionnez la tâche **Sauvegarde des données du Serveur d'administration**.
2. Cliquez sur la tâche **Sauvegarde des données du Serveur d'administration**.

   La fenêtre de propriétés de la tâche s'affiche.

3. Le cas échéant, définissez les paramètres généraux de la tâche en fonction de vos besoins.

4. Dans la section **Paramètres de l'application**, indiquez le chemin d'accès au dossier de stockage des copies de sauvegarde des données du Serveur d'administration, définissez le mot de passe de la protection des copies de sauvegarde et, si nécessaire, le nombre de copies de sauvegarde.

5. Cliquez sur **Enregistrer** pour appliquer les modifications.

La tâche *Sauvegarde des données du Serveur d'administration* est configurée.

Déplacement du Serveur d'administration sur un autre appareil

Si vous devez utiliser le Serveur d'administration sur un nouvel appareil, vous pouvez le déplacer de l'une des manières suivantes :

- Déplacez le Serveur d'administration et le serveur de base de données vers un nouvel appareil (le serveur de base de données peut être installé sur le nouvel appareil avec le Serveur d'administration ou sur un autre appareil).

- Conservez le serveur de base de données sur l'appareil précédent et déplacez uniquement le Serveur d'administration sur un nouvel appareil.

Pour déplacer le Serveur d'administration et le serveur de base de données vers un nouvel appareil, procédez comme suit :

1. Sur l'appareil précédent, créez une sauvegarde des données du Serveur d'administration.

   Pour ce faire, vous pouvez exécuter la tâche de sauvegarde des données via Kaspersky Security Center Web Console ou exécuter l'utilitaire klbackup.

   Si vous utilisez actuellement SQL Server comme SGBD pour le Serveur d'administration, vous pouvez migrer les données de SQL Server vers le SGBD MySQL ou MariaDB. Pour ce faire, exécutez l' utilitaire klbackup en mode interactif pour créer une sauvegarde des données. Activez l'option **Migrer au format MySQL/MariaDB** dans la fenêtre **Paramètres de sauvegarde** de l'Assistant de sauvegarde et de restauration des données. Kaspersky Security Center créera une sauvegarde compatible avec MySQL et MariaDB. Après cela, vous pouvez restaurer les données de la sauvegarde dans MySQL ou MariaDB.

   Vous pouvez également activer l'option **Migrer au format Azure** si vous souhaitez migrer les données depuis le SGBD SQL Server vers le SGBD SQL Azure.

2. Sur l'ancien appareil, déconnectez le Serveur d'administration du réseau.

3. Sélectionnez un nouvel appareil sur lequel installer le Serveur d'administration. Assurez-vous que le matériel et les logiciels de l'appareil sélectionné répondent à la configuration requise pour le Serveur d'administration, Kaspersky Security Center Web Console et l'Agent d'administration. Vérifiez également que les ports utilisés sur le Serveur d'administration sont disponibles.

4. Attribuez la même adresse au nouvel appareil.

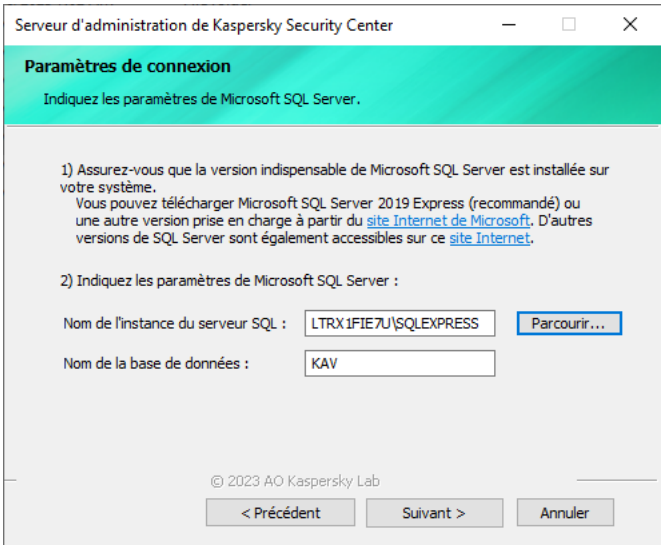
   Le nouveau Serveur d'administration peut recevoir le nom NetBIOS, le FQDN et l'adresse IP statique. Cela dépend de l'adresse du Serveur d'administration qui a été définie dans le paquet d'installation de l'Agent d'administration lors du déploiement des Agents d'administration. Vous pouvez également utiliser l'adresse de connexion qui détermine le Serveur d'administration auquel l'Agent d'administration se connecte (vous pouvez obtenir cette adresse sur les appareils administrés à l'aide de l'utilitaire klnagchk).

5. Sur le nouvel appareil, installez le système d'administration de base de données (SGBD) que le Serveur d'administration utilisera.

   La base de données peut être installée sur le nouvel appareil avec le Serveur d'administration ou sur un autre appareil. Assurez-vous que cet appareil répond aux exigences matérielles et logicielles. Lorsque vous sélectionnez un SGBD, tenez compte du nombre d'appareils couverts par le Serveur d'administration.

6. Lancez l'installation du Serveur d'administration sur le nouvel appareil.

7. Lors de l'installation du Serveur d'administration, configurez les paramètres de connexion au serveur de base de données.



Exemple de la fenêtre Paramètres de connexion pour Microsoft SQL Server

Selon l'emplacement du serveur de base de données, exécutez l'une des actions suivantes :

- Conserver le serveur de base de données sur l'appareil précédent

  1. Cliquez sur le bouton **Parcourir** en regard du champ **Nom de l'instance du serveur SQL**, puis sélectionnez le nom de l'appareil précédent dans la liste qui s'affiche.

     Notez que l'appareil précédent doit être disponible pour la connexion avec le nouveau Serveur d'administration.

  2. Saisissez le nom de la base de données précédente dans le champ **Nom de la base de données** de données.

- Déplacer le serveur de base de données vers un autre appareil

  1. Cliquez sur le bouton **Parcourir** en regard du champ **Nom de l'instance du serveur SQL**, puis sélectionnez le nom de l'appareil dans la liste qui s'affiche.

  2. Saisissez le nouveau nom de la base de données dans le champ **Nom de la base de données** de la base de données.

     Notez que le nom de la nouvelle base de données doit correspondre au nom de la base de données de l'appareil précédent. Les noms des bases de données doivent être identiques pour que vous puissiez utiliser la sauvegarde du Serveur d'administration. Le nom par défaut de la base de données est *KAV*.

8. Une fois l'installation terminée, restaurez les données du Serveur d'administration sur le nouvel appareil à l'aide de l'utilitaire klbackup.

Si vous utilisez SQL Server comme SGBD sur l'ancien et le nouvel appareil, notez que la version de SQL Server installée sur le nouvel appareil doit être identique ou ultérieure à la version de SQL Server installée sur l'appareil précédent. Sinon, vous ne pouvez pas récupérer les données du Serveur d'administration sur le nouvel appareil.

9. Ouvrez Kaspersky Security Center Web Console et connectez-vous au Serveur d'administration.
10. Vérifiez que tous les appareils administrés sont connectés au Serveur d'administration.
11. Désinstallez le Serveur d'administration et le serveur de base de données de l'appareil précédent.

Vous pouvez également utiliser la Console d'administration pour déplacer le Serveur d'administration et un serveur de base de données vers un autre appareil.

Vérification de l'intégrité des modules à l'aide des utilitaires klscmodchk et integrity_checker

Kaspersky Security Center contient plusieurs modules binaires qui se présentent sous la forme de bibliothèques liées dynamiquement, de fichiers exécutables, de fichiers de configuration et de fichiers d'interface. Les intrus peuvent remplacer un ou plusieurs modules exécutables ou fichiers d'application par d'autres fichiers contenant du code malveillant. Pour éviter la substitution de modules et de fichiers, Kaspersky Security Center fournit une vérification de l'intégrité des modules à l'aide des utilitaires klscmodchk et integrity_checker. Ces utilitaires vérifient que les modules et les fichiers n'ont pas été modifiés ni endommagés sans autorisation. Si la somme de contrôle du module ou du fichier d'application est incorrecte, celui-ci est considéré comme étant endommagé.

L'utilitaire klscmodchk effectue des contrôles d'intégrité pour les modules Kaspersky Security Center suivants :

- Serveur d'administration
- Agent d'administration
- Plug-ins d'administration pour la Console d'administration des fichiers manifestes

L'utilitaire Integrity_checker exécute des contrôles d'intégrité pour les modules Kaspersky Security Center suivants :

- Serveur d'administration
- Agent d'administration
- Kaspersky Security Center Web Console

Les deux utilitaires vérifient l'intégrité des modules sur la base du fichier manifeste kl_file_integrity_manifest.xml, qui fait partie de Kaspersky Security Center et se trouve dans le dossier d'installation. Le fichier manifeste du module contient des fichiers dont l'intégrité est importante pour le bon fonctionnement du module Kaspersky Security Center. L'intégrité des fichiers manifestes eux-mêmes est également vérifiée.

Il est fortement déconseillé de modifier le fichier manifeste kl_file_integrity_manifest.xml, car cela invaliderait la signature numérique et ferait échouer le contrôle d'intégrité.

Pour vérifier l'intégrité du module Kaspersky Security Center, exécutez une des commandes suivantes :

- `$ klscmodchk [ paramètres ]`

  L'utilitaire klscmodchk lance l'utilitaire integrity_checker avec le paramètre `--verbose` et vérifie l'intégrité des modules.

  Paramètres de l'utilitaire klscmodchk :

  - `-logfile <log_file_path>` : indiquez le chemin d'accès au fichier sur le disque pour la journalisation. Par défaut, les informations sont affichées dans la console.
  - `-chkplugins` : vérifie l'intégrité des plug-ins d'administration installés pour la Console d'administration qui contiennent des fichiers manifestes. Par défaut, les plug-ins d'administration ne sont pas cochés.
  - `-verbose` : affiche des informations élargies pendant la vérification de l'intégrité.

- `$ integrity_checker [ paramètres ] <chemin_fichier_manifest>`

  Paramètres de l'utilitaire integrity_checker :

  - `--help` : affiche l'aide de l'utilitaire integrity_checker.
  - `--version` : affiche la version de l'utilitaire integrity_checker.
  - `--verbose` : affiche les informations sur le fonctionnement de l'utilitaire. Lors d'une vérification de l'intégrité, il suffit d'utiliser ce paramètre dans la commande.

Le résultat de la vérification de chaque fichier manifeste est affiché à côté du nom du fichier manifeste dans le format suivant :

- SUCCEEDED : intégrité du fichier confirmée (code retour 0).
- ÉCHEC : intégrité du fichier non confirmée (code retour différent de zéro).

Vous pouvez également programmer des vérifications de l'intégrité qui s'exécuteront automatiquement au lancement de l'application. Par défaut, la vérification automatique de l'intégrité est désactivée.

Pour activer la vérification automatique de l'intégrité, procédez comme suit :

1. Sur l'appareil où le Serveur d'administration est installé, à l'invite de commande Windows, saisissez la commande suivante :

   ```
   klscflag.exe -fset -pv klserver -n KLMODCHK_ENABLE_CHECKING -t d -v 1
   ```

2. Redémarrez l'appareil.

La vérification automatique de l'intégrité est activée.

Au prochain démarrage de Kaspersky Security Center, l'utilitaire klscmodchk s'exécutera en même temps que le Serveur d'administration et lancera la vérification de l'intégrité des modules. Le résultat des vérifications d'intégrité est écrit dans le Journal des événements Kaspersky.

Configuration initiale de Kaspersky Security Center Web Console

Cette section décrit les étapes à suivre absolument après l'installation de Kaspersky Security Center Web Console pour effectuer la configuration initiale.

Assistant de configuration initiale de l'application (Kaspersky Security Center Web Console)

Cette section reprend les informations sur le fonctionnement de l'Assistant de configuration initiale du Serveur d'administration.

L'Assistant nécessite un accès Internet. Si votre Serveur d'administration n'a pas accès à Internet, nous vous recommandons d'effectuer manuellement toutes les étapes de l'Assistant via l'interface de Kaspersky Security Center Web Console.

L'application Kaspersky Security Center permet de configurer un ensemble minimum de paramètres indispensables à l'établissement d'un système d'administration centralisée pour protéger votre réseau contre les menaces pour la sécurité. Cette configuration s'opère via l'Assistant de configuration initiale de l'application. Pendant le fonctionnement de l'Assistant, vous pouvez introduire les modifications suivantes dans l'application :

- Ajouter des fichiers de clés ou saisir des codes d'activation qui peuvent être diffusés automatiquement sur les appareils dans les groupes d'administration.
- Configurer l'interaction avec Kaspersky Security Network (KSN). Si vous avez autorisé l'utilisation de KSN, l'Assistant active le service du serveur proxy KSN qui assure l'interaction entre KSN et les appareils.
- Configurer l'envoi de notifications par email des événements survenus pendant l'utilisation du Serveur d'administration et des applications administrées (afin qu'une notification passe avec succès, sur le Serveur d'administration et sur tous les appareils, le service Windows Messenger doit être lancé).
- Configurer la stratégie de protection des postes de travail et des serveurs, ainsi que les tâches de recherche de logiciels malveillants, de récupération des mises à jour et de sauvegarde des données pour le niveau supérieur de la stratégie des appareils administrés.

  L'Assistant de configuration initiale de l'application crée les stratégies uniquement pour les applications dont le dossier **Appareils administrés** ne contient pas encore de stratégies. L'Assistant de configuration initiale de l'application ne crée pas les tâches si les tâches avec de tels noms ont déjà été formées pour le niveau supérieur de la hiérarchie des appareils administrés.

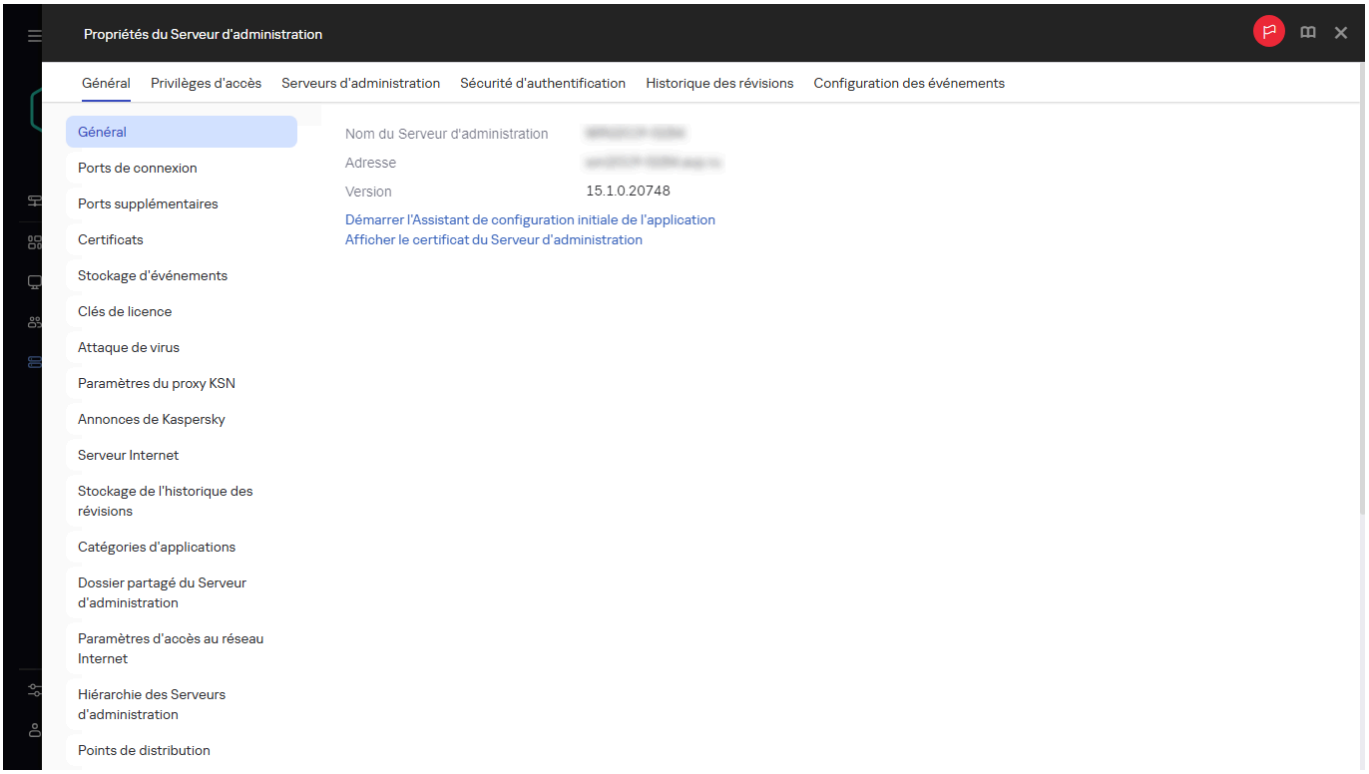
L'application vous invite automatiquement à lancer l'Assistant de configuration initiale de l'application après l'installation du Serveur d'administration, lors de la première connexion au Serveur d'administration. Vous pouvez aussi lancer l'Assistant de configuration initiale de l'application manuellement à tout moment.

Pour lancer manuellement l'Assistant de configuration initiale de l'application, procédez comme suit :

1. Dans le menu principal, cliquez sur l'icône des paramètres ( ) à côté du nom du Serveur d'administration.

   La fenêtre des propriétés du Serveur d'administration s'ouvre.

2. Sous l'onglet **Général**, sélectionnez la section **Général**.



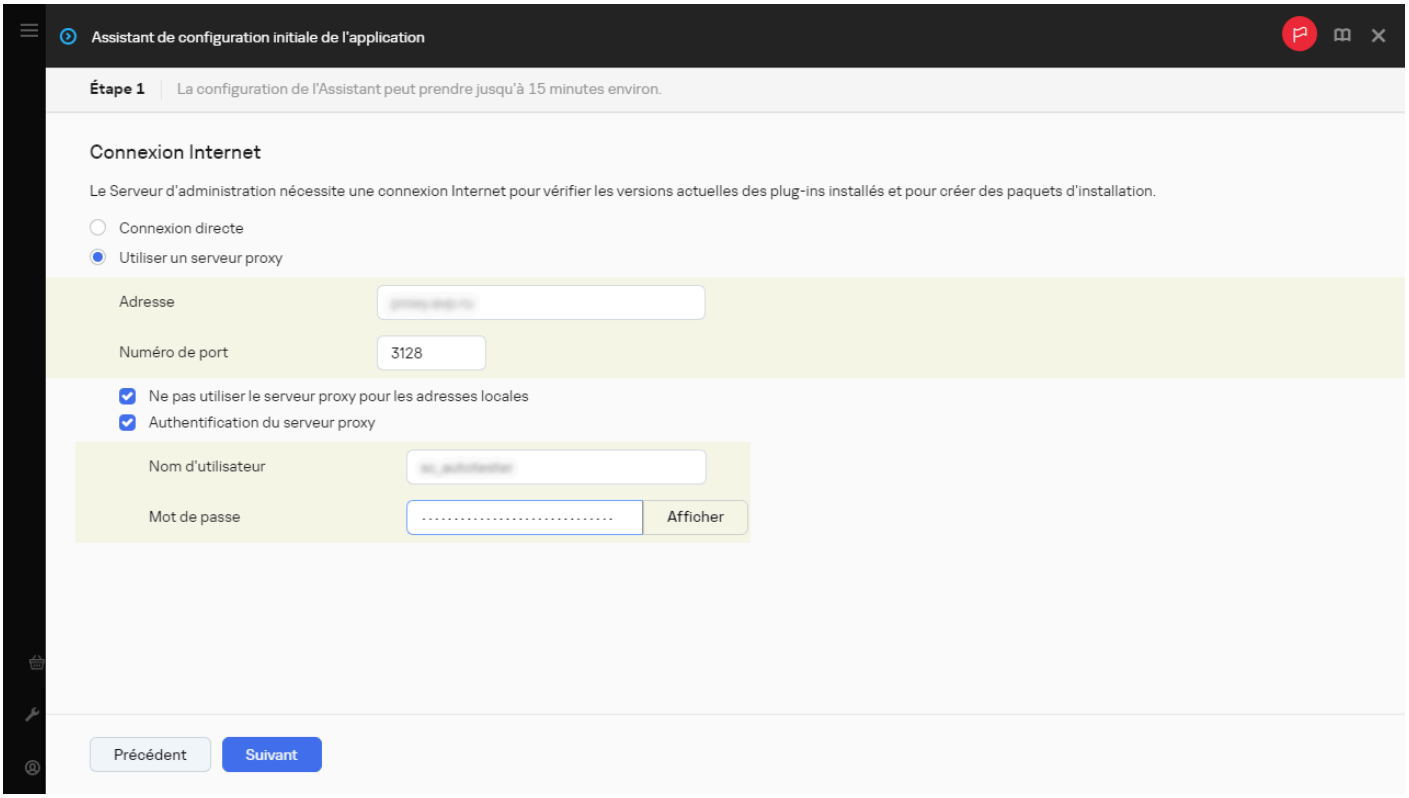
Fenêtre des propriétés du Serveur d'administration

3. Cliquez sur **Démarrer l'Assistant de configuration initiale de l'application**.

L'Assistant propose de réaliser la configuration initiale du Serveur d'administration. Suivez les instructions de l'assistant. Parcourez les étapes de l'Assistant à l'aide du bouton **Suivant**.

Étape 1. Spécification des paramètres de connexion Internet

Indiquez les paramètres d'accès Internet du Serveur d'administration. Vous devez configurer l'accès Internet pour utiliser Kaspersky Security Network et télécharger les mises à jour des bases antivirus pour Kaspersky Security Center et les applications Kaspersky administrées.



Paramètres de connexion à Internet

Activer l'option **Utiliser un serveur proxy** si vous souhaitez utiliser un serveur proxy pour vous connecter à Internet. Si cette option est activée, les champs de saisie des paramètres sont accessibles. Configurez les paramètres suivants de connexion au serveur proxy :

- Adresse

  Adresse du serveur proxy pour la connexion de Kaspersky Security Center à Internet.

- Numéro de port

  Numéro du port via lequel la connexion proxy à Kaspersky Security Center sera établie.

- Ne pas utiliser le serveur proxy pour les adresses locales

  Le serveur proxy n'est pas utilisé lors de la connexion aux appareils dans le réseau local.

- Authentification du serveur proxy

  Si la case est cochée, les champs de saisie permettent d'indiquer les identifiants pour l'authentification sur le serveur proxy.

  Ce champ de saisie est accessible si la case **Utiliser un serveur proxy** est cochée.

- Nom d'utilisateur

  Compte utilisateur sous lequel la connexion au serveur proxy est établie (ce champ est disponible si la case **Authentification du serveur proxy** est cochée).

- Mot de passe

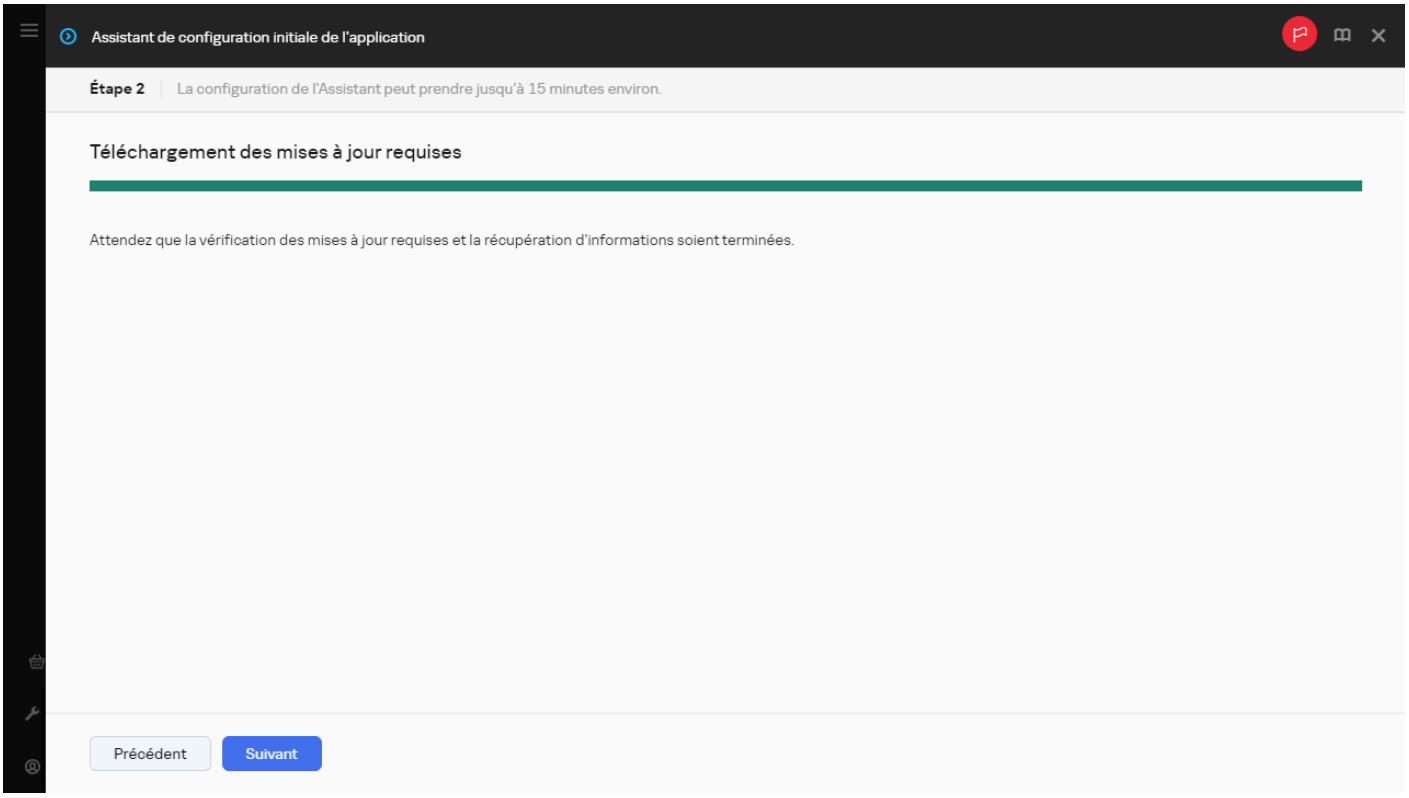
  Mot de passe défini par l'utilisateur sous le compte duquel la connexion au serveur proxy est établie (ce champ est disponible si la case **Authentification du serveur proxy** est cochée).

  Pour voir le mot de passe saisi, cliquez sur le bouton **Afficher** et maintenez-le enfoncé aussi longtemps que vous en avez besoin.

Vous pouvez aussi configurer l'accès à Internet plus tard, indépendamment de l'Assistant de démarrage rapide.

Étape 2. Téléchargement des mises à jour requises

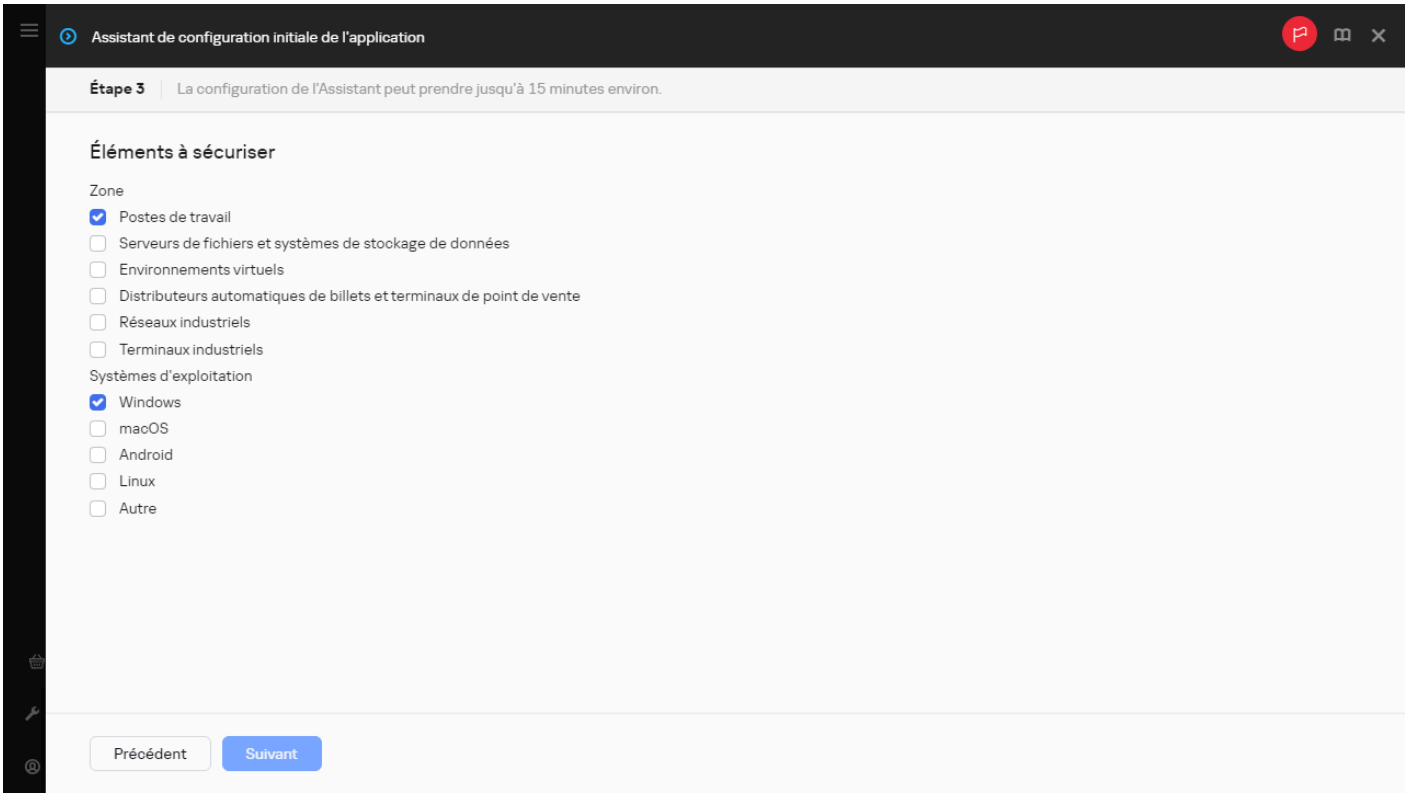
Les mises à jour requises sont automatiquement téléchargées des serveurs Kaspersky.



Téléchargement des mises à jour requises

Étape 3. Sélection des actifs à sécuriser

Sélectionnez les zones de protection et les systèmes d'exploitation utilisés sur votre réseau. Lorsque vous sélectionnez ces options, vous spécifiez les filtres pour les plug-ins d'administration des applications et les paquets de distribution sur les serveurs Kaspersky que vous pouvez télécharger pour les installer sur les appareils clients de votre réseau.



Sélection des actifs à sécuriser

Sélectionnez les options :

- **Zone**

  Vous pouvez sélectionner les zones de protection suivantes :

  - **Postes de travail**. Sélectionnez cette option si vous souhaitez protéger les postes de travail de votre réseau. L'option Poste de travail est sélectionnée par défaut.
  - **Serveurs de fichiers et systèmes de stockage de données**. Sélectionnez cette option si vous souhaitez protéger les serveurs de fichiers de votre réseau.
  - **Appareils mobiles**. Sélectionnez cette option si vous souhaitez protéger les appareils mobiles appartenant à l'entreprise ou aux employés de l'entreprise. Si vous sélectionnez cette option mais que vous n'avez pas fourni de licence avec la Fonction Administration des appareils mobiles, un message s'affiche vous informant de la nécessité de fournir une licence avec la Fonction Administration des appareils mobiles. Si vous ne fournissez pas de licence, vous ne pouvez pas utiliser la fonction Appareil mobile.
  - **Environnements virtuels**. Sélectionnez cette option si vous souhaitez protéger les machines virtuelles de votre réseau.
  - **Anti-Spam Kaspersky**. Sélectionnez cette option si vous souhaitez protéger les serveurs email de votre organisation contre le spam, la fraude et la diffusion de logiciels malveillants.
  - **Systèmes intégrés**. Sélectionnez cette option si vous souhaitez protéger les systèmes intégrés Windows, tels que les distributeurs automatiques de billets (ATM).
  - **Réseaux industriels**. Sélectionnez cette option si vous souhaitez surveiller les données de sécurité sur votre réseau industriel et à partir des points d'extrémité du réseau protégés par les applications Kaspersky.
  - **Terminaux industriels**. Sélectionnez cette option si vous souhaitez protéger des abonnés individuels au sein d'un réseau industriel.

- **Systèmes d'exploitation**

  Vous pouvez sélectionner les plateformes suivantes :

  - Microsoft Windows
  - macOS
  - Android
  - Linux
  - Autres

  Pour en savoir plus sur les systèmes d'exploitation pris en charge, consultez la section Configuration matérielle et logicielle requise pour Kaspersky Security Center Web Console.

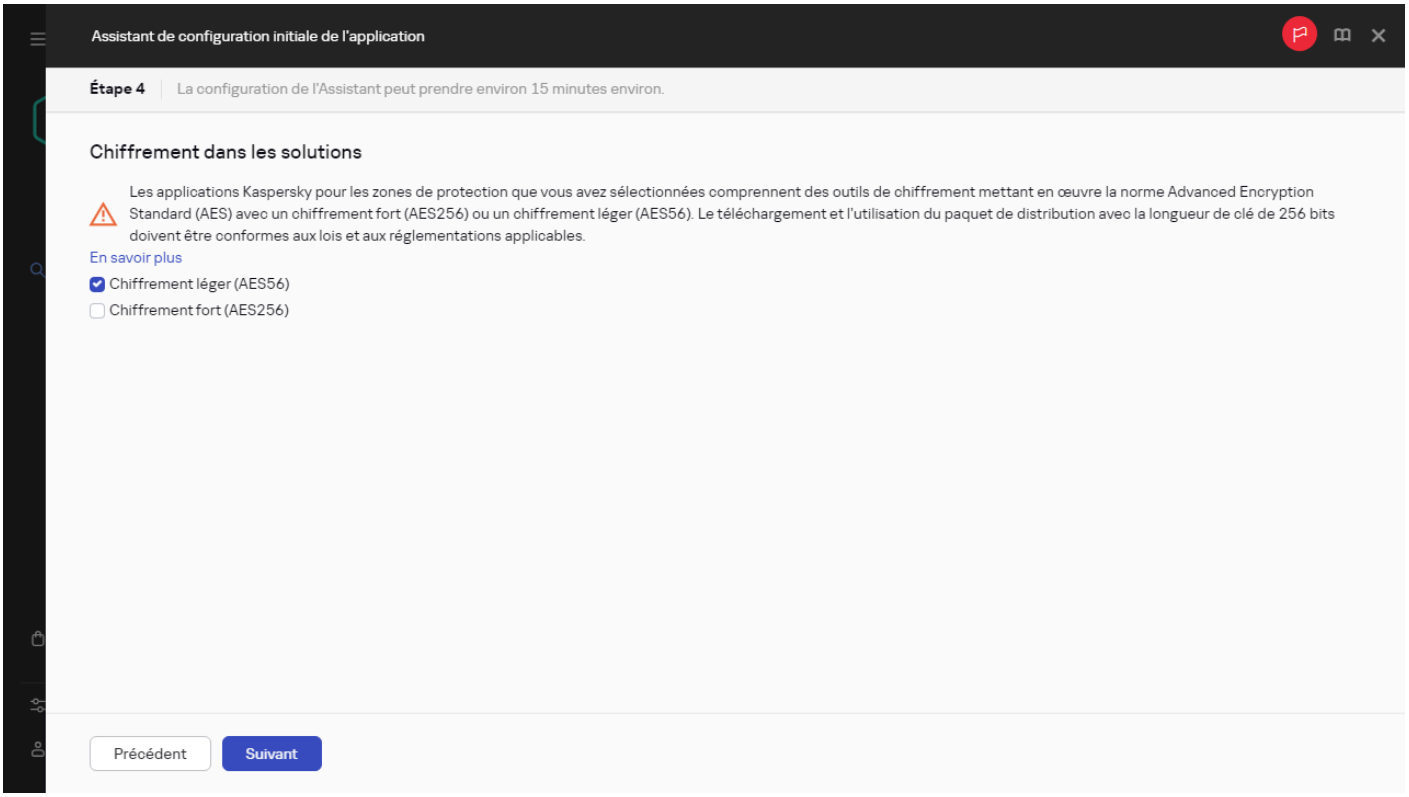
Vous pouvez sélectionner les paquets de l'application Kaspersky dans la liste des paquets disponibles ultérieurement, indépendamment de l'Assistant de configuration initiale de l'application. Pour simplifier la recherche des paquets requis, vous pouvez filtrer la liste des packages disponibles selon différents critères.

Étape 4. Sélection du chiffrement dans les solutions

La fenêtre **Chiffrement dans les solutions** s'affiche uniquement si vous avez sélectionné **Postes de travail** en tant que zone de protection.

Kaspersky Endpoint Security for Windows inclut des outils de chiffrement pour les informations stockées sur les appareils clients Windows. Ces outils de chiffrement ont la norme de chiffrement avancée (AES) implémentée avec une longueur de clé de 256 bits ou 56 bits.

Le téléchargement et l'utilisation du paquet de distribution avec une longueur de clé de 256 bits doivent être effectués conformément aux lois et aux réglementations applicables. Pour télécharger un paquet de distribution de Kaspersky Endpoint Security for Windows adapté aux besoins de votre organisation, consultez la législation du pays où se trouvent les appareils clients de votre organisation.



Sélection du chiffrement dans les solutions

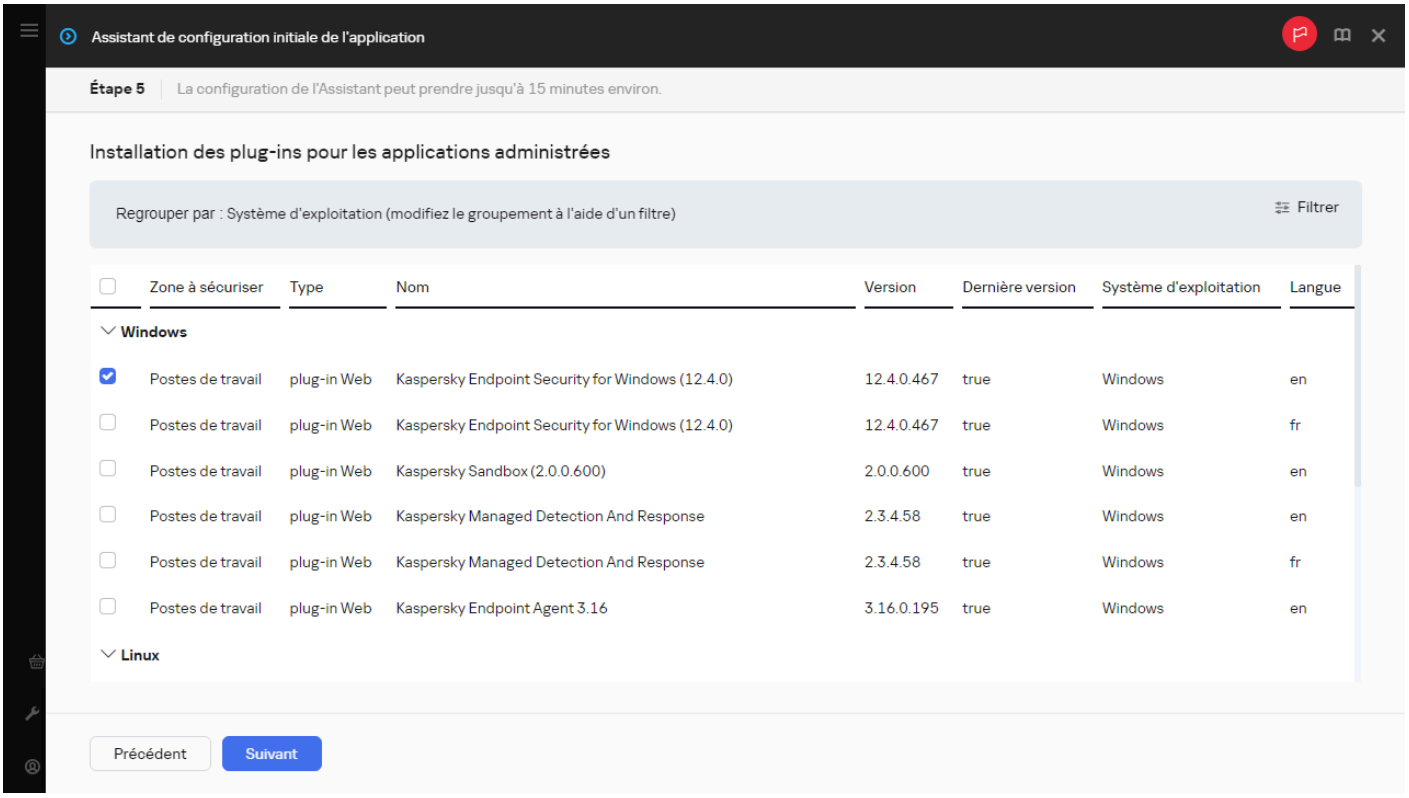
Dans la fenêtre **Chiffrement dans les solutions**, sélectionnez l'un des types de chiffrement suivants :

- Chiffrement léger. Ce type de chiffrement utilise une longueur de clé de 56 bits.
- Chiffrement fort. Ce type de chiffrement utilise une longueur de clé de 256 bits.

Vous pouvez sélectionner le paquet de distribution de Kaspersky Endpoint Security for Windows avec le type de chiffrement requis ultérieurement, indépendamment de l'Assistant de configuration initiale de l'application.

Étape 5. Configuration de l'installation de plug-ins pour les applications administrées

Sélectionnez les plug-ins pour les applications administrées à installer. Une liste des plug-ins situés sur les serveurs de Kaspersky s'affiche. La liste est filtrée selon les options sélectionnées à l'étape précédente de l'Assistant. Par défaut, une liste complète comprend des plug-ins dans toutes les langues. Pour afficher uniquement le plug-in dans une langue en particulier, utilisez le filtre.



Installation de plug-ins pour les applications administrées

La liste des plug-ins comprend les colonnes suivantes :

- **Zone à sécuriser**

  Cette colonne affiche la sélection des zones à protéger.

- **Type**

  Les types de plug-ins sont affichés dans cette colonne.

- **Nom**

  Les plug-ins en fonction des zones de protection et des plates-formes que vous avez sélectionnées à l'étape précédente sont sélectionnés.

- Version

  La liste comprend des plug-ins de toutes les versions placées sur les serveurs de Kaspersky. Par défaut, les plug-ins des dernières versions sont sélectionnés.

- Dernière version

  Cette colonne indique s'il s'agit de la dernière version du plug-in. Si la **true** valeur est affichée, le plug-in correspondant utilise la dernière version. Si la valeur **false** s'affiche, le plug-in correspondant possède une version plus récente.

- Système d'exploitation

  Cette colonne affiche les plug-ins des systèmes d'exploitation.

- Langue

  Par défaut, la langue de localisation d'un plug-in est définie par la langue Kaspersky Security Center que vous avez sélectionnée lors de l'installation. Vous pouvez spécifier d'autres langues dans la liste déroulante **Afficher la langue de la Console d'administration ou**.

Une fois les plug-ins sélectionnés, cliquez sur **Suivant** pour démarrer l'installation.

Vous pouvez installer les plug-ins d'administration pour les applications Kaspersky manuellement, indépendamment de l'Assistant de configuration initiale de l'application.

L'Assistant de configuration initiale de l'application installe automatiquement les plug-ins sélectionnés. Pour installer certains plug-ins, vous devez accepter les conditions du CLUF. Lisez le CLUF, cochez la case **J'accepte les termes du Kaspersky Security Network** et cliquez sur le bouton **Installer**. Si vous n'acceptez pas les termes du CLUF, le plug-in n'est pas installé.

Lorsque tous les plug-ins sélectionnés sont installés, l'Assistant de configuration initiale de l'application vous amène automatiquement à l'étape suivante.

Étape 6. Installation des plug-ins sélectionnés

L'Assistant de configuration initiale de l'application installe automatiquement les plug-ins sélectionnés à l'étape précédente. Pour installer certains plug-ins, vous devez accepter les conditions du CLUF. Lisez le CLUF, cochez la case **J'accepte les termes du Kaspersky Security Network** et cliquez sur le bouton **Installer**. Si vous n'acceptez pas les termes du CLUF, le plug-in n'est pas installé.

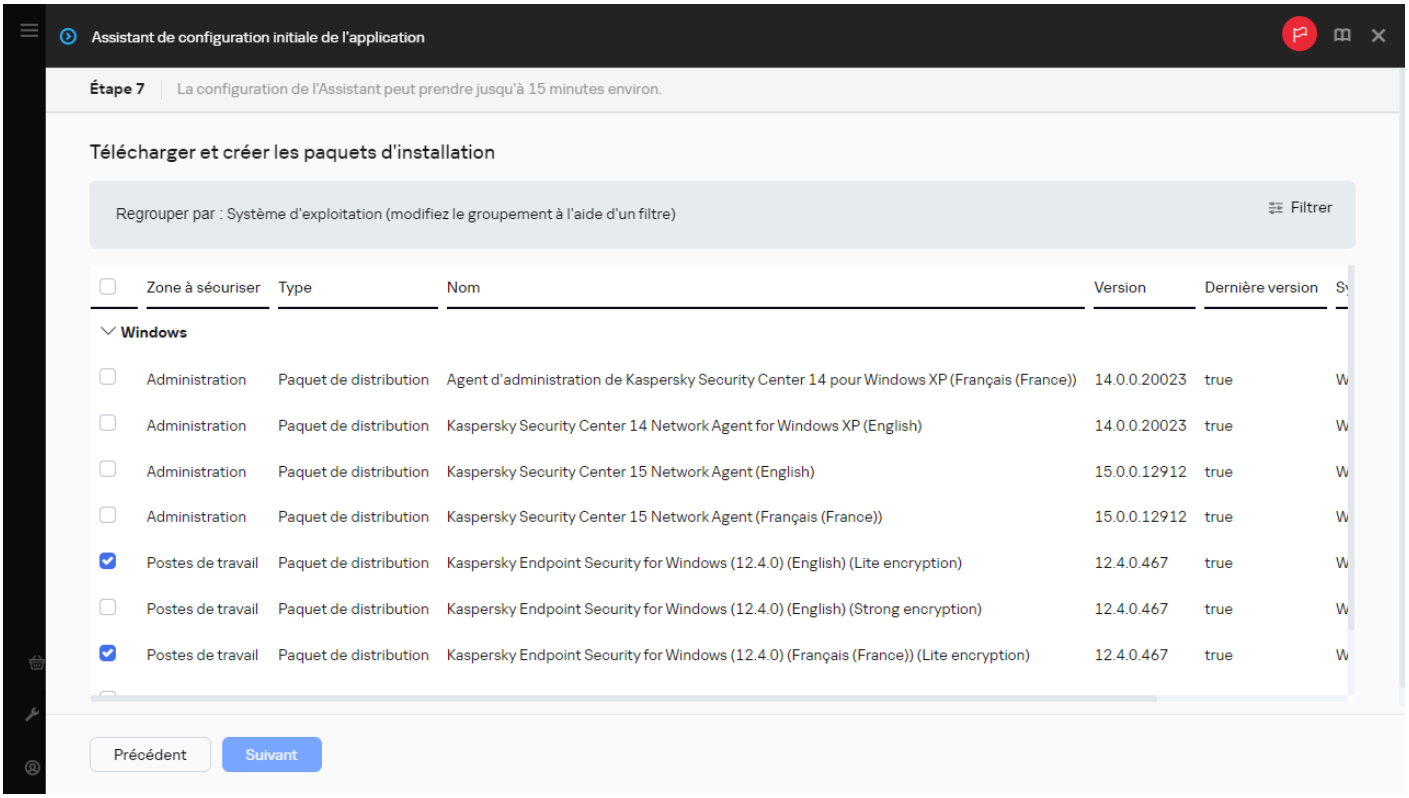
Lorsque tous les plug-ins sélectionnés sont installés, l'Assistant de configuration initiale de l'application vous amène automatiquement à l'étape suivante.

Étape 7. Téléchargement des paquets de distribution et création des paquets d'installation

Sélectionnez les paquets de distribution à télécharger.

Les distributifs des applications administrées peuvent nécessiter l'installation d'une version minimale spécifique de Kaspersky Security Center.

Une fois que vous avez sélectionné un type de chiffrement pour Kaspersky Endpoint Security for Windows, la liste des paquets de distribution des deux types de chiffrement s'affiche. Un paquet de distribution avec le type de chiffrement choisi est sélectionné dans la liste. Vous pouvez sélectionner des paquets de distribution de tout type de chiffrement. La langue du paquet de distribution correspond à la langue de Kaspersky Security Center. Si aucun paquet de distribution de Kaspersky Endpoint Security for Windows n'existe pour la langue de Kaspersky Security Center, le paquet de distribution anglais est sélectionné.



Téléchargement des paquets de distribution et création des paquets d'installation

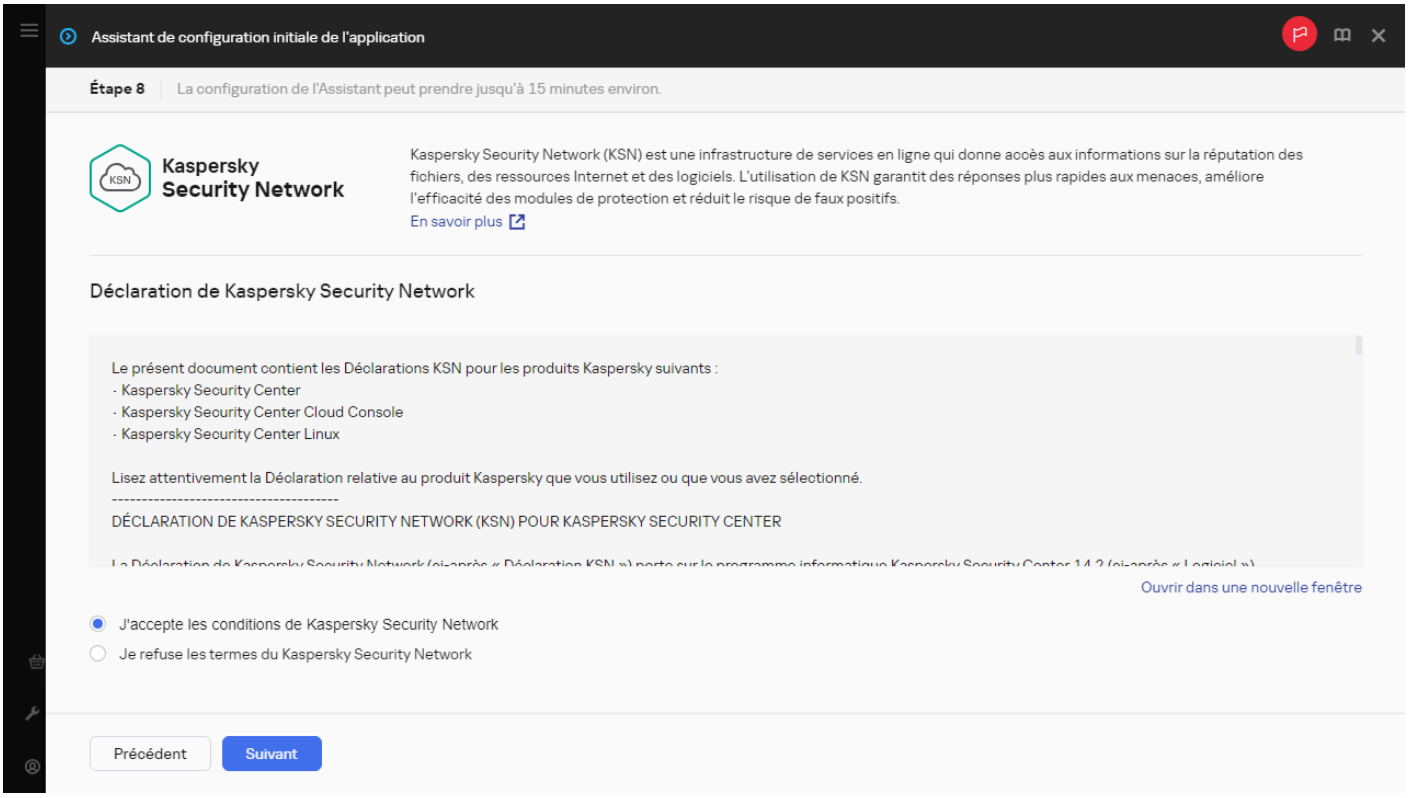
Pour terminer le téléchargement de certains paquets de distribution, vous devez accepter le CLUF. Lorsque vous cliquez sur le bouton **Accepter**, le texte du CLUF s'affiche. Pour passer à l'étape suivante de l'Assistant, vous devez accepter les termes et conditions du CLUF et les termes et conditions de la politique de confidentialité de Kaspersky. Si vous n'acceptez pas les termes et conditions, le téléchargement du paquet est annulé.

Une fois que vous avez accepté les termes et conditions du CLUF et les termes et conditions de la politique de confidentialité de Kaspersky, le téléchargement des paquets de distribution se poursuit. Par la suite, vous pouvez utiliser les paquets d'installation pour déployer des applications Kaspersky sur les appareils clients.

Vous pouvez télécharger les paquets de distribution et créer des paquets d'installation ultérieurement, indépendamment de l'Assistant de configuration initiale de l'application.

Étape 8. Configuration de Kaspersky Security Network

Indiquer les paramètres du transfert des informations sur le fonctionnement de Kaspersky Security Center dans la base de connaissances de Kaspersky Security Network.



Configuration de Kaspersky Security Network

Sélectionnez l'une des options ci-dessous :

- **J'accepte les termes du Kaspersky Security Network**

  Kaspersky Security Center et les applications administrées installées sur les appareils client transfèrent automatiquement les détails de leurs opérations à Kaspersky Security Network. La coopération avec Kaspersky Security Network garantit une mise à jour plus rapide des bases de données sur les virus et les menaces, ce qui améliore la vitesse de réaction face aux menaces naissantes.

- **Je refuse les termes du Kaspersky Security Network**

  Kaspersky Security Center et les applications administrées ne fourniront aucune information à Kaspersky Security Network.

  Si vous sélectionnez cette option, l'utilisation de Kaspersky Security Network sera désactivée.

Vous pouvez configurer l'accès à Kaspersky Security Network (KSN) ultérieurement, indépendamment de l'Assistant de configuration initiale de l'application.

Étape 9. Sélection de la méthode d'activation de l'application

Choisissez une des options suivantes pour activer Kaspersky Security Center :

- **Saisir votre code d'activation**

  Le *code d'activation* est une suite unique de 20 caractères alphanumériques. Vous le saisissez pour ajouter la clé activant le Kaspersky Security Center. Vous recevez le code d'activation à l'adresse email que vous avez indiquée après l'achat de Kaspersky Security Center.

  Pour activer l'application à l'aide du code d'activation, vous avez besoin d'un accès Internet pour vous connecter aux serveurs d'activation de Kaspersky.

  Si vous avez sélectionné cette option d'activation, vous pouvez activer l'option **Distribuer automatiquement la clé de licence sur les appareils administrés**.

  Si cette option est activée, la clé de licence sera déployée automatiquement sur les appareils administrés.

  Si cette option est désactivée, vous pouvez déployer la clé de licence sur les appareils administrés ultérieurement, dans le nœud **Licences pour les logiciels de Kaspersky** de l'arborescence de la Console d'administration.

- **Indiquez le fichier clé**

  Le *fichier clé* est un fichier doté d'une extension .key qui vous est fourni par Kaspersky. Il permet d'ajouter le fichier clé activant l'application.

  Les méthodes d'obtention du fichier clé sont décrites dans la section suivante : À propos du fichier clé.

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

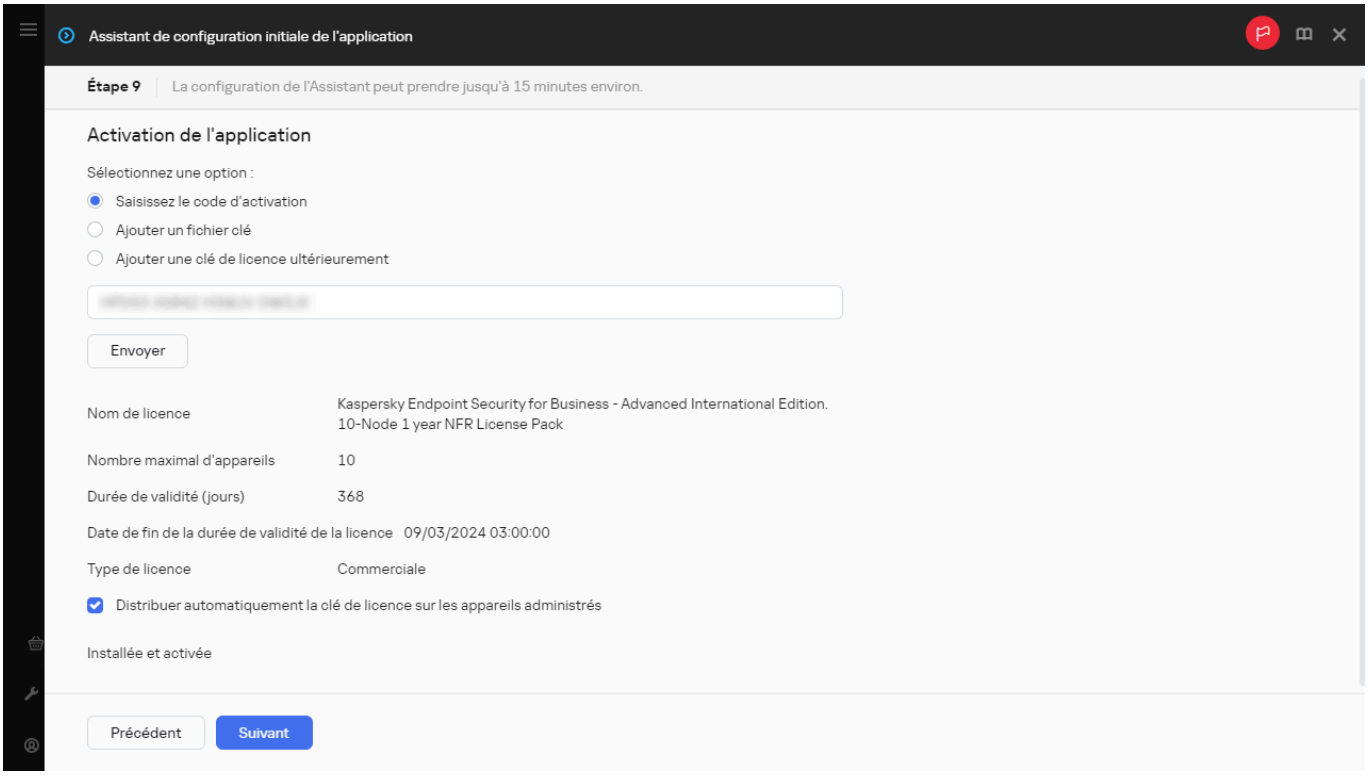
  Si vous avez sélectionné cette option d'activation, vous pouvez activer l'option **Distribuer automatiquement la clé de licence sur les appareils administrés**.

  Si cette option est activée, la clé de licence sera déployée automatiquement sur les appareils administrés.

  Si cette option est désactivée, vous pouvez déployer la clé de licence sur les appareils administrés ultérieurement, dans le nœud **Licences pour les logiciels de Kaspersky** de l'arborescence de la Console d'administration.

- **Reportez l'activation de l'application**

L'application fonctionne avec la fonctionnalité de base, sans l'Administration des appareils mobiles et sans la Gestion des vulnérabilités et des correctifs.



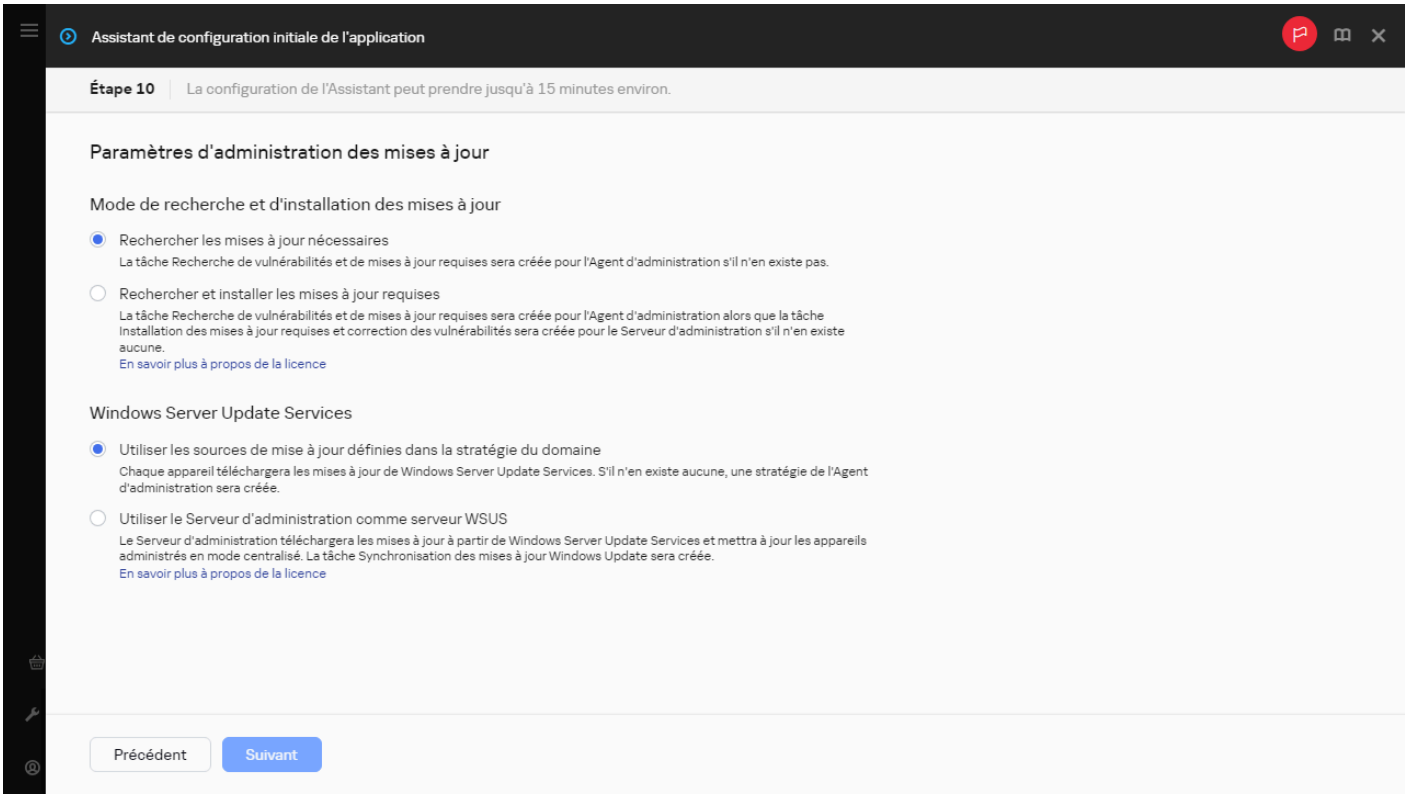
Sélection de la méthode d'activation de l'application

Si vous avez choisi l'activation reportée de l'application, vous pouvez ajouter une clé de licence plus tard à tout moment en sélectionnant **Opérations** → **Licence**.

Lors de l'utilisation de Kaspersky Security Center, déployé depuis une image AMI payante ou pour un SKU facturé mensuellement en fonction de l'utilisation, il est impossible d'ajouter un fichier clé ou de saisir un code.

Étape 10. Spécification des paramètres de gestion des mises à jour tierces

Cette étape ne s'affiche pas si vous ne disposez pas de licence pour le fonctionnement de Gestion des vulnérabilités et des correctifs et si la tâche *Recherche de vulnérabilités et de mises à jour requises* existe déjà.



Paramètres de gestion des mises à jour tierces

Pour les mises à jour logicielles tierces, sélectionnez l'une des options suivantes :

- **Rechercher les mises à jour nécessaires**

  La tâche *Recherche de vulnérabilités et de mises à jour requises* est créée automatiquement, si vous n'en avez pas.

  Par défaut, cette option est sélectionnée.

- **Rechercher et installer les mises à jour requises**

  Les tâches *Recherche de vulnérabilités et de mises à jour requises* et *Installation des mises à jour requises et correction des vulnérabilités* sont créées automatiquement, si vous n'en avez pas.

  Cette option est accessible uniquement en présence d'une licence pour le fonctionnement de Gestion des vulnérabilités et des correctifs.

Pour les mises à jour Windows Update, sélectionnez l'une des options suivantes :

- **Utiliser les sources de mise à jour définies dans la stratégie du domaine**

  Les appareils clients téléchargent les mises à jour de Windows Update en fonction des paramètres de stratégie de votre domaine. La stratégie d'Agent d'administration est créée automatiquement si vous n'en avez pas.

- **Utiliser le Serveur d'administration comme serveur WSUS**

  Les appareils clients téléchargent les mises à jour Windows Update à partir du Serveur d'administration. La tâche *Synchronisation des mises à jour Windows Update* et la stratégie d'Agent d'administration sont créées automatiquement, si vous n'en avez pas.

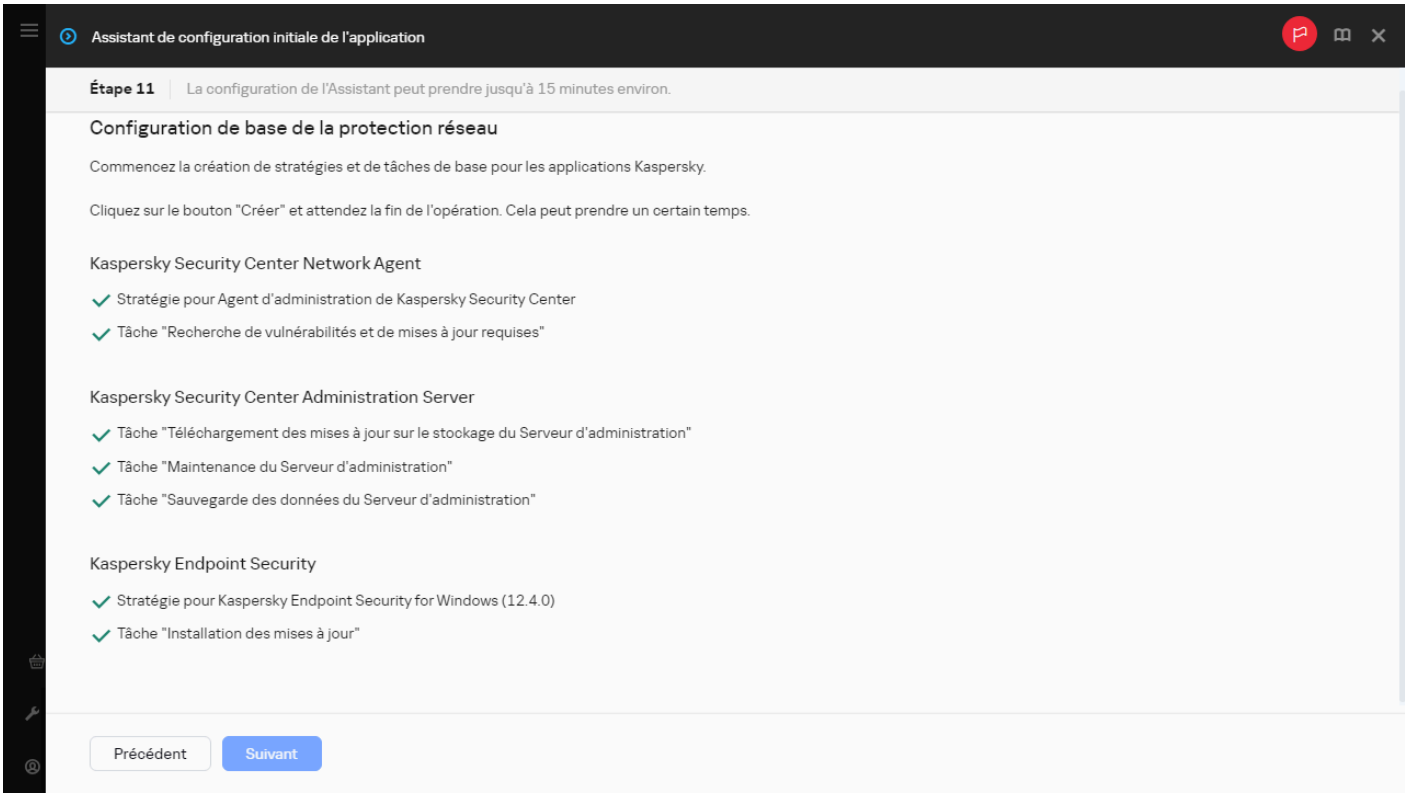
  Cette option est accessible uniquement en présence d'une licence pour le fonctionnement de Gestion des vulnérabilités et des correctifs.

Vous pouvez créer les tâches *Rechercher les vulnérabilités et les mises à jour requises* et *Installer les mises à jour requises et corriger les vulnérabilités* séparément de l'Assistant de configuration initiale de l'application. Pour utiliser le Serveur d'administration comme serveur WSUS, créez la tâche *Synchronisation des mises à jour Windows Update* et puis sélectionner l'option **&Utiliser le Serveur d'administration comme serveur WSUS** dans la stratégie de l'Agent d'administration.

Étape 11. Création de la configuration de base de la protection d'un réseau

Vous pouvez consulter une liste de stratégies et de tâches créées.

Avant de passer à l'étape suivante de l'Assistant, attendez la fin de la création des stratégies et des tâches.

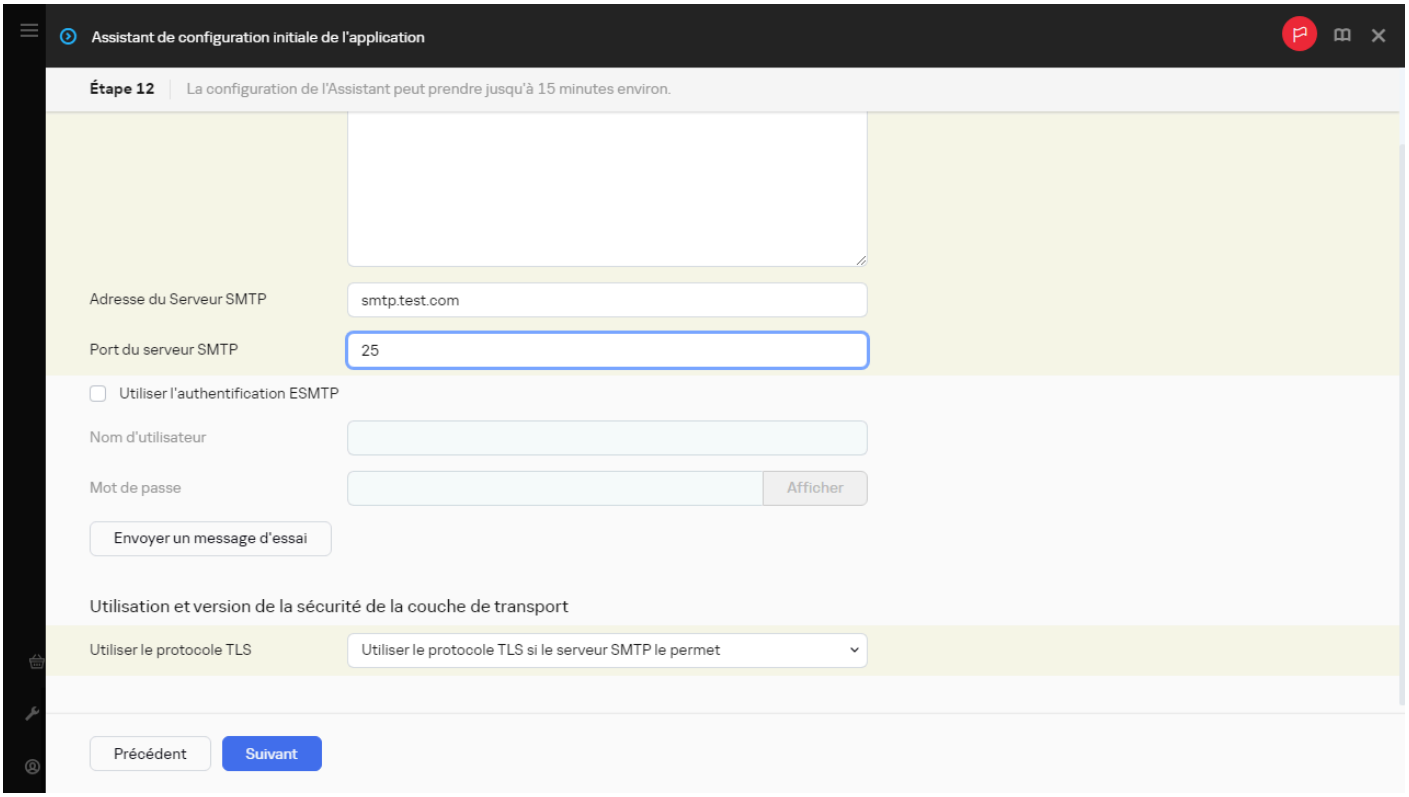


Création de la configuration de base de la protection d'un réseau

Vous pouvez créer les tâches et les stratégies requises ultérieurement, indépendamment de l'Assistant de configuration initiale de l'application.

Étape 12. Configuration des notifications par email

Configurez l'envoi des notifications sur les événements enregistrés lors du travail avec les applications de Kaspersky sur les appareils clients. Ces paramètres seront utilisés comme paramètres par défaut pour les stratégies d'applications.



Configuration des notifications par email

Pour configurer la diffusion des notifications relatives aux événements qui surviennent dans les applications de Kaspersky, utilisez les paramètres suivants :

- **Destinataires (adresses email)**

  Les adresses email des utilisateurs auxquels l'application va envoyer les notifications. Vous pouvez entrer une ou plusieurs adresse(s). Si vous entrez plusieurs adresses, séparez-les par un point-virgule.

- **Adresse du Serveur SMTP**

  L'adresse ou les adresses des serveurs de messagerie de votre organisation.

  Si vous entrez plusieurs adresses, séparez-les par un point-virgule. Vous pouvez utiliser les valeurs suivantes du paramètre :

  - Adresse IPv4 ou IPv6
  - Nom de réseau Windows (nom NetBIOS) de l'appareil
  - Nom complet du serveur SMTP

- Port du serveur SMTP

  Numéro du port de communication du serveur SMTP. Si vous utilisez plusieurs serveurs SMTP, la connexion à ceux-ci est établie via le port de communication indiqué. Le numéro de port par défaut est 25.

- Utiliser l'authentification ESMTP

  Activation de la prise en charge de l'authentification ESMTP. Après avoir coché la case, dans les champs **Nom d'utilisateur** et **Mot de passe**, vous pouvez définir les paramètres d'authentification ESMTP. Celle-ci est décochée par défaut.

- Utiliser le protocole TLS

Vous pouvez indiquer les paramètres TLS de connexion au serveur SMTP :

- **Ne pas utiliser le protocole TLS**

  Vous pouvez choisir cette option si vous désactivez le chiffrement des emails.

- **Utiliser le protocole TLS si le serveur SMTP le permet**

  Vous pouvez choisir cette option si vous voulez utiliser une connexion TLS pour un serveur SMTP. Si le serveur SMTP n'est pas compatible avec TLS, le Serveur d'administration connecte le serveur SMTP sans utiliser TLS.

- **Utiliser toujours le protocole TLS, vérifier la validité du certificat du serveur**

  Vous pouvez choisir cette option si vous voulez utiliser les paramètres d'authentification TLS. Si le serveur SMTP n'est pas compatible avec TLS, le Serveur d'administration ne peut pas connecter le serveur SMTP.

  Nous vous recommandons d'utiliser cette option pour améliorer la protection de la connexion avec un serveur SMTP. Si vous choisissez cette option, vous pouvez définir les paramètres d'authentification pour une connexion TLS.

  Si vous sélectionnez la valeur **Utiliser toujours le protocole TLS, vérifier la validité du certificat du serveur**, vous pouvez définir un certificat pour l'authentification du serveur SMTP et choisir si vous souhaitez activer la communication via n'importe quelle version de TLS ou uniquement via TLS 1.2 ou les versions ultérieures. Vous pouvez également spécifier un certificat pour l'authentification du client sur le serveur SMTP.

Vous pouvez préciser les certificats pour une connexion TLS en cliquant sur le lien **Indiquer les certificats** :

- Recherchez un fichier de certificat de serveur SMTP :

  Vous pouvez recevoir un fichier avec la liste des certificats de l'autorité de certification de confiance et charger le fichier sur le Serveur d'administration. Kaspersky Security Center vérifie si le certificat d'un serveur SMTP est également signé par une autorité de certification de confiance ou non. Kaspersky Security Center ne peut pas se connecter à un serveur SMTP si le certificat du serveur SMTP ne provient pas d'une autorité de certification de confiance.

- Recherchez un fichier de certificat client :

  Vous pouvez utiliser un certificat que vous avez reçu de n'importe quelle source, par exemple, de n'importe quelle autorité de certification de confiance. Vous devez spécifier le certificat et sa clé privée en utilisant l'un des types de certificats suivants :

  - Certificat X-509 :

    Vous devez spécifier un fichier avec le certificat et un fichier avec la clé privée. Les deux fichiers ne dépendent pas l'un de l'autre, et l'ordre de chargement des fichiers est sans importance. Lorsque les deux fichiers sont chargés, vous devez spécifier le mot de passe pour décoder la clé privée. Le mot de passe peut présenter une valeur vide si la clé privée n'est pas encodée.

  - Conteneur pkcs12 :

    Vous devez charger un seul fichier contenant le certificat et sa clé privée. Lorsque le fichier est chargé, vous devez ensuite indiquer le mot de passe pour décoder la clé privée. Le mot de passe peut présenter une valeur vide si la clé privée n'est pas encodée.

Vous pouvez vérifier les paramètres définis pour l'envoi des notifications par email à l'aide du bouton **Envoyer un message d'essai**.

Vous pouvez configurer les notifications relatives aux événements, indépendamment de l'Assistant de démarrage rapide.

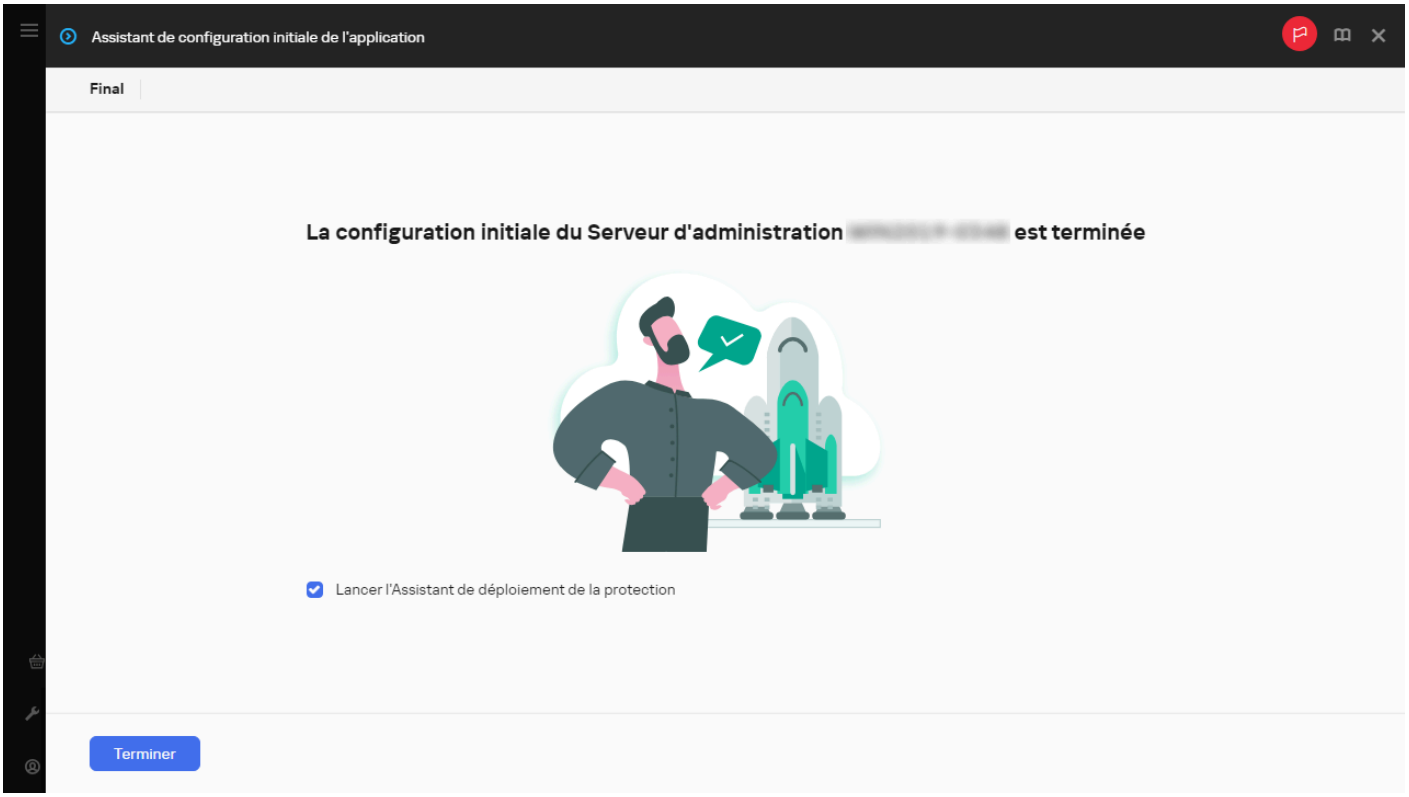
Étape 13. Réalisation d'un sondage réseau

Le Serveur d'administration exécute un sondage initial. Une barre de progression s'affiche pendant le sondage. Quand le sondage est terminé, le lien **Consulter les appareils détectés** devient accessible. Cliquez sur ce lient pour voir les appareils réseau détectés par le Serveur d'administration. Pour retourner à l'Assistant de configuration initiale de l'application, appuyez sur la touche **Échap**.

Vous pouvez interroger votre réseau ultérieurement, indépendamment de l'Assistant de configuration initiale de l'application. Utilisez Kaspersky Security Center Web Console pour configurer le sondage d'un contrôleur de domaine, des domaines Windows, des plages IP et des réseaux IPv6.

Étape 14. Fin de l'Assistant de configuration initiale de l'application

Dans la fenêtre de fin de l'Assistant de configuration initiale de l'application, cochez la case **Lancer l'Assistant de déploiement de la protection** si vous voulez lancer l'installation automatique des applications antivirus et/ou de l'Agent d'administration sur les appareils de votre réseau.



Dernière étape de l'Assistant de configuration initiale de l'application

Cliquez sur **Terminer** pour terminer le travail de l'Assistant.

Connexion d'appareils itinérants

Cette section décrit comment connecter au Serveur d'administration des appareils itinérants (c'est-à-dire des appareils administrés situés en dehors du réseau principal).

Scénario : connexion d'appareils itinérants via une passerelle de connexion

Ce scénario décrit comment connecter au Serveur d'administration des appareils administrés situés en dehors du réseau principal.

Prérequis

Le scénario prévoit les conditions préalables suivantes :

- Une zone démilitarisée (DMZ) est organisée dans le réseau de votre organisation.
- Le Serveur d'administration de Kaspersky Security Center Administration est déployé sur le réseau de l'organisation.

Étapes

Ce scénario se déroule par étapes :

1. **Sélection d'un appareil client dans la DMZ**

   Cet appareil sera utilisé comme passerelle de connexion L'appareil que vous sélectionnez doit répondre aux exigences en matière de passerelles de connexion.

2. **Installation de l'Agent d'administration dans le rôle de passerelle de connexion**

   Nous vous recommandons d'utiliser une installation locale pour installer l'Agent d'administration sur l'appareil sélectionné.

   Par défaut, le fichier d'installation se trouve à l'adresse suivante : \\<nom du serveur>\KLSHARE\PkgInst\NetAgent_<numéro de la version>

   Dans la fenêtre **Passerelle de connexion** de l'Assistant d'installation de l'Agent d'administration, sélectionnez l'option **Utiliser l'Agent d'administration en tant que passerelle de connexion en DMZ**. Ce mode active simultanément le rôle de passerelle de connexion et indique à l'Agent d'administration d'attendre les connexions du Serveur d'administration plutôt que d'établir des connexions avec le Serveur d'administration.

   Vous pouvez également installer l'Agent d'administration sur un appareil Linux et le configurer pour qu'il fonctionne en tant que passerelle de connexion, mais faites attention à la liste des limitations de l'Agent d'administration s'exécutant sur les appareils Linux.

3. **Autorisation de connexions dans les pare-feux sur la passerelle de connexion**

   Pour vous assurer que le Serveur d'administration peut réellement se connecter à la passerelle de connexion dans la DMZ, autorisez les connexions au port TCP 13000 dans tous les pare-feux entre le Serveur d'administration et la passerelle de connexion.

   Si la passerelle de connexion ne dispose d'aucune adresse IP réelle sur Internet, mais se trouve plutôt derrière une Traduction d'adresses réseau (NAT), configurez une règle pour transférer les connexions via la NAT.

4 **Création d'un groupe d'administration pour les appareils externes**

Créez un nouveau groupe sous le groupe **Appareils administrés**. Ce nouveau groupe contiendra des appareils externes administrés.

5 **Connexion de la passerelle de connexion au Serveur d'administration**

La passerelle de connexion que vous avez configurée attend une connexion à partir du Serveur d'administration. Cependant, le Serveur d'administration n'énumère pas l'appareil avec la passerelle de connexion parmi les appareils administrés. Cela est dû au fait que la passerelle de connexion n'a pas tenté d'établir une connexion avec le Serveur d'administration. Par conséquent, vous avez besoin d'une procédure spéciale pour vous assurer que le Serveur d'administration amorce une connexion à la passerelle de connexion.

Procédez comme suit :

1. Ajoutez la passerelle de connexion en tant que point de distribution.
2. Déplacez la passerelle de connexion du groupe **Appareils non définis** vers le groupe que vous avez créé pour les appareils externes.

La passerelle de connexion est connectée et configurée.

6 **Connexion d'appareils de bureau externes au Serveur d'administration**

En règle générale, les appareils de bureau externes ne sont pas déplacés à l'intérieur du périmètre. Par conséquent, vous devez les configurer pour vous connecter au Serveur d'administration via la passerelle lors de l'installation de l'Agent d'administration.

7 **Configuration des mises à jour pour les appareils de bureau externes**

Si les mises à jour des applications de sécurité sont configurées de manière à être téléchargées à partir du Serveur d'administration, les appareils externes téléchargent les mises à jour via la passerelle de connexion. Ceci présente deux inconvénients :

- Il s'agit d'un trafic inutile, qui occupe la bande passante du canal de communication via Internet de l'entreprise.
- Il ne s'agit pas nécessairement du moyen le plus rapide d'obtenir des mises à jour. Il est très probable qu'il serait moins coûteux et plus rapide pour les appareils externes de recevoir les mises à jour à partir des serveurs de mise à jour de Kaspersky.

Procédez comme suit :

1. Déplacez tous les appareils externes vers le groupe d'administration distinct que vous avez créé précédemment.
2. Excluez le groupe contenant les appareils externes de la tâche de mise à jour.
3. Créez une tâche de mise à jour distincte pour le groupe contenant les appareils externes.

8 **Connexion d'ordinateurs portables itinérants au Serveur d'administration**

Les ordinateurs portables itinérants se trouvent parfois au sein du réseau, et parfois en dehors de celui-ci. Pour assurer une gestion efficace, vous avez besoin qu'ils se connectent au Serveur d'administration différemment en fonction de leur position. Pour utiliser le trafic de manière efficace, ils doivent également recevoir des mises à jour de différentes sources en fonction de leur position.

Vous devez configurer des règles pour les utilisateurs itinérants : profils de connexion et descriptions d'emplacement réseau. Chaque règle définit l'instance de Serveur d'administration à laquelle les ordinateurs portables itinérants doivent se connecter en fonction de leur position et l'instance de Serveur d'administration à partir de laquelle ils doivent recevoir les mises à jour.

Scénario : Connexion d'appareils itinérants via un Serveur d'administration secondaire dans la DMZ

Si vous souhaitez connecter au Serveur d'administration des appareils administrés situés en dehors du réseau principal, vous pouvez le faire à l'aide d'un Serveur d'administration secondaire situé dans la zone démilitarisée (DMZ).

Prérequis

Avant de démarrer, assurez-vous que vous avez :

- Une zone démilitarisée (DMZ) est organisée dans le réseau de votre organisation.
- Le serveur d'administration de Kaspersky Security Center est déployé sur le réseau interne de l'organisation.

Étapes

Ce scénario se déroule par étapes :

1. **Sélection d'un appareil client dans la DMZ**

   Dans le DMZ, sélectionnez un appareil client qui va servir de Serveur d'administration secondaire.

2. **Installation du Serveur d'administration de Kaspersky Security Center**

   Installer le Serveur d'administration de Kaspersky Security Center sur cet appareil client.

3. **Création d'une hiérarchie des Serveurs d'administration**

   Si vous placez un Serveur d'administration secondaire dans la DMZ, le Serveur d'administration secondaire doit recevoir une connexion du Serveur d'administration primaire. Pour ce faire, ajoutez un nouveau Serveur d'administration à titre de Serveur secondaire de telle sorte que le Serveur d'administration primaire se connecte au Serveur d'administration secondaire via le port 13000. Lorsque vous combinez deux Serveurs d'administration dans une hiérarchie, assurez-vous que le port 13299 est accessible sur les deux Serveurs d'administration. Kaspersky Security Center Web Console se connecte au Serveur d'administration via le port 13299.

4. **Connexion des appareils administrés hors du bureau au Serveur d'administration secondaire**

   Vous pouvez connecter des appareils itinérants au Serveur d'administration dans la DMZ de la même manière qu'une connexion s'opère entre le Serveur d'administration et les appareils administrés dans le réseau principal. Les appareils administrés itinérants initient la connexion via le port 13000.

À propos de la connexion d'appareils itinérants

Certains appareils administrés se trouvent toujours en dehors du réseau principal (par exemple, les appareils dans les succursales régionales d'une entreprise ; les kiosques, les distributeurs de billets et les terminaux installés dans différents points de vente ; les appareils dans les bureaux à domicile des employés). Certains appareils sortent du périmètre de temps en temps (par exemple, les ordinateurs portables des utilisateurs qui visitent les succursales régionales ou le bureau d'un client).

Vous devez toujours surveiller et administrer la protection des appareils itinérants : recevoir des informations réelles sur leur état de la protection et maintenir leurs applications de sécurité à jour. Cela est nécessaire, car, par exemple, si un tel appareil est compromis alors qu'il est éloigné du réseau principal, il pourrait devenir une plateforme de propagation de menaces dès qu'il se connecte au réseau principal. Pour connecter des appareils itinérants au Serveur d'administration, vous pouvez utiliser deux méthodes :

- Passerelle de connexion dans la zone démilitarisée (DMZ)

  Voir le schéma de trafic de données : Serveur d'administration sur LAN, appareils administrés sur Internet, passerelle de connexion utilisée

- Serveur d'Administration dans la zone démilitarisée

  Voir le schéma de trafic de données : Serveur d'administration dans la DMZ, appareils administrés sur Internet.

Une passerelle de connexion dans la DMZ

Une méthode recommandée pour connecter des appareils itinérants au Serveur d'administration consiste à organiser une DMZ dans le réseau de l'organisation et à installer une passerelle de connexion dans la DMZ. Les appareils externes se connecteront à la passerelle de connexion, et le Serveur d'administration à l'intérieur du réseau amorcera la connexion aux appareils via la passerelle de connexion.

Par rapport à l'autre méthode, celle-ci est plus sécurisée :

- Il n'est pas nécessaire d'ouvrir l'accès au Serveur d'administration depuis l'extérieur du réseau.
- Une passerelle de connexion compromise ne présente pas un risque élevé pour la sécurité des appareils du réseau. Une passerelle de connexion ne gère rien elle-même et n'établit aucune connexion.

En outre, une passerelle de connexion ne nécessite pas de nombreuses ressources matérielles.

Cependant, cette méthode comporte un processus de configuration plus compliqué :

- Pour qu'un appareil serve de passerelle de connexion dans la DMZ, vous devez installer l'Agent d'administration et le connecter au Serveur d'administration d'une manière très spécifique.
- Vous ne pourrez pas utiliser la même adresse pour vous connecter au Serveur d'administration dans toutes les situations. De l'extérieur du périmètre, vous devrez utiliser non seulement une adresse différente (adresse de passerelle de connexion), mais également un mode de connexion différent : via une passerelle de connexion.
- Vous devez également définir différents paramètres de connexion pour les ordinateurs portables situés à différents endroits.

Pour ajouter une passerelle de connexion à un réseau précédemment configuré, procédez comme suit :

1. Installer l'Agent d'administration en mode passerelle de connexion.
2. Réinstallez l'Agent d'administration sur les appareils que vous souhaitez connecter à la passerelle de connexion récemment ajoutée.

Serveur d'administration dans la DMZ

Une autre méthode consiste à installer un seul Serveur d'administration dans la DMZ.

Cette configuration est moins sécurisée que l'autre méthode. Pour gérer les ordinateurs portables externes dans ce cas, le Serveur d'administration doit accepter les connexions de n'importe quelle adresse sur Internet. Il gérera toujours tous les ordinateurs du réseau interne, mais à partir de la DMZ. Par conséquent, un serveur compromis pourrait causer d'énormes dégâts, malgré la faible probabilité d'un tel événement.

Le risque diminue considérablement si le Serveur d'administration de la DMZ ne gère pas les appareils du réseau interne. Une telle configuration peut être utilisée, par exemple, par un fournisseur de services pour gérer les appareils des clients.

Cette méthode peut être intéressante dans les cas suivants :

- Si vous connaissez bien l'installation et la configuration du Serveur d'administration et que vous ne souhaitez pas effectuer une autre procédure pour installer et configurer une passerelle de connexion.
- Si vous avez besoin de gérer plus d'appareils. La capacité maximale du Serveur d'administration est de 100 000 appareils, tandis qu'une passerelle de connexion peut prendre en charge jusqu'à 10 000 appareils.

Cette solution présente également des difficultés possibles :

- Le Serveur d'administration nécessite plus de ressources matérielles et une base de données supplémentaire.
- Les informations sur les ordinateurs seront stockées dans deux bases de données indépendantes (pour le Serveur d'administration à l'intérieur du réseau et une autre dans la DMZ), ce qui complique la surveillance.
- Pour gérer tous les appareils, le Serveur d'administration doit être intégré dans une hiérarchie, ce qui complique non seulement la surveillance, mais également la gestion. Une instance de Serveur d'administration secondaire impose des limitations sur les structures possibles des groupes d'administration. Vous devez décider quelles tâches et stratégies distribuer à une instance de Serveur d'administration secondaire et la manière de le faire.
- La configuration des appareils externes pour utiliser le Serveur d'administration dans la DMZ depuis l'extérieur et pour utiliser le Serveur d'administration principal depuis l'intérieur n'est pas plus simple que la configuration pour utiliser une connexion conditionnelle via une passerelle.
- Risques de sécurité élevés. Une instance de Serveur d'administration compromise facilite la compromission de ses ordinateurs portables administrés. Si cela se produit, il suffit aux pirates informatiques d'attendre que l'un des ordinateurs portables revienne sur le réseau de l'entreprise afin de pouvoir continuer leur attaque sur le réseau local.

Connexion d'appareils de bureau externes au Serveur d'administration

Les appareils de bureau qui sont toujours en dehors du réseau principal (par exemple, les appareils dans les succursales régionales de l'entreprise ; les kiosques, les distributeurs de billets et les terminaux installés dans différents points de vente ; les appareils dans les bureaux à domicile des employés) ne peuvent pas être connectés directement au Serveur d'administration. Ils doivent être connectés au Serveur d'administration via une passerelle de connexion installée dans une zone démilitarisée (DMZ). Cette configuration est effectuée lors de l'installation de l'Agent d'administration sur ces appareils.

Pour connecter des appareils de bureau externes au Serveur d'administration, procédez comme suit :

1. Créez un paquet d'installation pour l'Agent d'administration.
2. Ouvrez les propriétés du paquet d'installation créé et accédez à **Paramètres** → **Avancé**, puis sélectionnez l'option **Se connecter au Serveur d'administration au moyen d'une passerelle de connexion**.

   Le paramètre **Se connecter au Serveur d'administration au moyen d'une passerelle de connexion** est incompatible avec le paramètre **Utiliser l'Agent d'administration en tant que passerelle de connexion en DMZ**. Vous ne pouvez pas activer ces deux paramètres en même temps.

3. Dans le champ **Adresse de la passerelle de connexion**, indiquez l'adresse publique de la passerelle de connexion.

   Si la passerelle de connexion se trouve derrière une Traduction d'adresses réseau (NAT) et ne dispose pas de sa propre adresse publique, configurez une règle de passerelle NAT pour transférer les connexions de l'adresse publique à l'adresse interne de la passerelle de connexion.

4. Créez un paquet d'installation autonome fondé sur le paquet d'installation créé.
5. Fournissez le paquet d'installation autonome aux appareils cibles par voie électronique ou au moyen d'un disque amovible.
6. Installez l'Agent d'administration à partir du paquet autonome.

Les appareils de bureau externes sont connectés au Serveur d'administration.

À propos des profils de connexion pour les utilisateurs itinérants

Le travail des utilisateurs itinérants avec des ordinateurs portables (ci-après, les " appareils ") peut imposer une modification du mode de connexion au Serveur d'administration ou la permutation entre les Serveurs d'administration en fonction de la situation actuelle de l'appareil sur le réseau.

Les profils des connexions ne sont pris en charge que pour les appareils fonctionnant sous Windows et macOS.

Utilisation de différentes adresses du même Serveur d'administration

Les appareils dotés de l'Agent d'administration peuvent, à différents moments, se connecter au Serveur d'administration depuis le réseau interne de l'entreprise ou depuis Internet. Dans ce cas, il peut être nécessaire que l'Agent d'administration utilise différentes adresses pour la connexion au Serveur d'administration : l'adresse externe du Serveur pour la connexion depuis Internet et l'adresse interne du Serveur pour la connexion depuis le réseau interne.

Pour cela, ajoutez un profil de connexion au Serveur d'administration depuis Internet dans les propriétés de la stratégie de l'Agent d'administration (dans la section **Paramètres de l'application → Connectivité → Profils de connexion → Profils de connexion au Serveur d'administration**). Dans la fenêtre de création de profil, désactivez l'option **Utiliser uniquement pour récupérer les mises à jour** et assurez-vous que l'option **Synchroniser les paramètres de connexion aux paramètres du Serveur d'administration indiqués dans ce profil** est sélectionnée. Si l'accès au Serveur d'administration s'opère via une passerelle de connexion (cf. la configuration de Kaspersky Security Center de type Accès depuis Internet : Agent d'administration en tant que passerelle de connexion dans la zone démilitarisée), il faut indiquer l'adresse de la passerelle dans le champ correspondant.

Permutation entre les Serveurs d'administration en fonction du réseau actuel

Si la société compte plusieurs bureaux avec différents Serveurs d'administration et qu'une partie des appareils dotés de l'Agent d'administration se déplace entre ceux-ci, il faut que l'Agent d'administration puisse se connecter au Serveur d'administration du réseau local du bureau dans lequel l'appareil se trouve.

Dans ce cas, créez un profil de connexion au Serveur d'administration dans les propriétés de la stratégie de l'Agent d'administration pour chacun des bureaux, à l'exception du siège social où se trouve le Serveur d'administration d'origine. Indiquez les adresses des Serveurs d'administration correspondants dans les profils de connexion et activer ou désactiver l'option **Utiliser uniquement pour récupérer les mises à jour** :

- Sélectionnez cette option si vous souhaitez que l'Agent d'administration soit synchronisé avec le Serveur d'administration domestique, tout en utilisant le Serveur local pour télécharger les mises à jour uniquement.
- Désactivez cette option si l'Agent d'administration doit être entièrement administré par le Serveur d'administration local.

Ensuite, il faut configurer les conditions de permutation vers les profils créés : pas moins d'une condition pour chacun des bureaux, à l'exclusion du "bureau domestique". L'idée de cette condition est de détecter dans l'environnement réseau des détails propres à un des bureaux. Si la condition se vérifie, le profil correspondant s'active. Si aucune des conditions ne se vérifie, l'Agent d'administration passe au Serveur d'administration domestique.

Création d'un profil de connexion pour les utilisateurs itinérants

Un profil de connexion au Serveur d'administration est disponible uniquement sur les appareils exécutés sous Windows et macOS.

Pour créer le profil de connexion de l'Agent d'administration au Serveur d'administration pour les utilisateurs itinérants, procédez comme suit :

1. Si vous souhaitez créer un profil de connexion pour un groupe d'appareils administrés, ouvrez la stratégie de l'Agent d'administration de ce groupe. Pour ce faire, procédez comme suit :

   a. Dans le menu principal, accédez à **Ressources (Appareils)** → **Stratégies et profils**.

   b. Cliquez sur le lien du chemin actuel.

   c. Dans la fenêtre qui s'ouvre, sélectionnez un groupe d'administration requis.

      Après cela, le chemin actuel est modifié.

   d. Ajoutez la stratégie de l'Agent d'administration pour le groupe d'appareils administrés. Si vous l'avez déjà créé, cliquez sur le nom de la stratégie de l'Agent d'administration pour ouvrir les propriétés de la stratégie.

2. Si vous souhaitez créer un profil de connexion pour un appareil administré spécifique, procédez comme suit :

   a. Dans le menu principal, accédez à **Ressources (Appareils)** → **Appareils administrés**.

   b. Cliquez sur le nom de l'appareil administré.

   c. Dans la fenêtre des propriétés de l'appareil administré qui s'ouvre, accédez à l'onglet **Applications**.

   d. Cliquez sur le nom de la stratégie de l'Agent d'administration à laquelle seul l'appareil administré sélectionné s'applique.

3. Dans la fenêtre des propriétés qui s'ouvre, accédez à **Paramètres de l'application** → **Connectivité** → **Profils de connexion.**

4. Dans la section **Profils de connexion au Serveur d'administration**, cliquez sur le bouton **Ajouter**.

   Par défaut, la liste des profils de connexion contient les profils <Offline mode> et <Home Administration Server>. Les profils ne peuvent être modifiés ou supprimés.

   Le profil <Offline mode> ne définit aucun serveur pour la connexion. Par conséquent, l'Agent d'administration, une fois transféré vers ce profil, ne tente aucune connexion à un Serveur d'administration quelconque tant que les applications installées sur les appareils clients utilisent les stratégies pour les utilisateurs itinérants. Le profil <Offline mode> est invoqué quand les appareils sont déconnectés du réseau.

   Le profil <Home Administration Server> spécifie la connexion pour le Serveur d'administration qui a été sélectionnée lors de l'installation de l'Agent d'administration. Le profil <Home Administration Server> est invoqué quand un appareil qui fonctionnait dans un autre réseau se connecte à nouveau au Serveur d'administration domestique.

5. Dans la fenêtre **Configurer le profil** qui s'ouvre, configurez les paramètres du profil de connexion :

   - **Nom du profil**

     Le champ de saisie permet de consulter ou de modifier le nom du profil de connexion.

   - **Adresse du Serveur d'administration**

     Adresse du Serveur d'administration auquel l'appareil client doit se connecter lors de l'activation du profil.

   - **Numéro de port**

     Numéro du port utilisé pour la connexion.

   - **Port SSL**

     Numéro de port utilisé pour la connexion par protocole SSL.

   - **Utiliser une connexion SSL**

     Si l'option est activée, la connexion aura lieu via un port sécurisé à l'aide du protocole SSL.

     Cette option est activée par défaut. Nous vous recommandons de ne pas désactiver cette option afin que votre connexion reste sécurisée.

   - Sélectionnez l'option **Utiliser un serveur proxy** si vous souhaitez utiliser un serveur proxy pour vous connecter à Internet. Si cette option est sélectionnée, les champs sont disponibles pour saisir les paramètres. Configurez les paramètres suivants de connexion au serveur proxy :

     - **Adresse**

       Adresse du serveur proxy pour la connexion de Kaspersky Security Center à Internet.

     - **Numéro de port**

       Numéro du port via lequel la connexion proxy à Kaspersky Security Center sera établie.

- **Authentification du serveur proxy**

  Si la case est cochée, les champs de saisie permettent d'indiquer les identifiants pour l'authentification sur le serveur proxy.

- **Nom d'utilisateur**

  Compte utilisateur sous lequel la connexion au serveur proxy est établie (ce champ est disponible si la case **Authentification du serveur proxy** est cochée).

- **Mot de passe**

  Mot de passe défini par l'utilisateur sous le compte duquel la connexion au serveur proxy est établie (ce champ est disponible si la case **Authentification du serveur proxy** est cochée).

  Pour voir le mot de passe saisi, cliquez sur le bouton **Afficher** et maintenez-le enfoncé aussi longtemps que vous en avez besoin.

- **Adresse de la passerelle de connexion**

  Adresse de la passerelle via laquelle la connexion entre les appareils clients et le Serveur d'administration s'opère.

- **Activer le mode de l'utilisateur autonome quand le Serveur d'administration n'est pas disponible**

  Cochez cette case afin que lors de la connexion, les applications installées sur un appareil client utilisent les profils de stratégie pour les appareils en mode de l'utilisateur autonome et les stratégies pour les utilisateurs itinérants si le Serveur d'administration est inaccessible. Si aucune stratégie pour les utilisateurs autonomes n'est définie pour l'application, c'est la stratégie active qui sera utilisée.

  Si l'option est activée, les applications utiliseront les stratégies actives.

  Celle-ci est décochée par défaut.

- **Utiliser uniquement pour récupérer les mises à jour**

  Si l'option est désactivée, le profil sera utilisé uniquement lors du téléchargement des mises à jour par les applications installées sur l'appareil client. Pour les autres opérations, la connexion au Serveur d'administration sera réalisée selon les paramètres de connexion d'origine définis lors de l'installation de l'Agent d'administration.

  Cette option est activée par défaut.

- **&Synchroniser les paramètres de connexion aux paramètres du Serveur d'administration indiqués dans ce profil**

Si l'option est activée, l'Agent d'administration se connecte au Serveur d'administration en utilisant les paramètres utilisés dans les propriétés du profil.

Si l'option est désactivée, l'Agent d'administration se connecte au Serveur d'administration en utilisant les paramètres d'origine définis lors de l'installation.

Cette option n'est accessible que si l'option **Utiliser uniquement pour récupérer les mises à jour** est désactivée.

Cette option est Inactif par défaut.

Finalement, le profil de connexion de l'Agent d'administration au Serveur d'administration pour les utilisateurs itinérants sera créé. Lors de la connexion de l'Agent d'administration au Serveur d'administration via ce profil de l'application, les applications installées sur l'appareil client utiliseront les stratégies pour les appareils en mode de l'utilisateur autonome et les stratégies pour les utilisateurs autonomes.

À propos du transfert de l'Agent d'administration à d'autres Serveurs d'administration

L'application Kaspersky Security Center prévoit la possibilité de transférer l'Agent d'administration sur un appareil client vers d'autres Serveurs d'administration en cas de modification des caractéristiques du réseau suivantes :

- **Condition de l'adresse du serveur DHCP** : modification de l'adresse IP du serveur DHCP (Dynamic Host Configuration Protocol) dans le réseau.
- **Condition de l'adresse de la passerelle de connexion par défaut** : modification de la passerelle principale du réseau.
- **Condition du domaine DNS** : modification du suffixe DNS du sous-réseau.
- **Condition de l'adresse du serveur DNS** : l'adresse IP du serveur DNS dans le réseau a été modifiée.
- **Condition de l'adresse du serveur WINS** : modification de l'adresse IP du serveur WINS dans le réseau. Ce paramètre est disponible uniquement pour les appareils exécutant Windows.
- **Condition de la résolution des noms** : le nom DNS ou NetBIOS de l'appareil client a changé.
- **Condition du sous-réseau** : modifie l'adresse et le masque du sous-réseau.
- **Condition de l'accessibilité du domaine Windows** : modification de l'état du domaine Windows auquel l'appareil client est connecté. Ce paramètre est disponible uniquement pour les appareils exécutant Windows.
- **Condition de l'accessibilité de l'adresse de connexion SSL** : l'appareil client peut ou ne peut pas (selon l'option sélectionnée) établir une connexion SSL avec un serveur défini (nom:port). Pour chaque serveur, vous pouvez également définir un certificat SSL. Dans ce cas, l'Agent d'administration vérifie le certificat du Serveur en plus de vérifier la capacité d'une connexion SSL. Si le certificat ne correspond pas, la connexion échoue.

Cette fonctionnalité est prise en charge uniquement pour les Agents d'administration installés sur des appareils fonctionnant sous Windows ou macOS.

Paramètres de connexion d'origine de l'Agent d'administration au Serveur d'administration lors de l'installation de l'Agent d'administration. Par la suite, quand des règles de permutation de l'Agent d'administration sur d'autres Serveurs d'administration sont rédigées, l'Agent d'administration réagit aux modifications des caractéristiques du réseau de la manière suivante :

- Si les caractéristiques du réseau correspondent à une des règles formées, l'Agent d'administration se connecte au Serveur d'administration indiqué dans cette règle. Si la règle le prévoit, les applications installées sur les appareils clients adopteront les stratégies pour les utilisateurs autonomes.
- Si une des règles n'est pas exécutée, l'Agent d'administration revient aux paramètres d'origine de connexion au Serveur d'administration définis lors de l'installation. Les applications installées sur les appareils clients reviennent aux stratégies actives.
- Si le Serveur d'administration est inaccessible, l'Agent d'administration utilise les stratégies pour les utilisateurs autonomes.

L'Agent d'administration bascule vers la stratégie pour les utilisateurs autonomes uniquement si l'option **Activer le mode de l'utilisateur autonome quand le Serveur d'administration n'est pas disponible** est activée dans les paramètres de la stratégie de l'Agent d'administration.

Les paramètres de connexion de l'Agent d'administration au Serveur d'administration sont préservés dans le profil de connexion. Le profil de connexion permet de créer des règles de permutation des appareils clients vers les stratégies pour les utilisateurs autonomes, ainsi que de configurer le profil de sorte qu'il soit uniquement utilisé pour le téléchargement des mises à jour.

Création d'une règle de permutation de l'Agent d'administration selon l'emplacement réseau

La permutation de l'Agent d'administration selon emplacement réseau est disponible uniquement sur les appareils tournant sous Windows ou macOS.

Afin de créer la règle de permutation de l'Agent d'administration d'un Serveur d'administration sur un autre, lors de la modification des caractéristiques du réseau, procédez comme suit :

1. Si vous souhaitez créer une règle pour un groupe d'appareils administrés, ouvrez la stratégie de l'Agent d'administration de ce groupe. Pour ce faire, procédez comme suit :

   a. Dans le menu principal, accédez à **Ressources (Appareils)** → **Stratégies et profils**.

   b. Cliquez sur le lien du chemin actuel.

   c. Dans la fenêtre qui s'ouvre, sélectionnez un groupe d'administration requis.

      Après cela, le chemin actuel est modifié.

   d. Ajoutez la stratégie de l'Agent d'administration pour le groupe d'appareils administrés. Si vous l'avez déjà créé, cliquez sur le nom de la stratégie de l'Agent d'administration pour ouvrir les propriétés de la stratégie.

2. Si vous souhaitez créer une règle pour un appareil administré spécifique, procédez comme suit :

   a. Dans le menu principal, accédez à **Ressources (Appareils)** → **Appareils administrés**.

   b. Cliquez sur le nom de l'appareil administré.

   c. Dans la fenêtre des propriétés de l'appareil administré qui s'ouvre, accédez à l'onglet **Applications**.

   d. Cliquez sur le nom de la stratégie de l'Agent d'administration à laquelle seul l'appareil administré sélectionné s'applique.

3. Dans la fenêtre des propriétés qui s'ouvre, accédez à **Paramètres de l'application** → **Connectivité** → **Profils de connexion.**

4. Dans le groupe **Paramètres d'emplacement réseau**, cliquez sur le bouton **Ajouter**.

5. Dans la fenêtre des propriétés qui s'ouvre, configurez la description de l'emplacement réseau et la règle de permutation. Configurez les paramètres suivants de la description de l'emplacement de réseau :

   - **Description**

     Le nom de la descriptions de l'emplacement réseau ne peut pas contenir plus de 255 caractères, ni contenir les caractères spéciaux ("*<>?\/:|).

   - **Utiliser le profil de connexion**

     La liste déroulante permet de sélectionner le profil de connexion de l'Agent d'administration au Serveur d'administration. Le profil est utilisé quand les conditions de la description de l'emplacement réseau sont remplies. Le profil de connexion contient les paramètres de connexion de l'Agent d'administration au Serveur d'administration et définit le transfert des appareils clients aux stratégies pour les utilisateurs itinérants. Le profil est utilisé uniquement pour télécharger les mises à jour.

   - **La description est active**

     Cochez cette case pour activer l'utilisation de la nouvelle description de l'emplacement réseau.

6. Sélectionnez les conditions de la règle de changement de l'Agent d'administration :

   - **Condition de l'adresse du serveur DHCP** : modification de l'adresse IP du serveur DHCP (Dynamic Host Configuration Protocol) dans le réseau.
   - **Condition de l'adresse de la passerelle de connexion par défaut** : modification de la passerelle principale du réseau.
   - **Condition du domaine DNS** : modification du suffixe DNS du sous-réseau.
   - **Condition de l'adresse du serveur DNS** : l'adresse IP du serveur DNS dans le réseau a été modifiée.
   - **Condition de l'adresse du serveur WINS** : modification de l'adresse IP du serveur WINS dans le réseau. Ce paramètre est disponible uniquement pour les appareils exécutant Windows.
   - **Condition de la résolution des noms** : le nom DNS ou NetBIOS de l'appareil client a changé.
   - **Condition du sous-réseau** : modifie l'adresse et le masque du sous-réseau.
   - **Condition de l'accessibilité du domaine Windows** : modification de l'état du domaine Windows auquel l'appareil client est connecté. Ce paramètre est disponible uniquement pour les appareils exécutant Windows.
   - **Condition de l'accessibilité de l'adresse de connexion SSL** : l'appareil client peut ou ne peut pas (selon l'option sélectionnée) établir une connexion SSL avec un serveur défini (nom:port). Pour chaque serveur, vous pouvez également définir un certificat SSL. Dans ce cas, l'Agent d'administration vérifie le certificat du Serveur en plus de vérifier la capacité d'une connexion SSL. Si le certificat ne correspond pas, la connexion échoue.

   Les conditions dans une règle sont réunies via l'opérateur logique "ET". Pour que la règle de permutation selon la description de l'emplacement de réseau fonctionne, toutes les conditions de permutation de la règle doivent être remplies.

7. Dans la section du choix de condition, indiquez quand l'Agent d'administration doit basculer sur un autre Serveur d'administration. Pour ce faire, cliquez sur le bouton **Ajouter**, puis définissez la valeur de la condition.

   De plus, l'option **Correspond à au moins une valeur de la liste** est activée par défaut. Vous pouvez désactiver cette option si vous souhaitez que la condition soit remplie avec toutes les valeurs spécifiées.

8. Enregistrez vos modifications.

Ceci débouche sur la création d'une règle de permutation selon la description de l'emplacement réseau que l'Agent d'administration va utiliser, quand les conditions sont remplies, pour établir la connexion au Serveur d'administration renseigné dans la description du profil de connexion.

Assistant de déploiement de la protection

Pour installer les applications de Kaspersky, vous pouvez utiliser l'assistant de déploiement de la protection. L'Assistant de déploiement de la protection permet de réaliser l'installation à distance des applications, en utilisant les paquets d'installation formés ou directement depuis un paquet de distribution.

L'Assistant de déploiement de la protection effectue les actions suivantes :

- Télécharge un paquet d'installation pour installer l'application (s'il n'a pas été créé auparavant). Le paquet d'installation est situé dans **Découverte et déploiement** → **Déploiement et attribution** → **Paquets d'installation**. Vous pouvez utiliser ce paquet d'installation pour installer l'application ultérieurement.

- Crée et lance la tâche d'installation à distance pour un ensemble d'appareils ou pour un groupe d'administration. La tâche d'installation à distance nouvellement créée est stockée dans la section **Tâches**. Vous pouvez manuellement lancer cette tâche par la suite. Le type de tâche est **Installation à distance d'une application**.

Si vous souhaitez installer l'Agent d'administration sur des appareils dotés du système d'exploitation SUSE Linux Enterprise Server 15, installer le paquet insserv-compat en premier pour configurer l'Agent d'administration.

Étape 1. Démarrage de l'assistant de déploiement de la protection

Pour lancer manuellement l'assistant de déploiement de la protection, procédez comme suit

Dans le menu principal, accédez à **Découverte et déploiement** → **Déploiement et attribution** → **Assistant de déploiement de la protection**.

L'Assistant de déploiement de la protection démarre. Parcourez les étapes de l'assistant à l'aide du bouton **Suivant**.

Étape 2. Sélection du paquet d'installation

Sélectionnez le paquet d'installation de l'application que vous souhaitez installer.

Si le paquet d'installation de l'application en question ne figure pas dans la liste, cliquez sur le bouton **Ajouter**, puis sélectionnez l'application dans la liste.

Étape 3. Sélection d'une méthode pour la distribution du fichier clé ou du code d'activation

Sélectionnez une méthode pour la distribution du fichier clé ou du code d'activation :

- **Ne pas ajouter une clé de licence au paquet d'installation**

  La clé est diffusée automatiquement à tous les appareils avec lesquels elle est compatible :

  - Si la diffusion automatique est activée dans les propriétés de la clé.
  - Si la tâche **Ajout de la clé** est créée.

- **Ajouter une clé de licence au paquet d'installation**

  La clé est diffusée sur les appareils avec le paquet d'installation.

  Il n'est pas recommandé de distribuer la clé à l'aide de cette méthode, car les droits d'accès en lecture partagés sont activés sur le référentiel des paquets d'installation.

Si un fichier clé ou un code d'activation entre dans la composition du paquet d'installation, cette fenêtre est affichée, mais ne contient que les informations sur la clé de licence.

Étape 4. Sélection de la version de l'Agent d'administration

Si vous avez sélectionné le paquet d'installation d'une application autre que l'agent d'administration, vous devez aussi installer l'agent d'administration qui connecte l'application au serveur d'administration de Kaspersky Security Center.

Sélectionnez la dernière version de l'agent d'administration.

Étape 5. Sélection des appareils

Composez une liste d'appareils sur lesquels l'application va être installée :

- **Installer sur les appareils administrés**

  Si cette option a été sélectionnée, la tâche d'installation à distance de l'application sera créée pour le groupe des appareils.

- **Sélectionner les appareils à installer**

  La tâche est affectée aux appareils qui appartiennent à une sélection d'appareils. Vous pouvez définir une des sélections existantes.

  Par exemple, vous pourriez souhaiter utiliser cette option pour exécuter une tâche sur des appareils dotés d'une version du système d'exploitation spécifique.

Étape 6. Indiquez les paramètres de la tâche d'installation à distance

Sur la page **Paramètres de la tâche d'installation à distance**, configurez les paramètres de l'installation à distance de l'application.

Le groupe de paramètres **Forcer le téléchargement du paquet d'installation** permet de sélectionner le mode d'envoi des fichiers nécessaires pour l'installation de l'application sur les appareils clients :

- **En utilisant l'Agent d'administration**

  Si l'option est activée, l'Agent d'administration installé sur les appareils clients fournit les paquets d'installation à ces derniers.

  Si cette option est désactivée, les paquets d'installation sont fournis à l'aide des outils du système d'exploitation des appareils client.

  Il est recommandé d'activer cette option si la tâche concerne des appareils sur lesquels un Agent d'administration est installé.

  Cette option est activée par défaut.

- **En utilisant les ressources du système d'exploitation via les points de distribution**

  Si l'option est activée, les paquets d'installation sont transmis sur les appareils clients via les outils du système d'exploitation par les points de distribution. Cette option peut être sélectionnée si au moins un point de distribution se trouve sur le réseau.

  Si l'option **À l'aide de l'Agent d'administration** est activée, les fichiers seront livrés via les outils du système d'exploitation uniquement dans le cas où il n'est pas possible d'utiliser les moyens de l'Agent d'administration.

  Par défaut, l'option est activée pour les tâches d'installation à distance créées sur le Serveur d'administration virtuel.

- **En utilisant les ressources du système d'exploitation via le Serveur d'administration**

  Si cette option est activée, les fichiers sont transmis aux appareils clients à l'aide des outils du système d'exploitation des appareils clients via le Serveur d'administration. Cette option peut être activée si l'Agent d'administration n'est pas installé sur l'appareil client, mais que l'appareil client fait partie du même réseau que le Serveur d'administration.

  Cette option est activée par défaut.

Configurez les paramètres avancés :

- **Ne pas réinstaller l'application si elle est déjà installée**

  Si l'option est activée, l'application sélectionnée n'est pas installé à nouveau, si l'appareil client en est déjà équipé.

  Si l'option est désactivée, l'application sera malgré tout installée.

  Cette option est activée par défaut.

- **Réparer l'installation du paquet d'installation dans les stratégies de groupe d'Active Directory**

  Si l'option est activée, le paquet d'installation s'installera à l'aide des stratégies de groupes Active Directory.

  L'option est disponible si le paquet d'installation de l'Agent d'administration est sélectionné.

  Cette option est Inactif par défaut.

Étape 7. Administration du redémarrage

Définir l'action à appliquer s'il faut redémarrer le système d'exploitation pendant l'installation de l'application.

- **Ne pas redémarrer l'appareil**

  Les appareils clients ne redémarrent pas automatiquement après l'opération. Pour arrêter le fonctionnement, il faut redémarrer l'appareil (par exemple, manuellement ou à l'aide d'une tâche d'administration des appareils). Les informations sur la nécessité du redémarrage sont enregistrées dans les résultats de la tâche et dans l'état de l'appareil. Cette option convient aux tâches d' sur les serveurs et autres appareils pour lesquels la continuité des opérations est critique.

- **Redémarrer l'appareil**

  Dans ce cas, le redémarrage des appareils clients est toujours exécuté automatiquement, si celui-ci est requis pour terminer l'opération. Cette option convient aux tâches d' sur des appareils pour lesquels des interruptions périodiques sont admises (débranchement, redémarrage).

- **Confirmer l'action auprès de l'utilisateur**

  Le message qui signale que l'appareil client doit être redémarré manuellement s'affiche sur l'écran de l'appareil. Pour cette option, il est possible de configurer des paramètres avancés : le texte du message pour l'utilisateur, la fréquence du message, ainsi que le délai à l'issue duquel le redémarrage sera forcé (sans confirmation de l'utilisateur). Cette option convient le mieux pour les postes de travail sur lesquels les utilisateurs doivent pouvoir sélectionner l'heure de redémarrage qui leur convient le mieux.

  Cette option est sélectionnée par défaut.

  - **Répéter la demande toutes les (min.)**

    Quand cette option est activée, l'application invite l'utilisateur à redémarrer le système d'exploitation selon la fréquence indiquée.

    Cette option est activée par défaut. L'intervalle par défaut est de 5 minutes. La valeur peut être comprise entre 1 et 1 440 minutes.

    Si cette option est désactivée, l'invite est affichée une seule fois.

  - **Redémarrer le système au bout de (min.)**

    Après avoir averti l'utilisateur, l'application force le redémarrage du système d'exploitation à l'issue de l'intervalle défini.

    Cette option est activée par défaut. Le délai par défaut est de 30 minutes. La valeur peut être comprise entre 1 et 1 440 minutes.

- **Forcer la fermeture des applications dans les sessions bloquées**

  Les applications en cours d'exécution peuvent empêcher le redémarrage de l'appareil client. Par exemple, si un document est en train d'être modifié dans un logiciel de traitement de texte et qu'il n'est pas enregistré, l'application n'autorise pas le redémarrage de l'appareil.

  Quand cette option est activée, l'arrêt forcé de ces applications sur un appareil verrouillé doit avoir lieu avant de pouvoir redémarrer l'appareil. Les utilisateurs pourraient perdre toute modification qui n'a pas été enregistrée à ce moment.

  Si cette option est désactivée, un appareil verrouillé n'est pas redémarré. L'état de la tâche sur cet appareil indique qu'il faut redémarrer l'appareil. Les utilisateurs doivent quitter manuellement toutes les applications en cours d'exécution sur les appareils verrouillés, puis redémarrer ces appareils.

  Cette option est Inactif par défaut.

Étape 8. Suppression des applications incompatibles avant l'installation

Cette étape est présente uniquement si l'application que vous déployez est incompatible avec d'autres applications.

Sélectionnez cette option si vous souhaitez que Kaspersky Security Center supprime automatiquement les applications incompatibles avec l'application que vous déployez.

La liste des applications incompatibles s'affiche aussi.

Si vous ne sélectionnez pas cette option, l'application ne sera installée que sur des appareils dont aucune application n'est incompatible.

Étape 9. Déplacement des appareils vers Appareils administrés

Indiquez si les appareils doivent être déplacés vers un groupe d'administration après l'installation de l'agent d'administration.

- **Ne pas déplacer les appareils**

  Les appareils demeurent dans les groupes où ils se trouvent. Les appareils qui n'ont été placés dans aucun groupe restent non définis.

- **Déplacer les appareils non définis dans un groupe**

  Les appareils sont déplacés vers le groupe d'administration que vous avez sélectionné.

L'option **Ne pas déplacer les appareils** est sélectionnée par défaut. Pour des raisons de sécurité, envisagez de déplacer les appareils manuellement.

Étape 10. Sélection des comptes pour accéder aux appareils

Si nécessaire, ajoutez les comptes utilisateurs qui seront utilisés pour démarrer la tâche d'installation à distance :

- **Compte utilisateur non requis (Agent d'administration installé)**

  Si cette option est sélectionnée, il n'est pas nécessaire d'indiquer le compte utilisateur au nom duquel l'installateur de l'application sera lancé. La tâche est lancée sous le même compte utilisateur que le compte du service du Serveur d'administration.

  Si l'agent d'administration n'est pas installé sur les appareils clients, l'option n'est pas disponible.

- **Compte utilisateur requis (Agent d'administration non utilisé)**

Sélectionnez cette option si l'Agent d'administration n'est pas installé sur les appareils pour lesquels vous affectez la tâche d'installation à distance. Dans ce cas, vous pouvez spécifier un compte utilisateur ou un certificat SSH pour installer l'application.

- **Compte utilisateur local**. Si cette option est sélectionnée, spécifiez le compte utilisateur sous lequel le programme d'installation de l'application sera exécuté. Cliquez sur le bouton **Ajouter**, sélectionnez **Compte utilisateur local**, puis indiquez les informations d'identification du compte utilisateur.

  Vous pouvez désigner plusieurs comptes utilisateurs si aucun d'entre eux ne possède les privilèges nécessaires sur tous les appareils auxquels vous affectez la tâche. Dans ce cas, tous les comptes ajoutés sont utilisés pour exécuter la tâche, dans un ordre consécutif, de haut en bas.

- **Certificat SSH**. Si vous souhaitez installer l'application sur un appareil client basé sur Linux, vous pouvez indiquer un certificat SSH au lieu d'un compte utilisateur. Cliquez sur le bouton **Ajouter**, sélectionnez **Certificat SSH**, puis indiquez les clés privée et publique du certificat.

  Pour générer une clé privée, vous pouvez utiliser l'utilitaire ssh-keygen. Notez que Kaspersky Security Center prend en charge le format PEM des clés privées, mais que l'utilitaire ssh-keygen génère par défaut des clés SSH au format OPENSSH. Le format OPENSSH n'est pas pris en charge par Kaspersky Security Center. Pour créer une clé privée au format PEM pris en charge, ajoutez l'option -m PEM dans la commande ssh-keygen. Par exemple :

  ```
  ssh-keygen -m PEM -t rsa -b 4096 -C "<user email>"
  ```

Étape 11. Démarrage de l'installation

Cette page est la dernière étape de l'assistant. À cette étape, la **Tâche d'installation à distance** a été créée et configurée avec succès.

Par défaut, l'option **Lancer la tâche à la fin de l'Assistant** n'est pas sélectionnée. Si vous sélectionnez cette option, la **Tâche d'installation à distance** démarre immédiatement après la fin de l'assistant. Si vous ne sélectionnez pas cette option, la **Tâche d'installation à distance** ne démarre pas. Vous pouvez manuellement lancer cette tâche par la suite.

Cliquez sur **OK** pour terminer l'étape finale de l'assistant de déploiement de la protection.

Déploiement d'applications Kaspersky dans Kaspersky Security Center Web Console

Cette section explique comment déployer les applications Kaspersky sur les appareils clients dans votre organisation administrés par Kaspersky Security Center Web Console.

Scénario : déploiement d'applications Kaspersky dans Kaspersky Security Center Web Console

Ce scénario explique comment déployer les applications Kaspersky via Kaspersky Security Center Web Console. Vous pouvez utiliser l'Assistant de configuration initiale de l'application et l'Assistant de déploiement de la protection ou vous pouvez réaliser les étapes nécessaires manuellement.

Les applications suivantes sont disponibles pour le déploiement par Kaspersky Security Center Web Console :

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Linux

Étapes

Le déploiement des applications Kaspersky se déroule par étapes :

1. **Téléchargement du plug-in d'administration pour l'application**

   Cette étape est gérée par l'Assistant de configuration initiale de l'application. Si vous décidez de ne pas lancer l'assistant, téléchargez le plug-in pour Kaspersky Endpoint Security for Windows manuellement.

   Si vous prévoyez d'administrer des appareils mobiles d'entreprise, suivez les instructions fournies dans l'aide de Kaspersky Security for Mobile pour télécharger et installer les plug-ins d'administration de Kaspersky Endpoint Security for Android.

2. **Téléchargement et création des paquet d'installation**

   Cette étape est gérée par l'Assistant de configuration initiale de l'application.

   L'Assistant de configuration initiale de l'application vous permet de télécharger le paquet d'installation avec le plug-in d'administration. Si vous n'aviez pas choisi cette option lors de l'exécution de l'Assistant ou si vous n'aviez pas exécuté l'Assistant, vous devez télécharger le paquet manuellement.

   Si vous ne pouvez pas installer les applications Kaspersky au moyen de Kaspersky Security Center sur certains appareils, par exemple sur les appareils des employés distants, vous pouvez créer des paquets d'installation autonomes pour les applications. Si vous utilisez des paquets autonomes pour installer les applications Kaspersky, vous n'avez pas besoin de créer et d'exécuter une tâche d'installation à distance, ni de créer et de configurer des tâches pour Kaspersky Endpoint Security for Windows.

3. **Création, configuration et exécution d'une tâche d'installation à distance**

   Pour Kaspersky Endpoint Security for Windows, cette étape fait partie de l'Assistant de déploiement de la protection qui démarre automatiquement une fois l'Assistant de configuration initiale de l'application terminé. Si vous décidez de ne pas exécuter l'Assistant de déploiement de la protection, vous devez créer cette tâche manuellement et la configurer manuellement.

   Vous pouvez créer manuellement plusieurs tâches d'installation à distance pour différents groupes d'administration ou différentes sélections d'appareils. Vous pouvez aussi déployer différentes versions d'une application dans ces tâches.

   Vérifiez que tous les appareils du réseau sont détectés, puis exécutez l'installation à distance de la ou des tâches.

   > Installez l'utilitaire nmap sur vos ressources fonctionnant sous Linux. Cet utilitaire est requis pour activer la fonctionnalité Reconnaissance de l'emplacement réseau.

Si vous souhaitez installer l'Agent d'administration sur des appareils dotés du système d'exploitation SUSE Linux Enterprise Server 15, installer le paquet insserv-compat en premier pour configurer l'Agent d'administration.

Si vous souhaitez installer l'Agent d'administration sur des appareils qui utilisent le système d'exploitation RED OS 7.3.4 ou une version ultérieure ou MSVSPHERE 9.2 ou une version ultérieure, installez le paquet libxcrypt-compat pour assurer le bon fonctionnement de l'Agent d'administration.

4. **Création et configuration de tâches pour l'application administrée**

   La *tâche Installer la mise à jour* de Kaspersky Endpoint Security for Windows doit être configurée.

   Cette étape fait partie de l'Assistant de configuration initiale de l'application : la tâche est créée et configurée automatiquement selon les paramètres par défaut. Si vous n'avez pas exécuté l'Assistant, vous devez créer ces tâches manuellement et les configurer manuellement. Si vous utilisez l'Assistant de configuration initiale de l'application, confirmez que la programmation des tâches répond à vos exigences. (Par défaut, la programmation des tâches est **Manuelle**, mais vous pouvez choisir une autre option.)

   D'autres applications de Kaspersky peuvent avoir d'autres tâches par défaut. Consultez la documentation des applications concernées pour en savoir plus.

   Assurez-vous que la programmation pour chaque tâche que vous créez répond à vos exigences.

5. **Installation de Kaspersky Security for Mobile (facultatif)**

   Si vous prévoyez d'administrer des appareils mobiles d'entreprise, suivez les instructions fournies dans l'aide de Kaspersky Security for Mobile pour obtenir plus d'informations sur le déploiement de Kaspersky Endpoint Security for Android.

6. **Création des stratégies**

   Créez la stratégie pour chaque application manuellement ou (avec Kaspersky Endpoint Security for Windows) par l'Assistant de configuration initiale de l'application. Vous pouvez utiliser les paramètres par défaut de la stratégie ; vous pouvez aussi modifier les paramètres par défaut de la politique en fonction de vos besoins à tout moment.

7. **Contrôle des résultats**

   Confirmez que le déploiement a réussi : vous avez des stratégies et des tâches pour chaque application, et ces applications sont installées sur les appareils administrés.

Résultats

La réalisation du scénario donne les résultats suivants :

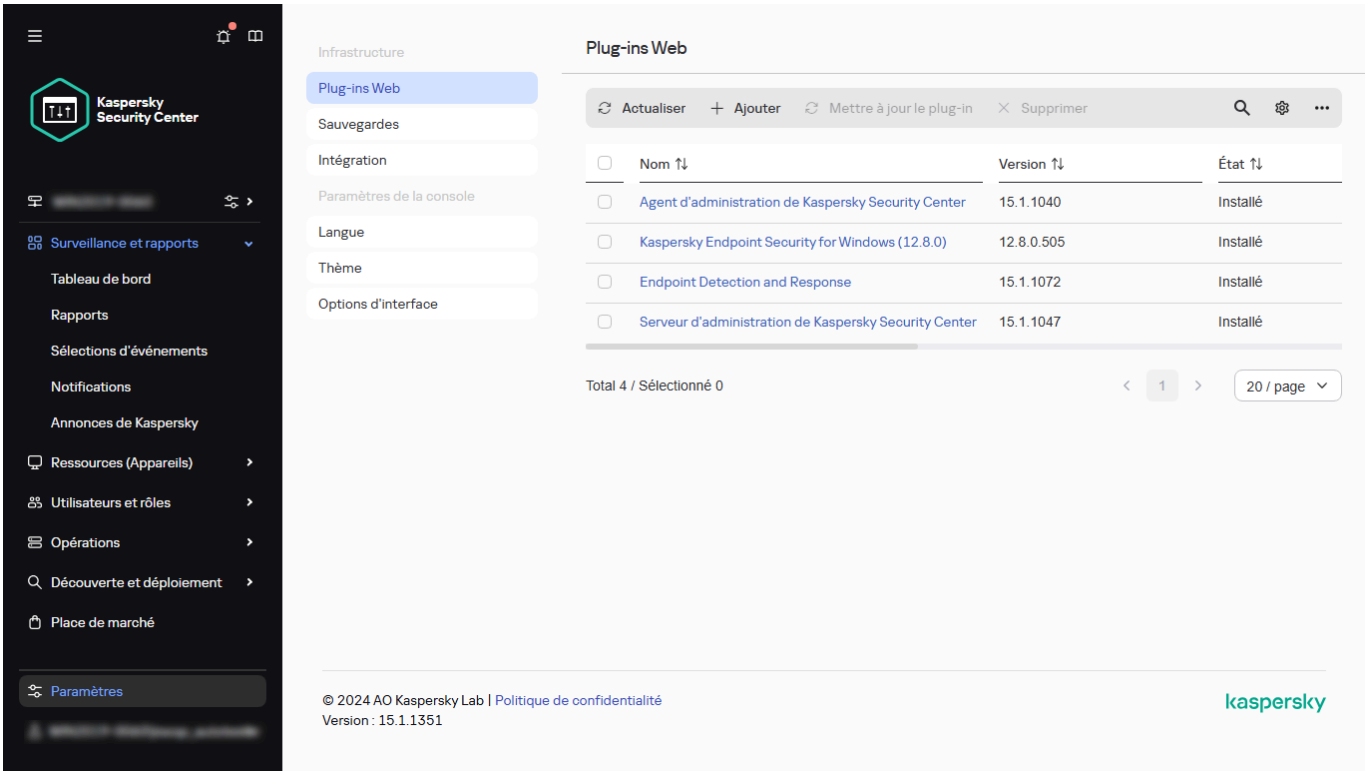
- Toutes les stratégies et les tâches requises pour les applications sont créées.
- Les programmes de tâches sont configurés en fonction de vos besoins.
- Les applications sélectionnées sont déployé ou son déploiement est programmé sur les appareils clients sélectionnés.

Obtention des plug-ins pour les applications de Kaspersky

Pour déployer une application de Kaspersky comme Kaspersky Endpoint Security for Windows, vous devez télécharger le plug-in d'administration pour l'application.

Pour télécharger un plug-in d'administration pour une applications de Kaspersky, procédez comme suit :

1. Dans le menu principal, accédez à **Paramètres** → **Plug-ins Web**.



La liste des plug-ins Internet installés

2. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Ajouter**.

   Une liste des plug-ins disponibles s'affiche.

3. Dans la liste des plug-ins disponibles, sélectionnez le plug-in que vous souhaitez télécharger (par exemple, Kaspersky Endpoint Security 11 for Windows) en cliquant sur son nom.

   Une page de description du plug-in s'affiche.

4. Sur la page de description du plug-in, cliquez sur **Installer le plug-in**.

5. Une fois l'installation terminée, cliquez sur **OK**.

Le plug-in d'administration est téléchargé avec la configuration par défaut et s'affiche dans la liste des plug-ins d'administration.

Vous pouvez ajouter des plug-ins et mettre à jour les plug-ins téléchargés à partir d'un fichier. Vous téléchargez des plug-ins d'administration et des plug-ins d'administration Web à partir de la page du Support Technique de Kaspersky.

Pour télécharger ou mettre à jour le plug-in à partir d'un fichier :

1. Dans le menu principal, accédez à **Paramètres** → **Plug-ins Web**.
2. Exécutez une des actions suivantes :
   - Cliquez sur **Ajouter à partir d'un fichier** pour télécharger un plug-in à partir d'un fichier.
   - Cliquez sur **Mettre à jour à partir d'un fichier** pour télécharger la mise à jour d'un plug-in à partir d'un fichier.
3. Indiquez le fichier et la signature du fichier.
4. Télécharger les fichiers indiqués.

Le plug-in d'administration est téléchargé à partir du fichier et s'affiche dans la liste des plug-ins d'administration.

Téléchargement et création des paquets d'installation pour les applications de Kaspersky

Vous pouvez créer des paquets d'installation des applications pour Kaspersky sur les serveurs Internet de Kaspersky si votre Serveur d'administration a accès à Internet.

Pour télécharger et créer un paquet d'installation pour l'application Kaspersky, procédez comme suit :

1. Exécutez une des actions suivantes :
   - Dans le menu principal, accédez à **Découverte et déploiement** → **Déploiement et attribution** → **Paquets d'installation**.
   - Dans le menu principal, accédez à **Opérations** → **Stockages** → **Paquets d'installation**.

   Vous pouvez également consulter des notifications sur les nouveaux paquets pour les applications Kaspersky dans la liste des notifications à l'écran. Si des notifications sur un nouveau paquet sont présentes, vous pouvez cliquer sur le lien en regard de la notification et accéder à la liste des paquets d'installation disponibles.

   Une liste des paquets d'installation disponibles sur le Serveur d'administration s'affiche.
2. Cliquez sur **Ajouter**.

   L'Assistant de création du paquet d'installation se lance. Parcourez les étapes de l'assistant à l'aide du bouton **Suivant**.
3. Sélectionnez **Générer un paquet d'installation pour une application Kaspersky**.

   Une liste des paquets d'installation disponibles sur les serveurs Web de Kaspersky apparaît. La liste contient uniquement les paquets d'installation des applications compatibles avec la version actuelle de Kaspersky Security Center.

4. Cliquez sur le nom d'un paquet d'installation, par exemple, Kaspersky Endpoint Security for Windows (11.1.0).

   Une fenêtre s'ouvre avec des informations sur le paquet d'installation.

   > Vous pouvez télécharger et utiliser un paquet d'installation qui comprend des outils de chiffrement qui mettent en œuvre un chiffrement fort, s'il est conforme aux lois et réglementations applicables. Pour télécharger un paquet d'installation de Kaspersky Endpoint Security for Windows valable pour les besoins de votre organisation, consultez la législation du pays où se trouvent les appareils clients de votre organisation.

5. Lisez les informations et cliquez sur le bouton **Télécharger et créer le paquet d'installation**.

   Si un paquet de distribution ne peut pas être converti en un paquet d'installation, le bouton **Télécharger le paquet de distribution** s'affiche à la place du bouton **Télécharger et créer le paquet d'installation**.

   Le téléchargement du paquet d'installation sur le Serveur d'administration commence. Vous pouvez fermer la fenêtre de l'Assistant ou passer à l'étape suivante de l'instruction. Si vous fermez la fenêtre de l'assistant, le processus de téléchargement se poursuivra en arrière-plan.

   Si vous souhaitez suivre le processus de téléchargement d'un paquet d'installation, procédez comme suit :

   a. Dans le menu principal, accédez à **Opérations** → **Stockages** → **Paquets d'installation** → **En cours ()**.

   b. Suivez la progression de l'opération dans la colonne **Progression du téléchargement** et dans la colonne **État de téléchargement** du tableau.

   Une fois le processus terminé, le paquet d'installation est ajouté à la liste sous l'onglet **Téléchargé**. Si le processus de téléchargement s'arrête et que l'état du téléchargement passe à **Accepter le CLUF**, cliquez sur le nom du paquet d'installation, puis passez à l'étape suivante de l'instruction.

   > Si la taille des données contenues dans le paquet de distribution sélectionné dépasse la limite actuelle, un message d'erreur s'affiche. Vous pouvez modifier la valeur limite, puis poursuivre la création du paquet d'installation.

6. Pour certaines applications de Kaspersky, le bouton **Afficher le CLUF** s'affiche pendant le téléchargement. Si c'est le cas, procédez comme suit :

   a. Cliquez sur le bouton **Afficher le CLUF** pour lire le contrat de licence utilisateur final (CLUF).

   b. Lisez le CLUF affiché à l'écran, puis cliquez sur **Accepter**.

      L'installation se poursuit après que vous avez accepté le CLUF. Si vous cliquez sur **Refuser**, le téléchargement cesse.

7. Une fois le téléchargement terminé, cliquez sur le bouton **Fermer**.

Le paquet d'installation sélectionné est téléchargé dans le dossier partagé du Serveur d'administration, dans le sous-dossier Packages. Après le téléchargement, le paquet d'installation s'affiche dans la liste des paquets d'installation.

Modification de la limite de la taille des données du paquet d'installation personnalisé

La taille totale des données décompressées lors de la création d'un paquet d'installation personnalisé est limitée. La limite par défaut est de 1 Go.

Si vous essayez de charger un fichier d'archive contenant des données dépassant la limite actuelle, un message d'erreur s'affiche. Vous devrez peut-être augmenter cette valeur limite lors de la création de paquets d'installation à partir de paquets de distribution volumineux.

Pour modifier la valeur limite de la taille du paquet d'installation personnalisé, procédez comme suit :

1. Sur l'appareil du Serveur d'administration, exécutez l'invite de commande sous le compte utilisé pour installer le Serveur d'administration.

2. Remplacez votre répertoire actuel par le dossier d'installation de Kaspersky Security Center (généralement, <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center).

3. Selon le type d'installation du serveur d'administration, saisissez l'une des commandes suivantes avec les privilèges d'administrateur :

   - Installation locale normale :

     ```
     klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v <nombre d'octets>
     ```

   - Installation sur le cluster de basculement Kaspersky Security Center :

     ```
     klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v <nombre d'octets> --stp klfoc
     ```

   - Installation sur le cluster de basculement Windows Server :

     ```
     klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v <nombre d'octets> --stp cluster
     ```

   Où <nombre d'octets> est un nombre d'octets au format hexadécimal ou décimal.

   Par exemple, si la limite requise est de 2 Go, vous pouvez spécifier la valeur décimale 2147483648 ou la valeur hexadécimale 0x80000000. Dans ce cas, pour une installation locale du Serveur d'administration, vous pouvez utiliser la commande suivante :

   ```
   klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v 2147483648
   ```

La limite de la taille des données du paquet d'installation personnalisé est modifiée.

Téléchargement d'un paquet de distribution pour les applications Kaspersky

Dans Kaspersky Security Center Web Console, vous pouvez télécharger et sauvegarder des paquets de distribution pour les applications de Kaspersky. Vous pouvez utiliser les paquets de distribution pour installer les applications manuellement, sans utiliser Kaspersky Security Center.

Pour télécharger et sauvegarder des paquets de distribution pour les applications de Kaspersky :

1. Dans le menu principal, accédez à **Opérations → Applications Kaspersky → Versions actuelles des applications**.

   Une liste des paquets de distribution, plug-ins et correctifs disponibles s'ouvre. Kaspersky Security Center n'affiche que les éléments compatibles avec sa version actuelle.

2. Dans la liste, cliquez sur le nom du paquet que vous souhaitez modifier.

   La description du paquet s'ouvre.

3. Lisez la description et cliquez sur le bouton **Télécharger et créer le paquet d'installation**.

   Si un paquet de distribution ne peut pas être converti en un paquet d'installation, le bouton **Télécharger le paquet de distribution** s'affiche à la place du bouton **Télécharger et créer le paquet d'installation**.

   Le téléchargement du paquet d'installation sur le Serveur d'administration commence.

Le paquet d'installation ou de distribution sélectionné est téléchargé dans le dossier partagé du Serveur d'administration, dans le sous-dossier **Packages**. Après le téléchargement, le paquet d'installation apparaît dans la liste des paquets d'installation.

Vérification du bon déploiement de Kaspersky Endpoint Security

Vérifiez que vous avez correctement déployé les applications Kaspersky, comme Kaspersky Endpoint Security :

1. Avec Kaspersky Security Center Web Console, confirmez que vous possédez les éléments suivants :

   - Une stratégie pour Kaspersky Endpoint Security et/ou les autres applications de sécurité que vous utilisez.
   - Tâches pour Kaspersky Endpoint Security for Windows : *Recherche de virus rapide* et *Installer la mise à jour* (si vous utilisez Kaspersky Endpoint Security for Windows).
   - Les tâches pour d'autres applications de sécurité que vous utilisez.

2. Sur un des appareils administrés, sélectionnés pour l'installation, confirmez les éléments suivants :

   - Kaspersky Endpoint Security ou une autre application de sécurité Kaspersky est installée.
   - Dans Kaspersky Endpoint Security, les paramètres de la Protection contre les fichiers malicieux, la Protection contre les menaces Internet et la Protection contre les menaces par emails correspondent à la stratégie créée pour cet appareil.
   - Le service Kaspersky Endpoint Security peut être arrêté et lancé manuellement.
   - Les tâches de groupe peuvent être lancées et arrêtées manuellement.

Création de paquets d'installation autonomes

Vous et les autres utilisateurs d'appareils de votre organisation pouvez utiliser des paquets d'installation autonomes pour installer l'Agent d'administration sur des appareils manuellement.

Le paquet d'installation autonome est un fichier exécutable (installer.exe) qui peut être stocké sur un Serveur Web ou dans un dossier partagé, envoyé par email ou transmis à l'appareil client par une autre méthode. Sur l'appareil client, l'utilisateur peut exécuter en local le fichier reçu pour installer une application sans recourir à Kaspersky Security Center. Vous pouvez créer des paquets d'installation autonomes pour toutes les applications Kaspersky et pour les applications tierces pour Windows, macOS et Linux. Pour créer un paquet d'installation autonome pour une application tierce, vous devez créer un paquet d'installation personnalisé.

Assurez-vous que le paquet d'installation autonome n'est pas disponible pour des personnes non autorisées.

Pour créer un paquet d'installation autonome :

1. Exécutez une des actions suivantes :

   - Dans le menu principal, accédez à **Découverte et déploiement → Déploiement et attribution → Paquets d'installation**.
   - Dans le menu principal, accédez à **Opérations → Stockages → Paquets d'installation**.

   Une liste des paquets d'installation disponibles sur le Serveur d'administration s'affiche.

2. Dans la liste des paquets d'installation, sélectionnez le paquet d'installation de l'Agent d'administration et, au-dessus de la liste, cliquez sur le bouton **Déployer**.

3. Sélectionnez l'option **Utilisation d'un paquet autonome**.

   Finalement, l'assistant de création du paquet d'installation autonome se lance. Parcourez les étapes de l'assistant à l'aide du bouton **Suivant**.

4. Assurez-vous que l'option **Installer l'Agent d'administration avec cette application** est activée si vous souhaitez installer l'Agent d'administration avec l'application sélectionnée.

   L'option s'affiche en fonction de l'application pour laquelle vous créez un paquet d'installation autonome.

   Cette option est activée par défaut. Nous recommandons d'activer cette option si vous n'êtes pas sûr que l'Agent d'administration est installé sur l'appareil. Si l'Agent d'administration est déjà installé sur l'appareil, après l'installation du paquet d'installation autonome avec l'Agent d'administration, l'Agent d'administration est mis à jour vers la version la plus récente.

   Si vous désactivez cette option, l'Agent d'administration n'est pas installé sur l'appareil et l'appareil n'est pas administré.

   Si un paquet d'installation autonome pour l'application sélectionnée existe déjà sur le Serveur d'administration, l'assistant vous en informe. Dans ce cas, vous devez sélectionner l'une des actions suivantes :

   - **Créer un paquet d'installation autonome**. Sélectionnez cette option, par exemple, si vous souhaitez créer un paquet d'installation autonome pour une nouvelle version d'application et que vous souhaitez également conserver un paquet d'installation autonome que vous avez créé pour une version d'application précédente. Le nouveau paquet d'installation autonome est placé dans un autre dossier.
   - **Utiliser le paquet d'installation autonome existant**. Sélectionnez cette option si vous souhaitez utiliser un paquet d'installation autonome existant. Le processus de création du paquet n'est pas démarré.
   - **Reconstruire le paquet d'installation autonome existant**. Sélectionnez cette option si vous souhaitez créer de nouveau un paquet d'installation autonome pour la même application. Le paquet d'installation autonome est placé dans le même dossier.

5. À l'étape **Déplacement dans la liste des appareils administrés**, l'option **Ne pas déplacer les appareils** est activée par défaut. Si vous ne souhaitez pas déplacer l'appareil client dansun groupe d'administration après l'installation de l'Agent d'administration, laissez cette option activée.

   Si vous souhaitez déplacer les appareils clients vers un groupe d'administration après l'installation de l'Agent d'administration, sélectionnez l'option **Déplacer les appareils non définis dans ce groupe**, et spécifiez un groupe d'administration vers lequel vous souhaitez déplacer l'appareil client. Par défaut, l'appareil est déplacé vers le groupe **Appareils administrés**.

6. Lorsque le processus de création du paquet d'installation autonome est terminé, cliquez sur le bouton **TERMINER**.

   L'Assistant de création du paquet d'installation autonome se ferme.

Le paquet d'installation autonome est créé et placé dans le sous-dossier PkgInst du dossier partagé du Serveur d'administration. Vous pouvez afficher la liste des paquets autonomes en cliquant sur le bouton **Consulter la liste des paquets autonomes** situé au-dessus de la liste des paquets d'installation.

Affichage de la liste des paquets d'installation autonomes

Vous pouvez consulter la liste des paquets d'installation autonomes et des propriétés de chaque paquet d'installation autonome.

Pour consulter la liste des paquets d'installation autonomes pour tous les paquets d'installation :

Au-dessus de la liste, cliquez sur le bouton **Consulter la liste des paquets autonomes**.

Dans la liste des paquets d'installation autonomes, les propriétés de ceux-ci sont affichées comme suit :

- **Nom de l'archive**. Le nom de l'archive d'installation autonome formé automatiquement sous le nom de l'application inclus dans le paquet et la version de l'application.
- **Nom de l'application**. Nom de l'application inclus dans le paquet d'installation autonome.
- **Version de l'application**.
- **Nom du paquet d'installation de l'Agent d'administration**. La propriété n'est affichée que si l'Agent d'administration est inclus dans le paquet d'installation autonome.
- **Version de l'Agent d'administration**. La propriété n'est affichée que si l'Agent d'administration est inclus dans le paquet d'installation autonome.
- **Taille**. Taille du fichier en Mo.
- **Groupe**. Nom du groupe vers lequel l'appareil client est déplacé après l'installation de l'Agent d'administration.
- **Date de création**. Date et heure de création du paquet d'installation autonome.
- **Date de modification**. Date et heure de modification du paquet d'installation autonome.
- **Chemin**. Chemin d'accès complet au dossier où se trouve le paquet d'installation autonome.

- **Adresse Internet**. Adresse Internet de l'emplacement du paquet d'installation autonome.
- **Hash du fichier**. Cette propriété sert à certifier que le paquet d'installation autonome n'a pas été modifié par des personnes tierces et qu'un utilisateur dispose du même fichier que vous avez créé et transféré à l'utilisateur.

Pour consulter la liste des paquets d'installation autonomes dans un paquet d'installation spécifique :

Sélectionnez le paquet d'installation dans la liste, puis, au-dessus de la liste, cliquez sur le bouton **Consulter la liste des paquets autonomes**.

Dans la liste des paquets d'installation autonomes, vous pouvez faire ce qui suit :

- Publier un paquet d'installation autonome sur le serveur Web en cliquant sur le bouton **Publier**. Le paquet d'installation autonome publié est disponible au téléchargement pour les utilisateurs à qui vous avez envoyé le lien vers le paquet d'installation autonome.
- Annuler la publication d'un paquet d'installation autonome sur le Serveur Web en cliquant sur le bouton **Annuler la publication**. Un paquet d'installation autonome non publié est disponible au téléchargement uniquement pour vous et les autres administrateurs.
- Télécharger un paquet d'installation autonome sur votre appareil en cliquant sur le bouton **Télécharger**.
- Envoyer un email avec le lien vers un paquet d'installation autonome en cliquant sur le bouton **Envoyer par email**.
- Supprimer un paquet d'installation autonome en cliquant sur le bouton **Supprimer**.

Génération des paquets d'installation personnalisés

Vous pouvez utiliser des paquets d'installation personnalisés pour effectuer les opérations suivantes :

- Pour installer n'importe quelle application (comme un éditeur de texte) sur un appareil client, par exemple, au moyen d'une tâche.
- Pour créer un paquet d'installation autonome.

Un paquet d'installation personnalisé est un dossier avec un ensemble de fichiers. La source permettant de créer un paquet d'installation personnalisé est un *fichier archive*. Le fichier archive contient le ou les fichiers à inclure dans le paquet d'installation personnalisé. En créant un paquet d'installation personnalisé, vous pouvez spécifier des paramètres de ligne de commande pour installer l'application en mode silencieux, par exemple.

Si vous disposez d'une clé de licence active pour la fonction Gestion des vulnérabilités et des correctifs, vous pouvez convertir vos paramètres d'installation par défaut pour le paquet d'installation personnalisé correspondant et utiliser les valeurs recommandées par les experts de Kaspersky. Les paramètres sont automatiquement convertis lors de la création du paquet d'installation personnalisé uniquement si le fichier exécutable correspondant est inclus dans la base de données de Kaspersky d'applications tierces.

Pour créer le paquet d'installation personnalisé :

1. Exécutez une des actions suivantes :

   - Dans le menu principal, accédez à **Découverte et déploiement → Déploiement et attribution → Paquets d'installation**.
   - Dans le menu principal, accédez à **Opérations → Stockages → Paquets d'installation**.

   Une liste des paquets d'installation disponibles sur le Serveur d'administration s'affiche.

2. Cliquez sur **Ajouter**.

   L'Assistant de création du paquet d'installation se lance. Parcourez les étapes de l'Assistant à l'aide du bouton **Suivant**.

3. Sélectionnez l'option **Générer un paquet d'installation à partir d'un fichier**.

4. Définissez le nom du paquet et cliquez sur le bouton **Parcourir**.

   Une fenêtre Windows **Ouvrir** standard s'ouvre dans votre navigateur pour vous permettre de choisir un fichier pour créer le paquet d'installation.

5. Sélectionnez un fichier d'archive situé sur les disques disponibles.

   Vous pouvez charger un fichier d'archive ZIP, CAB, TAR ou TAR.GZ. Il est impossible de créer un paquet d'installation à partir d'un fichier SFX (archive auto-extractible).

   > Si vous souhaitez que les paramètres soient convertis lors de l'installation du paquet, assurez-vous que la case **Une fois que l'Assistant a terminé ses opérations, convertissez les paramètres en valeurs recommandées pour les applications reconnues par Kaspersky Security Center** est cochée, puis cliquez sur **Suivant**.

   Le chargement du fichier sur le Serveur d'administration de Kaspersky Security Center démarre.

   > Si vous avez activé l'utilisation des paramètres d'installation recommandés, Kaspersky Security Center 15.1 vérifie si le fichier exécutable est inclus dans la base de données de Kaspersky d'applications tierces. Si la vérification réussit, vous recevez une notification vous informant que le fichier est reconnu. Les paramètres sont convertis et le paquet d'installation personnalisé est créé. Il n'y a rien d'autre à faire. Cliquez sur le bouton **Terminer** pour fermer l'Assistant.

6. Sélectionnez un fichier (dans la liste des fichiers extraits du fichier d'archive choisi) et spécifiez les paramètres de ligne de commande d'un fichier exécutable.

   Vous pouvez spécifier des paramètres de ligne de commande pour installer l'application à partir du paquet d'installation en mode silencieux par exemple. La spécification des paramètres de ligne de commande est facultative.

   Le processus de création du paquet d'installation se lance.

   L'Assistant vous informe lorsque le processus est terminé.

   Si le paquet d'installation n'est pas créé, un message approprié s'affiche.

7. Cliquez sur le bouton **Terminer** pour fermer l'Assistant.

Le paquet d'installation que vous avez créé est téléchargé dans le sous-dossier Paquets du dossier partagé du Serveur d'administration. Après le téléchargement, le paquet d'installation apparaît dans la liste des paquets d'installation.

Dans la liste des paquets d'installation d'un Serveur d'administration, vous pouvez cliquer sur le lien portant le nom d'un paquet d'installation personnalisé pour :

- Afficher les propriétés suivantes d'un paquet d'installation :
  - **Nom**. Nom du paquet d'installation personnalisé.
  - **Source**. Nom du fournisseur de l'application.
  - **Application**. Nom de l'application intégrée au paquet d'installation personnalisé.
  - **Version**. Version de l'application.
  - **Langue**. Langue de l'application intégrée au paquet d'installation personnalisé.
  - **Taille (MO)**. Taille du paquet d'installation.
  - **Système d'exploitation**. Type de système d'exploitation pour lequel le paquet d'installation est destiné.
  - **Date de création**. Date de création du paquet d'installation.
  - **Date de modification**. Date de modification du paquet d'installation.
  - **Type**. Type de paquet d'installation.
- Modifiez le nom de l'archive et les paramètres de ligne de commande. Cette fonctionnalité n'est disponible que pour les paquets qui ne sont pas créés sur la base des applications Kaspersky.

Si vous avez converti les paramètres d'installation du paquet aux valeurs recommandées pour le processus de création de paquets personnalisés, deux sections supplémentaires peuvent s'afficher sous l'onglet **Paramètres** des propriétés du paquet d'installation personnalisé : **Paramètres** et **Séquence de l'installation**.

La section **Paramètres** contient les propriétés suivantes, présentées dans un tableau :

- **Nom**. Cette colonne affiche le nom attribué à un paramètre d'installation.
- **Type**. Cette colonne affiche le type d'un paramètre d'installation.
- **Valeur**. Cette colonne affiche le type de données défini par un paramètre d'installation (Bool, Filepath, Numeric, Path ou String).

La section **Séquence de l'installation** contient un tableau qui décrit les propriétés suivantes de la mise à jour incluse dans le paquet d'installation personnalisé :

- **Nom**. Le nom de la mise à jour.
- **Description**. La description de la mise à jour.
- **Source**. La source de la mise à jour, c'est-à-dire si elle a été publiée par Microsoft ou par un autre développeur tiers.

- **Type**. Le type de mise à jour, c'est-à-dire si elle est destinée à un pilote ou à une application.
- **Catégorie**. La catégorie Windows Server Update Services (WSUS) affichée pour les mises à jour Microsoft (mises à jour critiques, mises à jour des définitions, pilotes, paquets des modules complémentaires, mises à jour de la protection, Service Packs, outils, paquets cumulatifs de mise à jour, mises à jour, mise à niveau).
- **Niveau d'importance selon MSRC**. Le niveau d'importance de la mise à jour défini par Microsoft Security Response Center (MSRC).
- **Niveau d'importance**. Le niveau d'importance de la mise à jour défini par Kaspersky.
- **Niveau d'importance du correctif (pour les correctifs destinés aux applications Kaspersky)**. Le niveau d'importance du correctif s'il est destiné à une application Kaspersky.
- **Article**. L'identifiant (ID) de l'article dans la Base de connaissances décrivant la mise à jour.
- **Bulletin**. L'identifiant du bulletin de sécurité décrivant la mise à jour.
- **Non désigné pour l'installation**. Indique si la mise à jour présente l'état Non désigné pour l'installation.
- **À installer**. Indique si la mise à jour présente l'état À installer.
- **Installation**. Indique si la mise à jour présente l'état Installation.
- **Installée**. Indique si la mise à jour présente l'état Installée.
- **Échec**. Indique si la mise à jour présente l'état Échec.
- **Redémarrage requis**. Indique si la mise à jour présente l'état Redémarrage requis.
- **Enregistrée**. Affiche la date et l'heure d'enregistrement de la mise à jour.
- **Installation en mode non interactif**. Indique si la mise à jour nécessite une action de l'utilisateur pendant de l'installation.
- **Révoquée**. Affiche la date et l'heure de révocation de la mise à jour.
- **État d'approbation de la mise à jour**. Indique si la mise à jour est approuvée pour l'installation.
- **Révision**. Affiche le numéro de révision actuel de la mise à jour.
- **Identifiant de mise à jour**. Affiche l'identifiant de la mise à jour.
- **Version de l'application**. Affiche le numéro de version vers lequel l'application sera mise à jour.
- **Remplacée**. Affiche la ou les autres mises à jour qui peuvent remplacer la mise à jour.
- **Remplaçable**. Affiche la ou les autres mises à jour qui peuvent être remplacées par la mise à jour.
- **Il faut accepter les conditions du Contrat de licence**. Indique si la mise à jour nécessite l'acceptation des conditions d'un Contrat de licence utilisateur final (CLUF).
- **Éditeur**. Affiche le nom du fournisseur de la mise à jour.
- **Famille d'application**. Affiche le nom de la famille d'applications à laquelle appartient la mise à jour.

- **Application**. Affiche le nom de l'application à laquelle appartient la mise à jour.
- **Langue**. Affiche la langue de la localisation de la mise à jour.
- **Non désignée pour l'installation (nouvelle version)**. Indique si la mise à jour présente l'état Non désignée pour l'installation (nouvelle version).
- **L'installation des préaccessoires est requise**. Indique si la mise à jour présente l'état L'installation des préaccessoires est requise.
- **Mode de téléchargement**. Affiche le mode de téléchargement de la mise à jour.
- **Est un correctif**. Indique si la mise à jour est un correctif.
- **Non installée**. Indique si la mise à jour présente l'état Non installée.

Propagation des paquets d'installation sur les Serveurs d'administration secondaires

Kaspersky Security Center permet de créer des paquets d'installation pour les applications de Kaspersky et d'applications tierces, ainsi que de diffuser les paquets d'installation sur les appareils clients et d'installer les applications à partir des paquets. Pour optimiser la charge sur le Serveur d'administration primaire, vous pouvez distribuer les paquets d'installation sur les Serveurs d'administration secondaires. Après cela, les Serveurs secondaires transmettent les paquets aux appareils clients, puis vous pouvez effectuer l'installation à distance des applications sur vos appareils clients.

Pour propager les paquets d'installation sur les Serveurs d'administration secondaires, procédez comme suit :

1. Assurez-vous que les Serveurs d'administration secondaires sont connectés au Serveur d'administration principal.
2. Dans le menu principal, accédez à **Ressources (Appareils)** → **Tâches**.

   La liste des tâches s'affiche.
3. Cliquez sur le bouton **Ajouter**.

   Ceci permet de lancer l'assistant de création d'une tâche. Suivez les étapes de l'assistant.
4. Sur la page **Paramètres de nouvelle tâche**, sélectionnez **Kaspersky Security Center** dans la liste déroulante **Application**. Ensuite, dans la liste déroulante **Type de tâche**, sélectionnez **Diffusion du paquet d'installation**, puis indiquez le nom de la tâche.
5. Sur la page **Zone de la tâche**, sélectionnez les appareils auxquels la tâche est affectée de l'une des manières suivantes :

   - Si vous voulez créer une tâche pour les Serveurs d'administration secondaires dans un groupe d'administration sélectionné, sélectionnez ce groupe, puis créez une tâche de groupe pour celui-ci.
   - Si vous souhaitez créer une tâche pour certains Serveurs d'administration secondaires, sélectionnez ces Serveurs, puis créez une tâche pour eux.
6. Sur la page **Paquets d'installation distribués**, sélectionnez les paquets d'installation à copier sur les Serveurs d'administration secondaires.

7. Spécifiez un compte pour exécuter la tâche *Distribuer le paquet d'installation* sous ce compte. Vous pouvez utiliser votre compte et conserver l'option **Compte par défaut** activée. Vous pouvez également indiquer que la tâche doit être exécutée sous un autre compte disposant des droits d'accès nécessaires. Pour ce faire, sélectionnez l'option **Indiquer un compte**, puis saisissez les informations d'identification de ce compte.

8. Sur la page **Fin de la création de la tâche**, vous pouvez activer l'option **Ouvrir les détails de la tâche à la fin de la création** pour ouvrir la fenêtre des propriétés de la tâche et puis modifier les paramètres de la tâche par défaut. Sinon, vous pouvez configurer les paramètres de la tâche ultérieurement, à tout moment.

9. Cliquez sur le bouton **Terminer**.

   La tâche créée pour la distribution des paquets d'installation sur les Serveurs d'administration secondaires s'affiche dans la liste des tâches.

10. Vous pouvez lancer la tâche manuellement ou attendez son lancement conformément à la planification que vous avez indiquée dans les paramètres de la tâche.

Une fois la tâche terminée, les paquets d'installation sélectionnés sont copiés sur les Serveurs d'administration secondaires indiqués.

Installation des applications à l'aide de la tâche d'installation à distance

Kaspersky Security Center permet d'installer à distance des applications sur les appareils à l'aide des tâches d'installation à distance. Les tâches sont créées et attribuées à des appareils à l'aide d'un Assistant. Pour pouvoir attribuer une tâche plus vite et plus facilement, vous pouvez désigner les appareils (jusqu'à 1 000 appareils) dans la fenêtre de l'Assistant de la manière qui vous convient le plus :

- **Sélectionner les appareils détectés sur le réseau par le Serveur d'administration**. Dans ce cas la tâche est affectée à un ensemble d'appareils. L'ensemble d'appareils peut reprendre aussi bien des appareils de groupes d'administration que des appareils non définis.

- **Définir les adresses des appareils manuellement ou les importer à partir d'une liste**. Vous pouvez définir les noms NetBIOS, les noms DNS, les adresses IP, ainsi que les plages d'adresses IP auxquels il convient d'affecter la tâche.

- **Attribuer la tâche à une sélection d'appareils**. Dans ce cas, la tâche est affectée aux appareils qui appartiennent à une sélection préalable. Vous pouvez spécifier la sélection prédéfinie ou une sélection personnalisée que vous avez créée.

- **Attribuer la tâche à un groupe d'administration**. Dans ce cas, la tâche est affectée aux appareils qui appartiennent à un groupe d'administration déjà créé.

Pour éviter les problèmes pouvant survenir lors de l'installation de l'application sur un appareil client sans Agent d'administration installé, il faut procéder comme décrit dans le déploiement forcé via la tâche d'installation à distance de Kaspersky Security Center.

Installation d'une application à distance

Cette section contient des informations sur l'installation à distance d'une application sur un groupe d'administration, des appareils avec des adresses IP spécifiques ou une sélection d'appareils administrés.

Pour installer l'application sur les appareils spécifiques, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Tâches**.
2. Cliquez sur **Ajouter**.

   Ceci permet de lancer l'Assistant de création d'une tâche.
3. Dans le champ **Type de tâche**, sélectionnez **Installation à distance d'une application**.
4. Sélectionnez l'une des options ci-dessous :

   - **Attribuer la tâche à un groupe d'administration**

     La tâche est affectée aux appareils qui appartiennent à un groupe d'administration. Vous pouvez renseigner un des groupes existants ou en créer un.

     Par exemple, vous pourriez souhaiter utiliser cette option pour exécuter une tâche d'envoi de messages pour les utilisateurs si le message est particulier pour les appareils repris dans un groupe d'administration spécifique.

     Si une tâche est attribuée à un groupe d'administration, l'onglet **Sécurité** ne s'affiche pas dans la fenêtre des propriétés de la tâche, car les tâches de groupe sont soumises aux paramètres de sécurité des groupes auxquels elles s'appliquent.

   - **Définir les adresses des appareils manuellement ou les importer à partir d'une liste**

     Vous pouvez définir les noms NetBIOS, les noms DNS, les adresses IP, ainsi que les plages d'adresses IP auxquels il convient d'affecter la tâche.

     Vous pourriez utiliser cette option pour exécuter une tâche pour un sous-réseau défini. Par exemple, vous pourriez souhaiter installer une certaine application sur les appareils des comptables ou analyser des appareils dans un sous-réseau qui est probablement infecté.

   - **Attribuer la tâche à une sélection d'appareils**

     La tâche est affectée aux appareils qui appartiennent à une sélection d'appareils. Vous pouvez définir une des sélections existantes.

     Par exemple, vous pourriez souhaiter utiliser cette option pour exécuter une tâche sur des appareils dotés d'une version du système d'exploitation spécifique.

   La tâche *Installer l'application à distance* est créée pour les appareils indiqués. Si vous avez sélectionné l'option **Attribuer la tâche à un groupe d'administration**, la tâche est de groupe.
5. À l'étape Zone d' **Zone de la tâche**, indiquez un groupe d'administration, des appareils avec des adresses spécifiques ou une sélection d'appareils.

   Les paramètres disponibles dépendent de l'option sélectionnée à l'étape précédente.

6. À l'étape **Paquets d'installation**, spécifiez les paramètres suivants :

- Dans le champ **Sélection du paquet d'installation**, sélectionnez le paquet d'installation d'une application que vous souhaitez installer.
- Le groupe de paramètres **Forcer le téléchargement du paquet d'installation** permet de sélectionner le mode d'envoi des fichiers nécessaires pour l'installation de l'application sur les appareils clients :
  - **En utilisant l'Agent d'administration**

    Si l'option est activée, l'Agent d'administration installé sur les appareils clients fournit les paquets d'installation à ces derniers.

    Si cette option est désactivée, les paquets d'installation sont fournis à l'aide des outils du système d'exploitation des appareils client.

    Il est recommandé d'activer cette option si la tâche concerne des appareils sur lesquels un Agent d'administration est installé.

    Cette option est activée par défaut.

  - **En utilisant les ressources du système d'exploitation via les points de distribution**

    Si l'option est activée, les paquets d'installation sont transmis sur les appareils clients via les outils du système d'exploitation par les points de distribution. Cette option peut être sélectionnée si au moins un point de distribution se trouve sur le réseau.

    Si l'option **À l'aide de l'Agent d'administration** est activée, les fichiers seront livrés via les outils du système d'exploitation uniquement dans le cas où il n'est pas possible d'utiliser les moyens de l'Agent d'administration.

    Par défaut, l'option est activée pour les tâches d'installation à distance créées sur le Serveur d'administration virtuel.

  - **En utilisant les ressources du système d'exploitation via le Serveur d'administration**

    Si cette option est activée, les fichiers sont transmis aux appareils clients à l'aide des outils du système d'exploitation des appareils clients via le Serveur d'administration. Cette option peut être activée si l'Agent d'administration n'est pas installé sur l'appareil client, mais que l'appareil client fait partie du même réseau que le Serveur d'administration.

    Cette option est activée par défaut.

- Dans le champ **Nombre maximal de téléchargements simultanés**, indiquez le nombre maximal autorisé d'appareils clients auxquels le Serveur d'administration peut transmettre simultanément les fichiers.
- Dans le champ **Nombre maximal de tentatives d'installation**, indiquez le nombre maximal autorisé d'exécutions du programme d'installation.

  Si le nombre de tentatives indiqué dans le paramètre est dépassé, Kaspersky Security Center ne lance plus le programme d'installation sur l'appareil. Pour relancer la tâche *Installation à distance de l'application*, augmentez la valeur du paramètre **Nombre maximal de tentatives d'installation** et lancez la tâche. Sinon, vous pouvez aussi créer une nouvelle tâche *Install application remotely*.
- Si vous passez d'une application Kaspersky à une autre et que votre application actuelle est protégée par un mot de passe, saisissez le mot de passe dans le champ **Mot de passe pour désinstaller l'application Kaspersky actuelle**. Notez que lors de la migration, votre application Kaspersky actuelle sera désinstallée.

Le champ **Mot de passe pour désinstaller l'application Kaspersky actuelle** n'est accessible que si vous avez sélectionné l'option **En utilisant l'Agent d'administration** dans le groupe de paramètres **Forcer le téléchargement du paquet d'installation**.

Vous pouvez utiliser le mot de passe de désinstallation uniquement pour le scénario de migration de Kaspersky Security for Windows Server vers Kaspersky Endpoint Security for Windows lors de l'installation de Kaspersky Endpoint Security for Windows à l'aide de la tâche *Installation à distance de l'application*. L'utilisation du mot de passe de désinstallation lors de l'installation d'autres modules peut entraîner des erreurs d'installation.

Pour mener à bien la migration, assurez-vous que les conditions préalables suivantes sont remplies :

- Vous utilisez l'Agent d'administration de Kaspersky Security Center 14.2 for Windows ou une version ultérieure.
- Vous installez l'application sur les appareils fonctionnant sous Windows.

- Configurez les paramètres supplémentaires :
  - **Ne pas réinstaller l'application si elle est déjà installée**

    Si l'option est activée, l'application sélectionnée n'est pas installé à nouveau, si l'appareil client en est déjà équipé.

    Si l'option est désactivée, l'application sera malgré tout installée.

    Cette option est activée par défaut.

  - **Vérifier le type de système d'exploitation avant le téléchargement**

    Avant de transmettre les fichiers aux appareils clients, Kaspersky Security Center vérifie si les paramètres de l'utilitaire d'installation sont applicables au système d'exploitation de l'appareil client. Si les paramètres ne sont pas applicables, Kaspersky Security Center ne transmet pas les fichiers et n'essaie pas d'installer l'application. Par exemple, pour installer une application quelconque sur les appareils d'un groupe d'administration qui comprend des appareils fonctionnant sous divers systèmes d'exploitation, vous pouvez attribuer la tâche d'installation au groupe d'administration, puis activer cette option pour ignorer les appareils qui fonctionnent sous un système d'exploitation autre que celui requis.

  - **Réparer l'installation du paquet d'installation dans les stratégies de groupe d'Active Directory**

    Si l'option est activée, le paquet d'installation s'installera à l'aide des stratégies de groupes Active Directory.

    L'option est disponible si le paquet d'installation de l'Agent d'administration est sélectionné.

    Cette option est Inactif par défaut.

  - **Demander aux utilisateurs de fermer les applications en cours d'exécution**

Les applications en cours d'exécution peuvent empêcher le redémarrage de l'appareil client. Par exemple, si un document est en train d'être modifié dans un logiciel de traitement de texte et qu'il n'est pas enregistré, l'application n'autorise pas le redémarrage de l'appareil.

Quand cette option est activée, l'arrêt forcé de ces applications sur un appareil verrouillé doit avoir lieu avant de pouvoir redémarrer l'appareil. Les utilisateurs pourraient perdre toute modification qui n'a pas été enregistrée à ce moment.

Si cette option est désactivée, un appareil verrouillé n'est pas redémarré. L'état de la tâche sur cet appareil indique qu'il faut redémarrer l'appareil. Les utilisateurs doivent quitter manuellement toutes les applications en cours d'exécution sur les appareils verrouillés, puis redémarrer ces appareils.

Cette option est Inactif par défaut.

- Sélectionnez les appareils sur lesquels vous souhaitez installer l'application :
  - **Installer sur tous les appareils**

    L'application est installée même sur les appareils administrés par d'autres Serveurs d'administration.

    Par défaut, cette option est sélectionnée. Vous n'avez pas à modifier ce paramètre si vous n'avez qu'un seul Serveur d'administration sur votre réseau.

  - **Installer uniquement sur les appareils administrés via &ce Serveur d'administration**

    L'application est installée uniquement sur les appareils administrés par ce Serveur d'administration. Sélectionnez cette option si vous avez plus d'un Serveur d'administration dans votre réseau et que vous souhaitez évitez les conflits entre eux.

- Spécifiez si les appareils doivent être déplacés vers un groupe d'administration après l'installation :
  - **Ne pas déplacer les appareils**

    Les appareils demeurent dans les groupes où ils se trouvent. Les appareils qui n'ont été placés dans aucun groupe restent non définis.

  - **Déplacer les appareils non définis vers le groupe sélectionné (seul un groupe unique peut être sélectionné)**

    Les appareils sont déplacés vers le groupe d'administration que vous avez sélectionné.

Notez que l'option **Ne pas déplacer les appareils** est sélectionnée par défaut. Pour des raisons de sécurité, envisagez de déplacer les appareils manuellement.

7. À cette étape de l'assistant, indiquez si les appareils doivent être redémarrés lors de l'installation des applications :

- **Ne pas redémarrer l'appareil**

  Les appareils clients ne redémarrent pas automatiquement après l'opération. Pour arrêter le fonctionnement, il faut redémarrer l'appareil (par exemple, manuellement ou à l'aide d'une tâche d'administration des appareils). Les informations sur la nécessité du redémarrage sont enregistrées dans les résultats de la tâche et dans l'état de l'appareil. Cette option convient aux tâches d' sur les serveurs et autres appareils pour lesquels la continuité des opérations est critique.

- **Redémarrer l'appareil**

  Dans ce cas, le redémarrage des appareils clients est toujours exécuté automatiquement, si celui-ci est requis pour terminer l'opération. Cette option convient aux tâches d' sur des appareils pour lesquels des interruptions périodiques sont admises (débranchement, redémarrage).

- **Confirmer l'action auprès de l'utilisateur**

  Le message qui signale que l'appareil client doit être redémarré manuellement s'affiche sur l'écran de l'appareil. Pour cette option, il est possible de configurer des paramètres avancés : le texte du message pour l'utilisateur, la fréquence du message, ainsi que le délai à l'issue duquel le redémarrage sera forcé (sans confirmation de l'utilisateur). Cette option convient le mieux pour les postes de travail sur lesquels les utilisateurs doivent pouvoir sélectionner l'heure de redémarrage qui leur convient le mieux.

  Cette option est sélectionnée par défaut.

  - **Répéter la demande toutes les (min.)**

    Quand cette option est activée, l'application invite l'utilisateur à redémarrer le système d'exploitation selon la fréquence indiquée.

    Cette option est activée par défaut. L'intervalle par défaut est de 5 minutes. La valeur peut être comprise entre 1 et 1 440 minutes.

    Si cette option est désactivée, l'invite est affichée une seule fois.

  - **Redémarrer le système au bout de (min.)**

    Après avoir averti l'utilisateur, l'application force le redémarrage du système d'exploitation à l'issue de l'intervalle défini.

    Cette option est activée par défaut. Le délai par défaut est de 30 minutes. La valeur peut être comprise entre 1 et 1 440 minutes.

- **Forcer la fermeture des applications dans les sessions bloquées**

Les applications en cours d'exécution peuvent empêcher le redémarrage de l'appareil client. Par exemple, si un document est en train d'être modifié dans un logiciel de traitement de texte et qu'il n'est pas enregistré, l'application n'autorise pas le redémarrage de l'appareil.

Quand cette option est activée, l'arrêt forcé de ces applications sur un appareil verrouillé doit avoir lieu avant de pouvoir redémarrer l'appareil. Les utilisateurs pourraient perdre toute modification qui n'a pas été enregistrée à ce moment.

Si cette option est désactivée, un appareil verrouillé n'est pas redémarré. L'état de la tâche sur cet appareil indique qu'il faut redémarrer l'appareil. Les utilisateurs doivent quitter manuellement toutes les applications en cours d'exécution sur les appareils verrouillés, puis redémarrer ces appareils.

Cette option est Inactif par défaut.

8. Si nécessaire, à l'étape **Sélection des comptes utilisateurs pour accéder aux appareils**, ajoutez les comptes qui seront utilisés pour lancer la tâche *Installation à distance de l'application* :

- **Compte utilisateur &non requis (Agent d'administration installé)**

  Si cette option est sélectionnée, il n'est pas nécessaire d'indiquer le compte utilisateur au nom duquel l'installateur de l'application sera lancé. La tâche est lancée sous le même compte utilisateur que le compte du service du Serveur d'administration.

  Si l'agent d'administration n'est pas installé sur les appareils clients, l'option n'est pas disponible.

- **Compte utilisateur requis (&Agent d'administration non utilisé)**

  Sélectionnez cette option si l'Agent d'administration n'est pas installé sur les appareils pour lesquels vous affectez la tâche d'installation à distance. Dans ce cas, vous pouvez spécifier un compte utilisateur ou un certificat SSH pour installer l'application.

  - **Compte utilisateur local**. Si cette option est sélectionnée, spécifiez le compte utilisateur sous lequel le programme d'installation de l'application sera exécuté. Cliquez sur le bouton **Ajouter**, sélectionnez **Compte utilisateur local**, puis indiquez les informations d'identification du compte utilisateur.

    Vous pouvez désigner plusieurs comptes utilisateurs si aucun d'entre eux ne possède les privilèges nécessaires sur tous les appareils auxquels vous affectez la tâche. Dans ce cas, tous les comptes ajoutés sont utilisés pour exécuter la tâche, dans un ordre consécutif, de haut en bas.

  - **Certificat SSH**. Si vous souhaitez installer l'application sur un appareil client basé sur Linux, vous pouvez indiquer un certificat SSH au lieu d'un compte utilisateur. Cliquez sur le bouton **Ajouter**, sélectionnez **Certificat SSH**, puis indiquez les clés privée et publique du certificat.

    Pour générer une clé privée, vous pouvez utiliser l'utilitaire ssh-keygen. Notez que Kaspersky Security Center prend en charge le format PEM des clés privées, mais que l'utilitaire ssh-keygen génère par défaut des clés SSH au format OPENSSH. Le format OPENSSH n'est pas pris en charge par Kaspersky Security Center. Pour créer une clé privée au format PEM pris en charge, ajoutez l'option -m PEM dans la commande ssh-keygen. Par exemple :

    ```
    ssh-keygen -m PEM -t rsa -b 4096 -C "<user email>"
    ```

9. À l'étape **Fin de la création de la tâche**, cliquez sur le bouton **Terminer** pour créer la tâche et fermer l'Assistant.

   Si vous avez activé l'option **Ouvrir les détails de la tâche à la fin de la création**, la fenêtre des paramètres de la tâche s'ouvre. Dans cette fenêtre, vous pouvez vérifier les paramètres de la tâche, les modifier ou configurer une planification de lancement de la tâche, si nécessaire.

10. Dans la liste des tâches, sélectionnez la tâche que vous avez créée, puis cliquez sur **Démarrer**.

    Vous pouvez également attendre que la tâche se lance conformément à la planification que vous avez spécifiée dans les paramètres de la tâche.

Une fois la tâche d'installation à distance terminée, l'application sélectionnée est installée sur les appareils indiqués.

Installation de l'application à l'aide des stratégies de groupe Active Directory

Kaspersky Security Center permet d'installer les applications de Kaspersky sur les appareils administrés à l'aide des stratégies de groupe Active Directory.

L'installation des applications à l'aide des stratégies de groupe Active Directory est possible uniquement lors de l'utilisation des paquets d'installation incluant l'Agent d'administration.

Pour installer l'application à l'aide des stratégies de groupe Active Directory, procédez comme suit :

1. Exécutez l'Assistant de déploiement de la protection. Suivez les instructions de l'assistant.

2. Sur la page **Paramètres de la tâche d'installation à distance** de l'Assistant de déploiement de la protection, activez l'option **Réparer l'installation du paquet d'installation dans les stratégies de groupe d'Active Directory**.

3. Sur la page **Sélection des comptes utilisateurs pour accéder aux appareils**, sélectionnez l'option **Compte utilisateur requis (Agent d'administration non utilisé)**.

4. Ajoutez au compte les privilèges d'administrateur sur l'appareil où Kaspersky Security Center est installé ou au compte inclus dans le groupe de domaine Propriétaires créateurs de la stratégie du groupe.

5. Accordez les autorisations au compte sélectionné :

    a. Accédez à **Panneau de configuration** → **Outils d'administration** et ouvrez **Gestion des stratégies de groupe**.

    b. Cliquez sur le nœud avec le domaine requis.

    c. Cliquez sur la section **Délégation**.

    d. Choisissez l'option **Lier les objets de stratégie de groupe** dans la liste déroulante **Autorisation**.

    e. Cliquez sur **Ajouter**.

    f. Dans la fenêtre **Sélectionner un utilisateur, un ordinateur ou un groupe** qui s'ouvre, sélectionnez le compte requis.

    g. Cliquez sur **OK** pour fermer la fenêtre **Sélectionner un utilisateur, un ordinateur ou un groupe**.

    h. Dans la liste **Groupes et utilisateurs**, sélectionnez le compte que vous venez d'ajouter, puis cliquez sur **Avancé** → **Avancé**.

    i. Dans la liste des **entrées d'autorisation**, double-cliquez sur le compte que vous venez d'ajouter.

    j. Accordez les autorisations suivantes :

    - **Créer des objets du groupe**
    - **Supprimer des objets du groupe**
    - **Créer des objets conteneurs de stratégie de groupe**
    - **Supprimer des objets conteneurs de stratégie de groupe**

    k. Cliquez sur le bouton **OK** afin d'enregistrer les modifications.

6. Définissez d'autres paramètres en suivant les instructions de l'Assistant.

7. Lancez la tâche créée d'installation à distance ou attendez son lancement programmé.

Finalement, le mécanisme suivant de l'installation à distance sera lancé :

1. Après le lancement de la tâche dans chaque domaine comprenant les appareils clients de l'ensemble, les objets suivants seront créés :

    - L'objet de la stratégie de groupe (OSG) avec le nom **Kaspersky_AK{GUID}**.
    - Un groupe de sécurité qui correspond à l'objet de la stratégie de groupe. Ce groupe de sécurité contient les appareils clients sur lesquels la tâche se diffuse. Le contenu du groupe de sécurité détermine la zone d'action de l'objet de la stratégie du groupe.

2. Kaspersky Security Center installe les applications Kaspersky sélectionnées sur les appareils clients directement depuis le dossier KLSHARE, c'est-à-dire le dossier réseau partagé de l'application. Dans le dossier d'installation de Kaspersky Security Center, un sous-dossier auxiliaire sera créé contenant le fichier .msi de l'application à installer.

3. Lors de l'ajout de nouveaux appareils dans la zone d'action d'une tâche, ils seront ajoutés au groupe de protection après le lancement suivant d'une tâche. Si dans la programmation d'une tâche, l'option **Lancer les tâches non exécutées** est sélectionnée, les appareils seront immédiatement ajoutés au groupe de protection.

4. Lors de la suppression des appareils depuis la zone d'action d'une tâche, leur suppression depuis le groupe de sécurité se passera lors du prochain lancement d'une tâche.

5. Lorsqu'une tâche est supprimée à partir d'Active Directory, l'OSG, le lien vers cet OSG et le groupe de protection correspondant sont supprimés également.

Si vous voulez utiliser un autre schéma d'installation via Active Directory, vous pouvez manuellement configurer les paramètres d'installation. Cela peut être utile, par exemple, dans les cas suivants :

- Quand l'administrateur de protection antivirus ne possède pas les privilèges d'apporter les modifications de certains domaines dans Active Directory.
- Si le paquet d'installation doit être placé sur une ressource de réseau distincte.
- S'il est nécessaire de lier un OSG à des sous-divisions concrètes d'Active Directory.

Les options suivantes d'utilisation d'un autre schéma d'installation via Active Directory sont disponibles :

- Si l'installation doit être effectuée directement depuis le dossier partagé de Kaspersky Security Center, vous devez indiquer dans les propriétés de l'OSG le fichier d'extension msi, situé dans le sous-dossier exec du dossier du paquet d'installation de l'application concernée.
- Si le paquet d'installation doit être placé dans une autre ressource de réseau, il faut y copier tout le contenu du dossier exec, puisque, excepté le fichier avec extension msi, ce dossier contient les fichiers de configuration formés au moment de création du paquet d'installation. Pour que la clé de licence soit installée avec l'application, il faut aussi copier le fichier clé dans ce dossier.

Installation des applications sur les Serveurs d'administration secondaires

Pour installer l'application sur les Serveurs d'administration secondaires, procédez comme suit :

1. Connectez-vous au Serveur d'administration qui gère les Serveurs d'administration secondaires nécessaires.

2. Assurez-vous que le paquet d'installation correspondant à l'application à installer se trouve sur chaque Serveur d'administration secondaire sélectionné. Si vous ne trouvez pas le paquet d'installation sur l'un des Serveurs secondaires, distribuez-le. Pour ce faire, créez une tâche avec le type de tâche **Diffusion du paquet d'installation**

3. Créez une tâche pour l'installation à distance de l'application sur les Serveurs d'administration secondaires. Sélectionnez le type de tâche **Installer à distance l'application sur le Serveur d'administration secondaire**.

   L'Assistant de création d'une tâche crée une tâche d'installation à distance de l'application sélectionnée dans l'Assistant sur certains Serveurs d'administration secondaires.

4. Lancez la tâche manuellement ou attendez son lancement conformément à la planification que vous avez indiquée dans les paramètres de la tâche.

Une fois la tâche d'installation à distance terminée, l'application sélectionnée est installée sur les Serveurs d'administration secondaires.

Spécification des paramètres pour l'installation à distance sur les appareils Unix

Lorsque vous installez une application sur un appareil Unix à l'aide d'une tâche d'installation à distance, vous pouvez spécifier les paramètres propres à Unix pour la tâche. Ces paramètres sont disponibles dans les propriétés de la tâche une fois la tâche créée.

Pour spécifier des paramètres propres à Unix pour une tâche d'installation à distance, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Tâches**.
2. Cliquez sur le nom de la tâche d'installation à distance pour laquelle vous souhaitez spécifier les paramètres propres à Unix.

   La fenêtre de propriétés de la tâche s'affiche.
3. Accédez à **Paramètres de l'application** → **Paramètres propres à Unix**.
4. Définissez les paramètres suivants :

   - **Définir un mot de passe pour le compte root (uniquement pour le déploiement via SSH)**

     Si la commande `sudo` ne peut pas être utilisée sur l'appareil cible sans indiquer le mot de passe, sélectionnez cette option, puis indiquez le mot de passe du compte root. Kaspersky Security Center transmet le mot de passe sous une forme chiffrée à l'appareil cible, déchiffre le mot de passe, puis lance la procédure d'installation au nom du compte root avec le mot de passe indiqué.

     Kaspersky Security Center n'utilise pas le compte ni le mot de passe indiqué pour créer une connexion SSH.

   - **Définir le chemin d'accès à un dossier temporaire avec les autorisations Execute sur l'appareil cible (uniquement pour le déploiement via SSH)**

     Si le répertoire /tmp sur l'appareil cible ne dispose pas de l'autorisation d'exécution, sélectionnez cette option, puis indiquez le chemin d'accès au répertoire avec l'autorisation d'exécution. Kaspersky Security Center utilise le répertoire indiqué comme répertoire temporaire pour y accéder via le protocole SSH. L'application place le paquet d'installation dans le répertoire et exécute la procédure d'installation.
5. Cliquez sur le bouton **Enregistrer**.

Les paramètres de tâche indiqués sont enregistrés.

Lancement et arrêt des applications Kaspersky.

Vous pouvez utiliser la tâche *Lancer ou arrêter une application* pour lancer et arrêter des applications de Kaspersky sur les appareils administrés.

Pour créer la tâche Lancer ou arrêter une application, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Tâches**.
2. Cliquez sur **Ajouter**.

   Ceci permet de lancer l'assistant de création d'une tâche. Parcourez les étapes de l'assistant à l'aide du bouton **Suivant**.
3. Dans la liste déroulante **Application**, sélectionnez l'application pour laquelle vous voulez créer une tâche.

   Les applications de Kaspersky s'affichent dans la liste si vous avez déjà ajouté des plug-ins Internet d'administration pour ces applications.
4. À partir de la liste **Type de tâche**, sélectionnez la tâche **Activation de l'application**.
5. Dans le champ **Nom de la tâche**, indiquez le nom de la nouvelle tâche.

   Le nom de la tâche ne peut pas contenir plus de 100 symboles et contenir de symboles spéciaux ("*<>?\:|).
6. Sélectionnez les appareils auxquels les tâches seront affectées.
7. Dans la fenêtre **Applications**, réalisez les opérations suivantes :
   - Cochez les cases en regard du nom des applications pour lesquelles vous souhaitez créer une tâche.
   - Sélectionnez l'option **Lancer l'application** ou **Arrêter l'application**.
8. Si vous souhaitez modifier les paramètres de la tâche par défaut, activez l'option **Ouvrir les détails de la tâche à la fin de la création** à l'étape **Fin de la création de la tâche**. Si vous n'activez pas cette tâche, la tâche est créée selon les paramètres par défaut. Vous pourrez modifier ces paramètres par défaut plus tard, à tout moment.
9. Cliquez sur le bouton **Terminer**.

   La tâche est créée et s'affiche dans la liste des tâches.
10. Cliquez sur le nom de la tâche créée pour ouvrir la fenêtre de propriétés de la tâche.
11. Dans la fenêtre des propriétés de la tâche, indiquez les paramètres généraux de la tâche en fonction de vos besoins, puis enregistrez les paramètres.

La tâche est créée et configurée.

Si vous souhaitez exécuter la tâche, sélectionnez-la dans la liste des tâches, puis cliquez sur le bouton **Démarrer**.

Administration des appareils mobiles

L'administration de la protection des appareils mobiles via Kaspersky Security Center est confiée à la Fonction Administration des appareils mobiles qui requiert une licence dédiée. Si vous avez l'intention d'administrer les appareils mobiles qui appartiennent aux employés de votre organisation, activez et configurez l'Administration des appareils mobiles.

L'administration des appareils mobiles vous permet d'administrer les appareils Android des employés. La protection est assurée par l'application mobile Kaspersky Endpoint Security for Android installée sur les appareils. Cette application mobile assure la protection des appareils mobiles contre les menaces Web, les virus et les autres programmes qui présentent des menaces. Pour assurer une administration centralisée via Kaspersky Security Center Web Console, vous devez installer les plug-ins d'administration Web suivants sur l'appareil sur lequel Kaspersky Security Center Web Console est installé :

- Plug-in Kaspersky Security for Mobile
- Plug-in Kaspersky Endpoint Security for Android

Pour obtenir plus d'informations sur le déploiement de la protection et l'administration des appareils mobiles, consultez l'aide de Kaspersky Security for Mobile.

Modification des paramètres d'administration des appareils mobiles dans Kaspersky Security Center Web Console

Pour modifier les paramètres de l'Administration des appareils mobiles, procédez comme suit :

1. Dans le menu principal, cliquez sur l'icône des paramètres ( ) en regard du nom du Serveur d'administration requis.

   La fenêtre des propriétés du Serveur d'administration s'ouvre.

2. Sous l'onglet **Général**, sélectionnez la section **Ports supplémentaires**.

3. Modifiez les paramètres pertinents :

   - **Ouvrir le port pour les appareils mobiles**

     Si le commutateur est activé, le port pour les appareils mobiles sera ouvert sur le Serveur d'administration.

     L'utilisation du port pour les appareils mobiles n'est possible que si le composant Administration des appareils mobiles est installé.

     Si le commutateur est désactivé, le port des appareils mobiles du Serveur d'administration n'est pas utilisé.

     Par défaut, ce commutateur est désactivé.

   - **Port pour la synchronisation des appareils mobiles**

     Numéro de port utilisé pour connecter les appareils mobiles au Serveur d'administration. Le numéro de port par défaut est 13292.

     La forme d'écriture décimale est utilisée.

   - **Port pour l'activation des appareils mobiles**

     Port de connexion de Kaspersky Endpoint Security for Android aux serveurs d'activation de Kaspersky.

     Le numéro de port par défaut est 17100.

4. Cliquez sur le bouton **Enregistrer**.

Les appareils mobiles peuvent désormais se connecter au Serveur d'administration.

Remplacement d'application de sécurité d'éditeurs tiers

Pour installer des applications de sécurité de Kaspersky à l'aide des outils de Kaspersky Security Center, il faut peut-être supprimer tout logiciel tiers incompatible avec l'application à installer. Kaspersky Security Center offre plusieurs méthodes pour retirer des applications tiers.

Supprimez les applications incompatibles à l'aide du programme d'installation

Cette option est disponible uniquement dans la Console d'administration basée sur la console de gestion Microsoft.

La méthode qui consiste à supprimer les applications incompatibles convient à plusieurs types d'installation. Avant l'installation de l'application de sécurité, toutes les applications incompatibles sont supprimées automatiquement si, dans la fenêtre des propriétés du paquet d'installation de cette application de sécurité (section **Applications incompatibles**), l'option **Supprimer automatiquement les applications incompatibles** a été sélectionnée.

Suppression des applications incompatibles pour configurer l'installation à distance d'une application

Vous pouvez activer l'option **Supprimer automatiquement les applications incompatibles** lorsque vous configurez l'installation à distance d'une application de sécurité. Dans la Console d'administration basée sur la console de gestion Microsoft (MMC), cette option est disponible uniquement dans l'Assistant de l'installation à distance. Dans Kaspersky Security Center Web Console, cette option se trouve dans l'assistant de déploiement de la protection. Si cette option est activée, Kaspersky Security Center supprime les applications incompatibles avant d'installer une application de sécurité sur un appareil administré.

Instructions pour :

- Console d'administration : Suppression des applications incompatibles à l'aide de l'Assistant de l'installation à distance
- Kaspersky Security Center Web Console : Suppression des applications incompatibles avant l'installation

Suppression des applications incompatibles à l'aide d'une tâche distincte

Les applications incompatibles sont supprimées à l'aide de la tâche **Tâche de désinstallation à distance d'une application**. Il faut lancer la tâche sur les appareils avant la tâche d'installation de l'application de sécurité. Par exemple, dans la tâche d'installation, vous pouvez sélectionner **Après l'exécution d'une autre tâche** en tant que type de programmation lorsque l'autre tâche est **Tâche de désinstallation à distance d'une application**.

Ce mode de suppression est recommandé si le programme d'installation de l'application de sécurité ne parvient pas à supprimer une des applications incompatibles.

Instructions pratiques pour la Console d'administration : Création d'une tâche.

Recherche d'appareils en réseau

Cette section décrit les outils de recherche et de découverte des appareils du réseau.

Kaspersky Security Center permet de rechercher les appareils sur la base des critères définis. Vous pouvez enregistrer les résultats de la recherche dans un fichier texte.

La fonction de recherche permet de trouver les appareils suivants :

- Les appareils administrés dans les groupes d'administration du Serveur d'administration de Kaspersky Security Center et de ses Serveurs d'administration secondaires ;
- Les appareils non définis administrés sous le Serveur d'administration de Kaspersky Security Center et ses Serveurs secondaires.

Scénario de recherche d'appareils en réseau

Vous devez effectuer la recherche d'appareils avant l'installation des applications de sécurité. Le Serveur d'administration reçoit les informations sur les appareils détectés et vous permet d'administrer les appareils à l'aide de stratégies. Des sondages réguliers du réseau sont nécessaires pour mettre à jour la liste des appareils disponibles dans le réseau.

Avant de lancer le sondage du réseau, assurez-vous que le protocole SMB est activé. Sinon, Kaspersky Security Center ne peut pas détecter les appareils dans le réseau interrogé. Pour activer le protocole SMB, suivez les instructions correspondant à votre système d'exploitation.

La recherche d'appareils en réseau se déroule selon les étapes suivantes :

1. **Découvrir les appareils**

   L'Assistant de configuration initiale de l'application vous guide tout au long de la recherche initiale d'appareils et vous aide à rechercher des appareils connectés en réseau comme des ordinateurs, des tablettes et des téléphones mobiles. Vous pouvez aussi commencer la recherche d'appareils manuellement.

2. **Configurer les sondages programmés**

   Décidez quel(s) type(s) de sondage vous voulez utiliser régulièrement. Activez les types souhaités et configurez la programmation du sondage. Vous pouvez consulter les recommandations relatives à la fréquence des sondages du réseau.

3. **Configurer des règles pour ajouter des appareils découverts aux groupes d'administration (facultatif)**

   Si de nouveaux appareils apparaissent sur votre réseau, ils sont détectés à l'occasion de sondages réguliers et sont automatiquement inclus dans le groupe **Appareils non définis**. Vous pouvez configurer des règles de déplacement des appareils pour automatiser l'attribution des appareils au groupe **Appareils administrés**. Vous pouvez aussi configurer des règles de conservation.

   Si vous ignorez l'étape 3, les appareils nouvellement détectés sont affectés au groupe **Appareils non définis**. Vous pouvez déplacer ces appareils vers le groupe **Appareils administrés** manuellement. Si vous déplacez les appareils vers le groupe **Appareils administrés** manuellement, vous pouvez analyser les informations sur chaque appareil et décider si vous voulez le déplacer vers un groupe d'administration, et si oui, quel groupe exact.

Résultats

La réalisation du scénario donne les résultats suivants :

- Le Serveur d'administration de Kaspersky Security Center a trouvé des appareils présents sur le réseau et vous donne des informations à leur sujet.
- Les prochains sondages sont configurés et se déroulent selon le calendrier indiqué.
- Les appareils découverts sont classés selon les règles configurées. (Ou, en l'absence de règles, ils restent dans le groupe **Appareils non définis**).

Recherche d'appareils

Cette section décrit les types de recherche d'appareils disponibles dans le Kaspersky Security Center et explique l'utilisation de chaque type.

Le Serveur d'administration reçoit des informations sur la structure du réseau et des appareils sur ce réseau par des sondages régulières. Les informations sont enregistrées dans la base de données du Serveur d'administration. Le Serveur d'administration peut réaliser les types de sondage suivants :

- **Sondage du réseau Windows**. Le Serveur d'administration peut effectuer deux types de sondage du réseau Windows : rapide et complet. Lors du sondage rapide, le Serveur d'administration ne reçoit que les informations relatives à la liste des noms NetBIOS des appareils de tous les domaines et des groupes de travail du réseau. Pendant le sondage entier, d'autres informations sont demandées de chaque appareil client comme le nom du système d'exploitation, l'adresse IP, le nom DNS et le nom NetBIOS. Par défaut, les interrogations rapides et complètes sont activées. Le sondage du réseau Windows peut échouer, par exemple, si les ports UDP 137, UDP 138, TCP 139 sont fermés sur le routeur ou par le pare-feu.
- **Sondage du contrôleur de domaine**. Le Serveur d'administration ou le point de distribution reçoit les informations sur la structure du domaine et sur les noms DNS des appareils qui font partie du domaine. Par défaut, ce type de sondage est activé. Nous vous recommandons d'utiliser le sondage du contrôleur de domaine si tous les appareils en réseau sont membres d'un domaine. Si certains appareils en réseau ne sont pas inclus dans le domaine, ces appareils ne peuvent pas être découverts par le sondage du contrôleur de domaine.
- **Sondage des plages IP**. Le Serveur d'administration sonde les intervalles IP créés à l'aide de paquets ICMP ou le protocole NBNS et reçoit toutes les informations sur les appareils appartenant aux plages IP. Par défaut, ce type de sondage est désactivé. Il n'est pas recommandé d'utiliser ce type de sondage si vous utilisez le sondage réseau et/ou le sondage Active Directory.
- **Sondage Zeroconf**. Un point de distribution qui sonde le réseau IPv6 en utilisant la mise en réseau sans configuration (également appelé *Zeroconf*). Par défaut, ce type de sondage est désactivé. Vous pouvez utiliser le sondage Zeroconf si le point de distribution exécute Linux.

Si vous configurez et activez les règles de déplacement de l'appareil, les appareils détectés sont automatiquement inclus dans le groupe **Appareils administrés**. Si aucune règle de déplacement n'est activée, les nouveaux appareils détectés sont automatiquement inclus dans le groupe **Appareils non définis**.

Vous pouvez modifier les paramètres de recherche d'appareils pour chaque type. Par exemple, il se peut que vous souhaitiez modifier la programmation du sondage ou décider de sonder l'ensemble de la forêt de domaines ou uniquement un domaine en particulier.

Avant de lancer le sondage du réseau, assurez-vous que le protocole SMB est activé. Sinon, Kaspersky Security Center ne peut pas détecter les appareils dans le réseau interrogé. Pour activer le protocole SMB, suivez les instructions correspondant à votre système d'exploitation.

Sondage du réseau Windows

À propos du sondage du réseau Windows

Lors du sondage rapide, le Serveur d'administration ne reçoit que les informations relatives à la liste des noms NetBIOS des appareils de tous les domaines et des groupes de travail du réseau. Au cours d'un sondage complet, les informations suivantes sont demandées à chaque appareil client :

- Nom du système d'exploitation
- Adresse IP
- Nom DNS
- Nom NetBIOS

Les sondages rapides et complets nécessitent les éléments suivants :

- Les ports UDP 137/138, TCP 139, UDP 445 et TCP 445 doivent être disponibles sur le réseau.
- Le protocole SMB est activé.
- Le service Microsoft Computer Browser doit être utilisé et l'ordinateur du navigateur principal doit être activé sur le Serveur d'administration.
- Le service Microsoft Computer Browser doit être utilisé et l'ordinateur du navigateur principal doit être activé sur les appareils clients :
  - Sur au moins un appareil, si le nombre d'appareils en réseau ne dépasse pas 32.
  - Sur au moins un appareil pour 32 appareils en réseau.

Le sondage complet ne peut s'exécuter que si le sondage rapide a été exécuté au moins une fois.

Affichage et modification des paramètres de sondage du réseau Windows

Pour modifier les paramètres du sondage du réseau Windows, procédez comme suit :

1. Dans le menu principal, accédez à **Découverte et déploiement** → **Découverte** → **Domaines Windows**.
2. Cliquez sur le bouton **Propriétés**.
   La fenêtre des propriétés du domaine Windows s'ouvre.

3. Activez ou désactivez le sondage réseau Windows à l'aide du bouton à bascule **Autoriser le sondage du réseau Windows**.

4. Configuration de la programmation de l'interrogation Par défaut, le sondage rapide est exécutée toutes les 15 minutes, le sondage complet toutes les 60 minutes.

   Options de programmation du sondage :

   - **Tous les N jours**

     Le sondage s'exécute régulièrement, selon l'intervalle défini en jours, à partir de la date et heure définis.

     Le sondage s'exécute par défaut chaque jour, à partir de la date et de l'heure actuelle du système.

   - **Toutes les N minutes**

     Le sondage s'exécute régulièrement, selon l'intervalle défini en minutes, à partir de l'heure définie.

   - **Par jours de la semaine**

     Le sondage s'exécute régulièrement les jours définis de la semaine, à l'heure indiquée.

   - **Chaque mois, les jours indiqués des semaines sélectionnées**

     Le sondage s'exécute régulièrement les jours définis de chaque mois, à l'heure indiquée.

   - **Lancer les tâches non exécutées**

     Si le Serveur d'administration est éteint ou s'il n'est pas disponible au moment auquel le sondage a été programmé, le Serveur d'administrateur peut soit lancer le sondage immédiatement après que le Serveur d'administration a été allumé ou attendre la prochaine programmation du sondage.

     Si cette option est activée, le Serveur d'administration lance le sondage directement après qu'il a été allumé.

     Si cette option est désactivée, le Serveur d'administration attend la prochaine programmation du sondage.

     Cette option est Inactif par défaut.

5. Enregistrez les paramètres du sondage du réseau Windows.

Les propriétés sont enregistrées et appliquées à l'ensemble des domaines Windows et des groupes de travail.

Exécution manuelle du sondage

Pour exécuter le sondage immédiatement,

Cliquez sur **Lancer un sondage rapide** ou **Lancer un sondage complet**.

Lorsque l'interrogation est terminée, vous pouvez afficher la liste des appareils trouvés sur la page **Domaines Windows** en cochant la case à côté d'un nom de domaine, puis en cliquant sur le bouton **Appareils**.

Sondage des plages IP

Au début, Kaspersky Security Center obtient les plages IP pour le sondage dans les paramètres réseau de l'appareil sur lequel il est installé. Si l'adresse de l'appareil est 192.168.0.1 et si le masque de sous-réseau est 255.255.255.0, Kaspersky Security Center inclut automatiquement le réseau 192.168.0.0/24 dans la liste des adresses de sondage. Kaspersky Security Center sonde dans ce cas toutes les adresses entre 192.168.0.1 et 192.168.0.254.

Pour tous les hôtes Linux au sein d'un contrôleur de domaine Microsoft Active Directory ou Samba, spécifiez les paramètres `netbios name` et `workgroup` dans le fichier `/etc/samba/smb.conf`. Dans le cas contraire, les résultats du sondage peuvent contenir des hôtes en double.

Kaspersky Security Center peut interroger les plages d'adresses IP par recherche DNS inversée ou à l'aide du protocole NBNS :

- **Recherche DNS inversée**

  Kaspersky Security Center tente de réaliser une résolution de nom inverse pour chacune des adresses IP de la plage définie en un nom DNS à l'aide des requêtes DNS standard. Si cette opération réussit, le serveur envoie une requête `ICMP ECHO REQUEST` (idem qu'une commande ping) au nom reçu. Si l'appareil répond, les informations à son sujet sont ajoutées à la base de données de Kaspersky Security Center. La résolution de nom inverse est nécessaire pour exclure les appareils réseau qui ne peuvent avoir une adresse IP mais qui ne sont pas des ordinateurs, par exemple, les imprimantes réseau ou les routeurs.

  Cette méthode de sondage repose sur un service DNS local correctement configuré. Il doit avoir une zone de recherche inversée. Dans les réseaux qui utilisent Active Directory, cette zone est maintenue automatiquement. Mais dans ces réseaux, le sondage du sous-réseau IP n'offre pas plus d'informations que le sondage Active Directory. De plus, les administrateurs de petits réseaux configurent rarement la zone de recherche inversée car elle n'est pas indispensable au fonctionnement de nombreux services réseau. Pour toutes ces raisons, le sondage du sous-réseau IP est désactivé par défaut.

- **Protocole NBNS**

  Si la résolution inversée des noms n'est pas possible dans votre réseau pour une raison quelconque, Kaspersky Security Center utilise le protocole NBNS pour interroger les plages IP. Si une requête sur une adresse IP renvoie un nom NetBIOS, les informations relatives à cet appareil sont ajoutées à la base de données de Kaspersky Security Center.

Avant de lancer le sondage du réseau, assurez-vous que le protocole SMB est activé. Sinon, Kaspersky Security Center ne peut pas détecter les appareils dans le réseau interrogé. Pour activer le protocole SMB, suivez les instructions correspondant à votre système d'exploitation.

Affichage et modification des paramètres de sondage des plages IP

Affichage et modification des propriétés de sondage des plages IP :

1. Dans le menu principal, accédez à **Découverte et déploiement** → **Découverte** → **Plages IP**.
2. Cliquez sur le bouton **Propriétés**.

   La fenêtre des propriétés de l'interrogation IP s'ouvre.
3. Activez ou désactivez l'interrogation IP à l'aide du bouton bascule **Autoriser le sondage**.

4. Configuration de la programmation de l'interrogation Par défaut, l'interrogation IP est exécutée toutes les 420 minutes (sept heures).

   En fixant l'intervalle d'interrogation, veillez à ce que ce réglage ne dépasse pas la valeur du paramètre de durée de vie de l'adresse IP. Si une adresse IP n'est pas vérifiée par le sondage pendant la durée de vie de l'adresse IP, cette adresse IP est automatiquement retirée des résultats du sondage. Par défaut, les résultats du sondage ont une durée de vie de 24 heures car les adresses IP dynamiques (attribuées à l'aide du protocole DHCP) changent toutes les 24 heures.

   Options de programmation du sondage :

   - **Tous les N jours**

     Le sondage s'exécute régulièrement, selon l'intervalle défini en jours, à partir de la date et heure définis.

     Le sondage s'exécute par défaut chaque jour, à partir de la date et de l'heure actuelle du système.

   - **Toutes les N minutes**

     Le sondage s'exécute régulièrement, selon l'intervalle défini en minutes, à partir de l'heure définie.

   - **Par jours de la semaine**

     Le sondage s'exécute régulièrement les jours définis de la semaine, à l'heure indiquée.

   - **Chaque mois, les jours indiqués des semaines sélectionnées**

     Le sondage s'exécute régulièrement les jours définis de chaque mois, à l'heure indiquée.

   - **Lancer les tâches non exécutées**

     Si le Serveur d'administration est éteint ou s'il n'est pas disponible au moment auquel le sondage a été programmé, le Serveur d'administrateur peut soit lancer le sondage immédiatement après que le Serveur d'administration a été allumé ou attendre la prochaine programmation du sondage.

     Si cette option est activée, le Serveur d'administration lance le sondage directement après qu'il a été allumé.

     Si cette option est désactivée, le Serveur d'administration attend la prochaine programmation du sondage.

     Cette option est Inactif par défaut.

5. Cliquez sur le bouton **Enregistrer**.

Les propriétés sont enregistrées et appliquées à toutes les plages IP.

Exécution manuelle du sondage

Pour exécuter le sondage immédiatement,

cliquez sur **Démarrer le sondage**.

Ajout et modification d'une plage IP

Au début, Kaspersky Security Center obtient les plages IP pour le sondage dans les paramètres réseau de l'appareil sur lequel il est installé. Si l'adresse de l'appareil est 192.168.0.1 et si le masque de sous-réseau est 255.255.255.0, Kaspersky Security Center inclut automatiquement le réseau 192.168.0.0/24 dans la liste des adresses de sondage. Kaspersky Security Center sonde dans ce cas toutes les adresses entre 192.168.0.1 et 192.168.0.254. Vous pouvez modifier les plages IP définies automatiquement ou ajouter des plages IP personnalisées.

Vous pouvez créer une plage uniquement pour les adresses IPv4. Si vous activez le sondage Zeroconf, Kaspersky Security Center sonde l'ensemble du réseau.

Pour ajouter une nouvelle plage IP, procédez comme suit :

1. Dans le menu principal, accédez à **Découverte et déploiement** → **Découverte** → **Plages IP**.
2. Pour ajouter une nouvelle plage IP, cliquez sur le bouton **Ajouter**.
3. Dans la fenêtre qui s'ouvre, configurez les paramètres suivants :
   - **Nom de la plage IP**

     Nom d'une plage IP. Vous pouvez par exemple indiquer la plage IP même en tant que nom, par exemple, " 192.168.0.0/24 ".
   - **Masque et adresse de l'intervalle IP et du sous-réseau**

     Définissez la plage IP en indiquant les adresses IP de début et de fin ou l'adresse de sous-réseau et le masque de sous-réseau. Vous pouvez également sélectionner l'une des plages IP existantes en cliquant sur le bouton **Parcourir**.
   - **Durée de vie de l'adresse IP (heures)**

     En définissant ce paramètre, assurez-vous qu'il dépasse l'intervalle de sondage défini dans le calendrier de sondage. Si une adresse IP n'est pas vérifiée par le sondage pendant la durée de vie de l'adresse IP, cette adresse IP est automatiquement retirée des résultats du sondage. Par défaut, les résultats du sondage ont une durée de vie de 24 heures car les adresses IP dynamiques (attribuées à l'aide du protocole DHCP) changent toutes les 24 heures.
4. Sélectionnez **Autoriser le sondage de la plage IP** si vous voulez interroger le sous-réseau ou l'intervalle que vous avez ajouté. Sinon, le sous-réseau ou l'intervalle que vous avez ajouté ne sera pas sondé.
5. Cliquez sur le bouton **Enregistrer**.

La nouvelle plage IP est ajoutée à la liste des plages IP.

Vous pouvez exécuter le sondage de chaque plage IP à l'aide du bouton **Démarrer le sondage**. Une fois l'interrogation terminée, vous pouvez consulter la liste des appareils à l'aide du bouton **Appareils**. Par défaut, la durée de vie des résultats du sondage est de 24 heures, et est égale au réglage de la durée de vie de l'adresse IP.

Pour ajouter un sous-réseau à une plage IP existante, procédez comme suit :

1. Dans le menu principal, accédez à **Découverte et déploiement → Découverte → Plages IP**.
2. Cliquez sur le nom de la plage IP à laquelle vous souhaitez ajouter un sous-réseau.
3. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Ajouter**.
4. Définissez un sous-réseau soit via son adresse ou un masque, soit en utilisant la première et la dernière adresse IP de la plage IP. Ou, vous pouvez aussi ajouter un sous-réseau existant en cliquant sur le bouton **Parcourir**.
5. Cliquez sur le bouton **Enregistrer**.

   Le nouveau sous-réseau est ajouté à la plage IP.
6. Cliquez sur le bouton **Enregistrer**.

Les nouveaux paramètres de la plage IP sont enregistrés.

Vous pouvez ajouter autant de sous-réseaux que vous le souhaitez. Le chevauchement des plages IP nommées n'est pas autorisé, mais les sous-réseaux sans nom dans une plage IP n'ont pas ces restrictions. Il est possible d'activer et de désactiver l'interrogation de manière individuelle pour chaque plage IP.

Sondage Zeroconf

Ce type de sondage est pris en charge uniquement pour les points de distribution basés sur Linux.

Un point de distribution peut sonder les réseaux qui ont des appareils avec des adresses IPv6. Dans ce cas, les plages IP ne sont pas spécifiées et le point de distribution sonde l'ensemble du réseau en utilisant la mise en réseau sans configuration (également appelée *Zeroconf*). Pour commencer à utiliser Zeroconf, vous devez installer l'utilitaire avahi-browse sur le point de distribution.

Pour activer le sondage du réseau IPv6, procédez comme suit :

1. Dans le menu principal, accédez à **Découverte et déploiement → Découverte → Plages IP**.
2. Cliquez sur le bouton **Propriétés**.
3. Dans la fenêtre qui s'ouvre, activez le commutateur **Utiliser Zeroconf pour sonder les réseaux IPv6**.

Après cela, le point de distribution commence à sonder votre réseau. Dans ce cas, les plages IP spécifiées sont ignorées.

Sondage du contrôleur de domaine

Kaspersky Security Center prend en charge le sondage d'un contrôleur de domaine Microsoft Active Directory et d'un contrôleur de domaine Samba.

Kaspersky Security Center permet de sonder un contrôleur de domaine Samba uniquement à l'aide d'un point de distribution Linux. Pour un contrôleur de domaine Samba, Samba 4 est utilisé comme contrôleur de domaine Active Directory.

Lorsque vous interrogez un contrôleur de domaine, le Serveur d'administration ou un point de distribution récupère des informations sur la structure du domaine, les comptes d'utilisateurs, les groupes de sécurité et les noms DNS des appareils inclus dans le domaine.

Nous vous recommandons d'utiliser le sondage du contrôleur de domaine si tous les appareils en réseau sont membres d'un domaine. Si certains appareils en réseau ne sont pas inclus dans le domaine, ces appareils ne peuvent pas être découverts par le sondage du contrôleur de domaine.

Prérequis

Avant d'interroger un contrôleur de domaine, assurez-vous que vous autorisez les connexions au contrôleur de domaine via un pare-feu ou un serveur proxy. Assurez-vous également que les protocoles suivants sont activés sur le contrôleur de domaine :

- Protocole d'accès léger à l'annuaire (LDAP)
- Couche d'authentification et de sécurité simple (SASL)

  Ce protocole est utilisé si la connexion au contrôleur de domaine est établie à l'aide de l'authentification SASL. Le Serveur d'administration et les points de distribution ne prennent en charge que le mécanisme DIGEST-MD5.
- Lightweight Directory Access Protocol over Secure Sockets Layer (LDAPS)

  Ce protocole est utilisé si vous devez vous connecter au contrôleur de domaine via une connexion chiffrée.

Assurez-vous que les ports suivants sont disponibles sur l'appareil du contrôleur de domaine :

- 389 pour le protocole LDAP et l'authentification simple (y compris SASL)
- 636 pour le protocole LDAPS

Pour tous les hôtes Linux au sein d'un contrôleur de domaine Microsoft Active Directory ou Samba, vous devez spécifier les paramètres `netbios name` et `workgroup` dans le fichier `/etc/samba/smb.conf`. Dans le cas contraire, les résultats du sondage peuvent contenir des hôtes en double.

Sondage du contrôleur de domaine à l'aide du Serveur d'administration

Vous pouvez utiliser le Serveur d'administration pour sonder uniquement un contrôleur de domaine Microsoft Active Directory.

Pour interroger un contrôleur de domaine à l'aide du Serveur d'administration :

1. Dans le menu principal, accédez à **Découverte et déploiement → Découverte → Contrôleurs de domaine**.
2. Cliquez sur **Paramètres de sondage**.

   La fenêtre **Paramètres de sondage du contrôleur de domaine** s'ouvre.
3. Sélectionnez l'option **Activer le sondage du contrôleur de domaine**.
4. Dans la section **Paramètres avancés**, indiquez la zone de sondage :

   - **Sonder le domaine actuel**

     Sélectionnez cette option si vous voulez sonder le domaine auquel appartient Kaspersky Security Center.

   - **Sonder toute la forêt de domaines**

     Sélectionnez cette option si vous voulez sonder la forêt de domaines à laquelle appartient Kaspersky Security Center.

   - **Sonder les domaines indiqués**

     Sélectionnez cette option pour sonder le domaine avec l'adresse et les identifiants indiqués.

5. Le cas échéant, indiquez la programmation du sondage. La période par défaut est une heure. Les données obtenues à l'issue d'un sondage remplacent complètement les anciennes données.

   Les options de programmation du sondage sont disponibles :

   - **Tous les N jours**

     Le sondage s'exécute régulièrement, selon l'intervalle défini en jours, à partir de la date et heure définis.

     Le sondage s'exécute par défaut chaque jour, à partir de la date et de l'heure actuelle du système.

   - **Toutes les N minutes**

     Le sondage s'exécute régulièrement, selon l'intervalle défini en minutes, à partir de l'heure définie.

   - **Par jours de la semaine**

     Le sondage s'exécute régulièrement les jours définis de la semaine, à l'heure indiquée.

   - **Chaque mois, les jours indiqués des semaines sélectionnées**

     Le sondage s'exécute régulièrement les jours définis de chaque mois, à l'heure indiquée.

   - **Lancer les tâches non exécutées**

     Si le Serveur d'administration est éteint ou s'il n'est pas disponible au moment auquel le sondage a été programmé, le Serveur d'administrateur peut soit lancer le sondage immédiatement après que le Serveur d'administration a été allumé ou attendre la prochaine programmation du sondage.

     Si cette option est activée, le Serveur d'administration lance le sondage directement après qu'il a été allumé.

     Si cette option est désactivée, le Serveur d'administration attend la prochaine programmation du sondage.

     Cette option est Inactif par défaut.

   Si vous modifiez les comptes d'utilisateurs dans un groupe de sécurité du domaine, ces modifications seront affichées dans Kaspersky Security Center une heure après le sondage du contrôleur de domaine.

6. Cliquez sur **Enregistrer** pour appliquer les modifications.

7. Si vous souhaitez effectuer le sondage immédiatement, cliquez sur le bouton **Démarrer le sondage**.

Sondage du contrôleur de domaine à l'aide d'un point de distribution

Vous pouvez également sonder un contrôleur de domaine Microsoft Active Directory et un contrôleur de domaine Samba à l'aide d'un point de distribution. Un appareil administré basé sur Windows ou Linux peut servir de point de distribution.

Pour un point de distribution Linux, le sondage d'un contrôleur de domaine Microsoft Active Directory et d'un contrôleur de domaine Samba est pris en charge.
Pour un point de distribution Windows, seule le sondage d'un contrôleur de domaine Microsoft Active Directory est pris en charge.
Le sondage avec un point de distribution Mac n'est pas pris en charge.

Pour configurer le sondage du contrôleur de domaine à l'aide du point de distribution :

1. Ouvrez les propriétés du point de distribution.
2. Sélectionnez la section **Sondage du contrôleur de domaine**.
3. Sélectionnez l'option **Activer le sondage du contrôleur de domaine**.
4. Sélectionnez le contrôleur de domaine que vous souhaitez interroger.

   Si vous utilisez un point de distribution Linux, dans la section **Sonder les domaines indiqués**, cliquez sur **Ajouter**, puis spécifiez l'adresse et les informations d'identification de l'utilisateur du contrôleur de domaine.

   Si vous utilisez un point de distribution Windows, vous pouvez sélectionner une des options suivantes :

   - **Sonder le domaine actuel**
   - **Sonder toute la forêt de domaines**
   - **Sonder les domaines indiqués**
5. Cliquez sur le bouton **Planifier le sondage** pour spécifier les options de planification du sondage si nécessaire.

   Le sondage démarre uniquement selon le calendrier spécifié. Le démarrage manuel du sondage n'est pas disponible.

Une fois le sondage terminé, la structure du domaine sera affichée dans la section **Contrôleurs de domaine**.

Si vous configurez et activez les règles de déplacement de l'appareil, les appareils détectés sont automatiquement inclus dans le groupe **Appareils administrés**. Si aucune règle de déplacement n'est activée, les nouveaux appareils détectés sont automatiquement inclus dans le groupe **Appareils non définis**.

Les comptes d'utilisateurs découverts peuvent être utilisés pour l'authentification de domaine dans Kaspersky Security Center Web Console.

Authentification et connexion au contrôleur de domaine

Authentification et connexion au contrôleur de domaine lors du sondage du domaine

Lors du sondage d'un contrôleur de domaine à l'aide d'un point de distribution Linux, le point de distribution identifie le protocole de connexion pour établir la connexion initiale avec le contrôleur de domaine. Ce protocole sera utilisé pour toutes les connexions futures au contrôleur de domaine. Lors de la connexion initiale avec le contrôleur de domaine, vous pouvez modifier les options de connexion à l'aide des indicateurs de l'Agent d'administration `KLNAG_LDAP_TLS_REQCERT` et `KLNAG_LDAP_SSL_CACERT`. Vous pouvez configurer les indicateurs de l'Agent d'administration à l'aide de klscflag comme décrit dans cet article.

La connexion initiale à un contrôleur de domaine se déroule comme suit :

1. Un point de distribution Linux tente de se connecter au contrôleur de domaine via LDAPS.

   Par défaut, la vérification du certificat n'est pas requise. Définissez l'indicateur `KLNAG_LDAP_TLS_REQCERT` sur 1 pour appliquer la vérification du certificat.

   Valeurs possibles du paramètre `KLNAG_LDAP_TLS_REQCERT` :

   - `0` : le certificat est demandé, mais s'il n'est pas fourni ou si la vérification du certificat a échoué, la connexion TLS est toujours considérée comme créée avec succès (valeur par défaut).
   - `1` : une vérification stricte du certificat du serveur LDAP est requise.

   Par défaut, lorsque l'indicateur `KLNAG_LDAP_SSL_CACERT` n'est pas défini, le chemin d'accès à l'autorité de certification (CA) dépendant du système d'exploitation permet d'accéder à la chaîne de certification. Utilisez l'indicateur `KLNAG_LDAP_SSL_CACERT` pour spécifier un chemin d'accès personnalisé.

2. Si la connexion LDAPS échoue, un point de distribution Linux tente de se connecter au contrôleur de domaine via une connexion TCP non chiffrée en utilisant SASL (DIGEST-MD5).

Configuration des indicateurs

Vous pouvez utiliser l'utilitaire klscflag pour configurer les indicateurs.

Sur un point de distribution Linux, exécutez la ligne de commande, puis remplacez votre répertoire actuel par celui contenant l'utilitaire klscflag. Par défaut, sur le point de distribution Linux, l'utilitaire klscflag se trouve dans /opt/kaspersky/ksc64/sbin.

Par exemple, la commande suivante applique la vérification du certificat :

```
klscflag -fset -pv klnagent -n KLNAG_LDAP_TLS_REQCERT -t d -v 1
```

Configuration d'un contrôleur de domaine Samba

Kaspersky Security Center prend en charge un contrôleur de domaine Linux fonctionnant uniquement sur Samba 4.

Un contrôleur de domaine Samba prend en charge les mêmes extensions de schéma qu'un contrôleur de domaine Microsoft Active Directory. Vous pouvez activer la compatibilité totale d'un contrôleur de domaine Samba avec un contrôleur de domaine Microsoft Active Directory en utilisant l'extension de schéma Samba 4. Il s'agit d'une action facultative.

Nous vous recommandons d'activer la compatibilité totale d'un contrôleur de domaine Samba avec un contrôleur de domaine Microsoft Active Directory. Cela garantira l'interaction correcte entre Kaspersky Security Center et le contrôleur de domaine Samba.

Pour activer la compatibilité totale d'un contrôleur de domaine Samba avec un contrôleur de domaine Microsoft Active Directory :

1. Exécutez la commande suivante pour utiliser l'extension de schéma RFC2307 :

   ```
   samba-tool domain provision --use-rfc2307 --interactive
   ```

2. Activez la mise à jour du schéma dans un contrôleur de domaine Samba. Pour ce faire, ajoutez la ligne suivante au fichier `/etc/samba/smb.conf` :

   ```
   dsdb:schema update allowed = true
   ```

   Si la mise à jour du schéma aboutit à une erreur, vous devez effectuer une restauration complète du contrôleur de domaine qui fait office de maître de schéma.

Pour tous les hôtes Linux au sein d'un contrôleur de domaine Samba, spécifiez le `netbios name` et les paramètres `workgroup` dans le fichier `/etc/samba/smb.conf`. Dans le cas contraire, les résultats du sondage peuvent contenir des hôtes en double.

Configuration des règles de rétention pour les appareils non définis

Une fois le sondage du réseau Windows terminé, les appareils trouvés sont placés dans des sous-groupes du groupe d'administration Appareils non définis. Ce groupe d'administration se trouve à l'emplacement **Découverte et déploiement** → **Découverte** → **Domaines Windows**. Le dossier **Domaines Windows** est le groupe parent. Il contient les groupes enfants nommés après que les domaines et les groupes de travail correspondant ont été trouvés lors du sondage. Le groupe parent peut également contenir le groupe d'administration des appareils mobiles. Vous pouvez configurer les règles de rétention des appareils non définis pour le groupe parent et pour chacun des groupes enfant. Les règles de conservation ne dépendent pas des paramètres de recherche d'appareil et fonctionnent même si la recherche d'appareil est désactivée.

Les règles de conservation des appareils n'affectent pas les appareils dont un ou plusieurs disques sont chiffrés à l'aide du chiffrement du disque. Ces appareils ne sont pas supprimés automatiquement. Vous ne pouvez les supprimer que manuellement. Si vous devez supprimer un appareil doté d'un disque chiffré, commencez par déchiffrer le disque, puis supprimez l'appareil.

Pour configurer les règles de rétention pour les appareils non définis :

1. Dans le menu principal, accédez à **Découverte et déploiement → Découverte → Domaines Windows**.
2. Exécutez une des actions suivantes :
   - Pour configurer les paramètres du groupe parent, cliquez sur le bouton **Propriétés**.

     La fenêtre des propriétés du domaine Windows s'ouvre.
   - Pour configurer les paramètres d'un groupe enfant, cliquez sur son nom.

     La fenêtre des propriétés du groupe enfant s'ouvre.
3. Configurez les paramètres suivants :
   - **Supprimer l'appareil du groupe après une inactivité de plus de (jours)**

     Quand cette option est activée, vous pouvez définir la période à l'issue de laquelle un appareil est supprimé automatiquement du groupe. Cette option est également distribuée par défaut aux groupes enfants. Par défaut, la valeur de cet intervalle est de 7 jours.

     Cette option est activée par défaut.
   - **Hériter du groupe parent**

     Si cette option est activée, la période de conservation pour les appareils dans le groupe actif est héritée du groupe parent et ne peut être modifiée.

     Cette option est disponible uniquement pour les groupes enfant.

     Cette option est activée par défaut.
   - **Forcer l'héritage des groupes enfants**

     Les valeurs des paramètres sont diffusées dans les groupes enfants mais ces paramètres sont verrouillés dans les propriétés des groupes enfants.

     Cette option est Inactif par défaut.
4. Cliquez sur le bouton **Accepter**.

Vos modifications sont enregistrées et appliquées.

Inventaire du matériel

La liste du matériel (**Opérations → Stockages → Matériel**) que vous utilisez pour faire l'inventaire du matériel est alimentée de deux façons : automatiquement et manuellement. Après chaque sondage du réseau, tous les appareils détectés sont automatiquement ajoutés à la liste. Cependant, vous pouvez également ajouter des appareils manuellement si vous ne souhaitez pas sonder le réseau. Vous pouvez ajouter manuellement d'autres appareils à la liste, par exemple des routeurs, des imprimantes ou du matériel informatique.

Il est possible de consulter et de modifier les informations détaillées sur les appareils dans les propriétés de l'appareil.

La liste du matériel détecté peut contenir les types suivants des appareils :

- Ordinateurs
- Appareils mobiles
- Appareils réseau
- Appareils virtuels
- Modules d'ordinateur
- Périphérie d'ordinateur
- Appareils connectés
- Téléphonie VoIP
- Stockages réseau

L'administrateur peut attribuer l'indice *Matériel corporatif* aux appareils détectés. Cet indice peut être manuellement attribué dans les propriétés de l'appareil ou définir les critères pour son attribution automatique. Dans ce cas, l'indice *Matériel corporatif* est attribué selon le type d'appareil.

Kaspersky Security Center permet d'exécuter l'amortissement du matériel. Pour cela, sélectionnez l'option **Retiré du service** dans les propriétés d'un appareil. Un tel appareil ne s'affiche pas dans la liste du matériel.

L'administrateur peut manipuler la liste des contrôleurs logiques programmables (PLC) dans le dossier **Matériel**. Les informations détaillées sur la manipulation des listes de contrôleurs logiques programmables figurent dans le *Manuel de l'utilisateur de Kaspersky Industrial CyberSecurity for Nodes*.

Ajout d'informations sur les nouveaux appareils

Pour ajouter les informations sur les nouveaux appareils dans le réseau, procédez comme suit :

1. Dans le menu principal, accédez à **Opérations → Stockages → Matériel**.
2. Cliquez sur le bouton **Ajouter** pour ouvrir la fenêtre **Nouvel appareil**.
3. Dans la fenêtre **Nouvel appareil**, dans la liste déroulante **Type d'appareil**, sélectionnez le type d'appareil que vous souhaitez ajouter.
4. Cliquez sur le bouton **OK**.

   La fenêtre des propriétés de l'appareil s'ouvre sur la section **Général**.

5. Dans la section **Général**, remplissez les champs de saisie avec les données sur l'appareil. La section **Général** répertorie les paramètres suivants :

   - **&Appareil d'entreprise**. Cochez la case si vous voulez attribuer l'indice *Corporatif* à l'appareil. Avec cet attribut, il est possible de rechercher des appareils dans le dossier **Matériel**.
   - **Retiré du service**. Cochez la case si vous ne voulez pas afficher l'appareil dans la liste des appareils dans le dossier **Matériel**.

6. Cliquez sur le bouton **Appliquer**.

Le nouvel appareil s'affiche dans l'espace de travail de la page **Matériel**.

Configuration des critères de définition des appareils d'entreprise

Pour configurer les critères de définition des appareils d'entreprise, procédez comme suit :

1. Dans le menu principal, accédez à **Opérations** → **Stockages** → **Matériel**.
2. En haut de la page **Matériel**, cliquez sur le lien **Configurer la règle pour les appareils d'entreprise**.

   Un panneau **Configurer la règle pour les appareils d'entreprise** est invoqué.
3. Dans le panneau **Configurer la règle pour les appareils d'entreprise**, activez l'option **Établir &automatiquement l'Attribut Appareil d'entreprise pour l'appareil**. Spécifiez les types d'appareils auxquels l'attribut *Entreprise* est attribué automatiquement.

   Cette option affecte uniquement les appareils qui ont été ajoutés via l'interrogation du réseau. Pour les appareils ajoutés manuellement, définissez l'indice *Entreprise* manuellement.
4. Cliquez sur le bouton **OK**.

Les critères de détection des appareils d'entreprise sont configurés.

Applications Kaspersky : licence et activation

Cette section décrit les possibilités de Kaspersky Security Center sur l'utilisation des clés de licence des applications administrées de Kaspersky.

Kaspersky Security Center permet de diffuser de manière centralisée les clés de licence des applications de Kaspersky sur les appareils clients, suivre l'utilisation des clés et de prolonger la durée de validité des licences.

Lors de l'ajout de la clé de licence à l'aide de Kaspersky Security Center, les propriétés de la clé de licence sont enregistrées sur le Serveur d'administration. Sur la base de ces informations, l'application crée un rapport sur les clés de licence utilisées et notifie l'administrateur de l'expiration de la durée de validité des licences et du dépassement des restrictions de licence énoncées dans les propriétés des clés de licence. Vous pouvez configurer les paramètres de notifications sur l'utilisation des clés de licence dans la composition des paramètres du Serveur d'administration.

Licence des applications administrées

Les applications Kaspersky installées sur les appareils administrés doivent disposer d'une licence sous la forme d'un fichier clé ou d'un code d'activation pour chaque application. Le déploiement d'un fichier clé ou d'un code d'activation peut s'effectuer comme suit :

- Déploiement automatique
- Le paquet d'installation d'une application administrée
- La tâche *Ajout de clé de licence* pour une application administrée
- L'activation manuelle d'une application administrée

Vous pouvez ajouter une nouvelle clé de licence active ou de réserve par l'une des méthodes répertoriées ci-dessus. Une application Kaspersky utilise une clé active à l'instant présent et stocke une clé de réserve à appliquer après l'expiration de la clé active. L'application pour laquelle vous ajoutez une clé de licence définit si la clé est active ou de réserve. La définition de clé ne dépend pas de la méthode que vous utilisez pour ajouter une nouvelle clé de licence.

Déploiement automatique

Si vous utilisez différentes applications administrées et que vous devez absolument déployer un fichier clé ou un code d'activation spécifique sur les appareils, utilisez d'autres modes de déploiement du code d'activation ou du fichier clé.

Kaspersky Security Center permet automatiquement de diffuser les clés de licence se trouvant sur les appareils. Par exemple, le stockage du Serveur d'administration contient trois clés de licence. Vous avez sélectionné la case **Distribuer automatiquement la clé de licence sur les appareils administrés** pour les trois clés de licence. Sur les appareils de l'entreprise, l'application de sécurité de Kaspersky, par exemple, Kaspersky Endpoint Security for Windows est installée. Un nouvel appareil a été détecté sur lequel il faut diffuser la clé de licence. L'application définit pour cet appareil, par exemple, que deux des clés de licence du stockage, la clé de licence dénommée *Clé_1* et la clé de licence dénommée *Clé_2* peuvent être déployées. Une de ces clés de licence est déployée sur l'appareil. Une des clés de licence adaptées est diffusée, et dans ce cas, il n'est pas possible de savoir laquelle de ces deux clés sera diffusée sur l'appareil car le déploiement automatique des clés de licence ne prévoit pas l'intervention de l'administrateur.

Lors du déploiement de la clé, les appareils sont recalculés pour cette clé de licence. Vous devez vous assurer que le nombre d'appareils sur lequel la clé de licence est diffusée ne dépasse pas la restriction de licence. Si le nombre d'appareils dépasse la restriction de licence, l'état *Critique* est attribué à tous les appareils non couverts par la licence.

Avant le déploiement, le fichier clé ou le code d'activation doit être ajouté au Stockage du Serveur d'administration.

Instructions pour :

- Console d'administration :
  - Ajout de la clé de licence dans le stockage du Serveur d'administration
  - Diffusion automatique de la clé de licence

  ou

- Kaspersky Security Center Web Console :
  - Ajout de la clé de licence dans le stockage du Serveur d'administration
  - Diffusion automatique de la clé de licence

Veuillez noter qu'une clé de licence diffusée automatiquement peut ne pas s'afficher dans le stockage du Serveur d'Administration virtuel dans les cas suivants :

- La clé de licence n'est pas valide pour l'application.
- Le Serveur d'administration virtuel n'a pas d'appareils administrés.
- La clé de licence a déjà été utilisée pour des appareils administrés par un autre Serveur d'administration virtuel et la limite du nombre d'appareils a été atteinte.

Ajout d'un fichier clé ou d'un code d'activation dans le paquet d'installation de l'application administrée

Pour des raisons de sécurité, cette option n'est pas recommandée. Un fichier clé ou un code d'activation ajouté à un paquet d'installation peut être compromis.

En cas d'installation d'une application administrée à l'aide du paquet d'installation, vous pouvez indiquer le code d'activation ou le fichier clé dans ce paquet d'installation ou dans la stratégie de l'application. La clé de licence est diffusée sur les appareils administrés lors de la synchronisation ultérieure de l'appareil avec le Serveur d'administration.

Instructions pour :

- Console d'administration :
  - Génération du paquet d'installation
  - Installation des applications sur les appareils clients

  ou

- Kaspersky Security Center Web Console : Ajout d'une clé de licence à un paquet d'installation

Déploiement par la tâche Ajout de clé de licence pour une application administrée

En cas de l'utilisation de la tâche *Ajout de la clé de licence* de l'application administrée, vous pouvez choisir la clé de licence qu'il faut diffuser sur les appareils, et sélectionner les appareils de la manière qui vous convient, par exemple, en sélectionnant un groupe d'administration ou une sélection d'appareils.

Avant le déploiement, le fichier clé ou le code d'activation doit être ajouté au Stockage du Serveur d'administration.

Instructions pour :

- Console d'administration :
  - Ajout de la clé de licence dans le stockage du Serveur d'administration
  - Déploiement d'une clé de licence sur les appareils clients

  ou
- Kaspersky Security Center Web Console :
  - Ajout de la clé de licence dans le stockage du Serveur d'administration
  - Déploiement d'une clé de licence sur les appareils clients

Ajout d'un code d'activation ou d'un fichier clé manuellement sur les appareils

Vous pouvez activer l'application Kaspersky installée localement, avec les outils fournis dans l'interface de l'application. Consultez la documentation de l'application installée.

Ajout de la clé de licence dans le stockage du Serveur d'administration

Pour ajouter une clé de licence dans le stockage du Serveur d'administration, procédez comme suit :

1. Dans le menu principal, accédez à **Opérations → Licence → Licences pour les logiciels de Kaspersky**.
2. Cliquez sur le bouton **Ajouter**.
3. Choisissez ce que vous voulez ajouter :
   - **Ajouter un fichier clé**

     Cliquez sur le bouton **Sélectionner le fichier clé** et naviguez jusqu'au fichier .key que vous souhaitez ajouter.
   - **Saisir un code d'activation**

     Indiquez le code d'activation dans le champ texte et cliquez sur le bouton **Envoyer**.
4. Cliquez sur le bouton **Fermer**.

La ou les clé(s) de licence sont ajoutées au stockage du serveur d'administration.

Ajout de la clé de licence du Serveur d'administration

Pour ajouter une clé de licence du Serveur d'administration, procédez comme suit :

1. Dans le menu contextuel Serveur d'administration, sélectionnez l'option **Propriétés**.
2. Dans la fenêtre des propriétés du Serveur d'administration qui s'ouvre, sélectionnez la section **Clés de licence**.
3. Dans la section **Clé de licence active**, cliquez sur le bouton **Modifier**.
4. Dans la fenêtre qui s'ouvre, ajoutez une clé de licence en cliquant sur le bouton **Ajouter**.

   Assistant d'ajout de clé de licence démarre.

Une fois l'Assistant terminé, vous pouvez vérifier si les fonctionnalités s'affichent dans la Console d'administration conformément à la licence correspondante.

Déploiement d'une clé de licence sur les appareils clients

Kaspersky Security Center Web Console vous permet de distribuer une clé de licence aux appareils clients automatiquement ou via la tâche **Activation de l'application**. Vous pouvez utiliser la tâche pour distribuer des clés à un groupe d'appareils particulier. Lors de la distribution de la clé de licence via la tâche, la limite de licences sur le nombre d'appareils n'est pas prise en compte. La distribution automatique des clés permet d'interrompre automatiquement la distribution d'une clé de licence lorsque la limite de licence est atteinte.

Si vous activez la distribution automatique d'une clé de licence, ne créez pas de tâche **Activation de l'application** pour distribuer cette clé sur les appareils clients. Dans le cas contraire, la charge sur le Serveur d'administration augmentera en raison de la fréquence des synchronisations.

Avant le déploiement, ajoutez une clé de licence au stockage du Serveur d'administration.

*Pour diffuser une clé de licence sur les appareils clients via la tâche **Activation de l'application**, procédez comme suit :*

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Tâches**.
2. Cliquez sur **Ajouter**.

   Ceci permet de lancer l'**Assistant de création d'une tâche**. Parcourez les étapes de l'assistant à l'aide du bouton **Suivant**.
3. Dans la liste déroulante **Application**, sélectionnez l'application pour laquelle vous voulez ajouter une clé de licence.
4. À partir de la liste **Type de tâche**, sélectionnez la tâche **Activation de l'application**.
5. Dans le champ **Nom de la tâche**, indiquez le nom de la nouvelle tâche.
6. Sélectionnez les appareils auxquels les tâches seront affectées.

7. À l'étape **Sélection d'une clé de licence** de l'Assistant, cliquez sur le lien **Ajouter une clé** pour ajouter la clé de licence.

8. Dans le volet de l'ajout de clé, ajoutez la clé de licence à l'aide d'une des options suivantes :

   Il faut ajouter la clé de licence uniquement si vous ne l'avez pas ajoutée au stockage du Serveur d'administration avant la création de la tâche **Activation de l'application**.

   - Sélectionnez l'option **Saisir un code d'activation** pour saisir le code d'activation, puis procédez comme suit :

     a. Indiquez le code d'activation, puis cliquez sur le bouton **Envoyer**.

     Les informations sur la clé de licence apparaissent dans le volet d'ajout de clé.

     b. Cliquez sur le bouton **Enregistrer**.

     Si vous souhaitez diffuser automatiquement la clé de licence sur les appareils administrés, activez l'option **Distribuer automatiquement la clé de licence sur les appareils administrés**.

     La fenêtre d'ajout de clés se ferme.

   - Sélectionnez l'option **Ajouter un fichier clé** pour ajouter un fichier clé, puis procédez comme suit :

     a. Cliquez sur le bouton **Sélectionner le fichier clé**.

     b. Dans la fenêtre qui s'ouvre, sélectionnez un fichier clé, puis cliquez sur le bouton **Ouvrir**.

     Les informations sur la clé de licence apparaissent dans le volet d'ajout d'une clé de licence.

     c. Cliquez sur le bouton **Enregistrer**.

     Si vous souhaitez diffuser automatiquement la clé de licence sur les appareils administrés, activez l'option **Distribuer automatiquement la clé de licence sur les appareils administrés**.

     La fenêtre d'ajout de clés se ferme.

9. Sélectionnez la clé de licence dans le tableau des clés.

10. À l'étape **Informations sur la licence** de l'Assistant, décochez la case par défaut **Utiliser comme clé de réserve** si vous souhaitez remplacer la clé de licence active.

    Par exemple, cela est nécessaire lorsque l'organisation change et que la clé d'une autre organisation est requise sur l'appareil, ou si la clé a été réémise et qu'une nouvelle licence expire avant la licence actuelle. Pour éviter les erreurs, il convient de décocher la case **Utiliser comme clé de réserve**.

    Si vous souhaitez en savoir plus sur les problèmes qui peuvent survenir lors de l'ajout d'une clé de licence à Kaspersky Security Center et les moyens de les résoudre, consultez la Base de connaissances de Kaspersky Security Center.

11. À l'étape **Fin de la création de la tâche** de l'Assistant, activez l'option **Ouvrir les détails de la tâche à la fin de la création** pour modifier les paramètres de la tâche par défaut.

    Si vous n'activez pas cette tâche, la tâche sera créée selon les paramètres par défaut. Vous pourrez modifier ces paramètres par défaut plus tard.

12. Cliquez sur le bouton **Terminer**.

    L'Assistant crée la tâche. Si vous avez activé l'option **Ouvrir les détails de la tâche à la fin de la création**, la fenêtre des propriétés de la tâche s'ouvre automatiquement. Cette fenêtre permet de définir les paramètres généraux de la tâche et, si nécessaire, de modifier les paramètres définis lors de la création de la tâche.

    > Vous pouvez également ouvrir la fenêtre des propriétés de la tâche en cliquant sur le nom de la tâche créée dans la liste des tâches.

    La tâche est créée et configurée, et s'affiche dans la liste des tâches.

13. Pour exécuter la tâche, sélectionnez-la dans la liste des tâches, puis cliquez sur le bouton **Démarrer**.

    Vous pouvez également programmer le lancement d'une tâche dans l'onglet **Programmation** de la fenêtre des propriétés de la tâche.

    Pour obtenir la description détaillée des paramètres du lancement programmé, consultez les paramètres généraux de la tâche.

Une fois la tâche terminée, la clé de licence est déployée sur les appareils sélectionnés.

Diffusion automatique de la clé de licence

Kaspersky Security Center permet de diffuser automatiquement sur les appareils administrés les clés de licence placées dans le stockage des clés sur le Serveur d'administration.

Afin de diffuser automatiquement une clé de licence sur les appareils administrés, procédez comme suit :

1. Dans le menu principal, accédez à **Opérations → Licence → Licences pour les logiciels de Kaspersky**.
2. Sélectionnez la clé que vous souhaitez diffuser automatiquement sur l'appareil.
3. Dans la fenêtre ouverte des propriétés de la clé de licence, cochez la case **Distribuer automatiquement la clé de licence sur les appareils administrés**.
4. Cliquez sur le bouton **Enregistrer**.

La clé de licence est automatiquement distribuée à tous les appareils compatibles.

La diffusion de la clé de licence est exécutée via les moyens de l'Agent d'administration. Aucune tâche de distribution de la clé de licence n'est créée pour l'application.

Lors de la distribution automatique de la clé de licence, la limite de licences sur le nombre d'appareils est prise en compte. La restriction de licence est définie dans les propriétés de la clé de licence. Si la limite liée à la restriction de licence est atteinte, la diffusion de la clé de licence sur les appareils s'arrête automatiquement.

Veuillez noter qu'une clé de licence diffusée automatiquement peut ne pas s'afficher dans le stockage du Serveur d'Administration virtuel dans les cas suivants :

- La clé de licence n'est pas valide pour l'application.
- Le Serveur d'administration virtuel n'a pas d'appareils administrés.
- La clé de licence a déjà été utilisée pour des appareils administrés par un autre Serveur d'administration virtuel et la limite du nombre d'appareils a été atteinte.

Le Serveur d'administration virtuel distribue automatiquement les clés de licence depuis son stockage et depuis le stockage du Serveur d'administration. Voici nos recommandations :

- Utilisez la tâche *Ajouter une clé de licence* pour sélectionner la clé de licence qui doit être déployée sur les appareils.
- Évitez de désactiver l'option **Autoriser le déploiement automatique des clés de licence de ce Serveur d'administration virtuel sur ses appareils** dans les paramètres du Serveur d'administration virtuel. Sinon, le Serveur d'administration virtuel ne distribuera pas les clés de licence aux appareils, y compris les clés de licence du stockage du Serveur d'administration.

Si vous sélectionnez la case **Distribuer automatiquement la clé de licence sur les appareils administrés** dans la fenêtre des propriétés de la clé de licence, une clé de licence est immédiatement distribuée sur votre réseau. Si vous ne sélectionnez pas cette option, vous pouvez distribuer une clé de licence plus tard à l'aide d'une tâche.

La diffusion automatique des clés de licence configurée sur le Serveur d'administration principal ne s'étend pas aux appareils administrés par les Serveurs d'administration secondaires non virtuels.

Consultation des informations sur les clés de licence utilisées

Pour voir la liste des clés de licence ajoutées au stockage du Serveur d'administration :

Dans le menu principal, accédez à **Opérations → Licence → Licences pour les logiciels de Kaspersky**.

La liste affichée contient les fichiers clés et les codes d'activation ajoutés au stockage du Serveur d'administration.

Pour voir les informations détaillées d'une clé de licence :

1. Dans le menu principal, accédez à **Opérations → Licence → Licences pour les logiciels de Kaspersky**.
2. Cliquez sur le nom de la clé de licence concernée.

Dans la fenêtre des propriétés de la clé de licence qui s'ouvre, vous pouvez voir :

- Dans l'onglet **Général**, les principales informations sur la clé de licence
- Dans l'onglet **Appareils**, la liste des appareils clients où la clé de licence a été utilisée pour l'activation de l'application Kaspersky installée

Pour voir quelles clés de licence sont déployées sur un appareil client spécifique :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Appareils administrés**.
2. Cliquez sur le nom de l'appareil concerné.
3. Dans la fenêtre des propriétés de l'appareil qui s'ouvre, sélectionnez l'onglet **Applications**.
4. Cliquez sur le nom de l'application pour laquelle vous souhaitez voir les informations sur la clé de licence.
5. Dans les propriétés de la fenêtre d' application, sélectionnez l'onglet **Général**, puis ouvrez la section **Licence**.

Les informations principales sur les clés de licence actives et de réserve s'affichent.

Pour définir les paramètres actualisés des clés de licence du Serveur d'administration virtuel, le Serveur d'administration envoie une requête sur les serveurs d'activation de Kaspersky au moins une fois par jour. Si l'accès aux serveurs via le DNS système n'est pas possible, l'application utilise les serveurs DNS publics.

Suppression d'une clé de licence du stockage

Lorsque vous supprimez la clé de licence active pour une fonctionnalité supplémentaire du Serveur d'administration, par exemple la gestion des vulnérabilités et des correctifs ou l'administration des appareils mobiles : la fonction correspondante devient indisponible. Si une clé de licence de réserve a été ajoutée, la clé de licence de réserve devient automatiquement la clé de licence active après la suppression de l'ancienne clé de licence active.

Lorsque vous supprimez la clé de licence active déployée sur un appareil administré, l'application continue de fonctionner sur cet appareil administré.

Pour supprimer un fichier clé ou un code d'activation du stockage du Serveur d'administration, procédez comme suit :

1. Vérifiez que le Serveur d'administration n'utilise pas un fichier clé ou un code d'activation que vous souhaitez supprimer. Si le Serveur d'administration le fait, vous ne pouvez pas supprimer la clé. Pour effectuer le contrôle :
   a. Dans le menu principal, cliquez sur l'icône paramètres ( ) en face du nom du Serveur d'administration requis.

      La fenêtre des propriétés du Serveur d'administration s'ouvre.

   b. Sous l'onglet **Général**, sélectionnez la section **Clés de licence**.

   c. Si le fichier clé ou le code d'activation requis s'affiche dans la section qui s'ouvre, cliquez sur le bouton **Supprimer la clé de licence active**, puis confirmez l'opération. Après cela, le Serveur d'administration n'utilise pas la clé de licence supprimée, mais la clé reste dans le stockage du Serveur d'administration. Si le fichier clé ou le code d'activation requis ne s'affiche pas, le Serveur d'administration ne l'utilise pas.
2. Dans le menu principal, accédez à **Opérations** → **Licence** → **Licences pour les logiciels de Kaspersky**.
3. Sélectionnez le fichier clé ou le code d'activation requis, puis cliquez sur le bouton **Supprimer**.

Le fichier clé ou le code d'activation sélectionnés que vous voulez supprimer du stockage.

Vous pouvez ajouter de nouveau la clé de licence supprimée ou ajouter une autre clé de licence.

Révocation d'un Contrat de licence utilisateur final

Si vous décidez de ne plus protéger certains de vos appareils clients, vous pouvez révoquer le Contrat de licence utilisateur final (CLUF) pour toute application de Kaspersky administrée. Vous devez désinstaller l'application sélectionnée avant de révoquer son CLUF.

Les CLUF qui ont été acceptés sur un Serveur d'administration virtuel peuvent être révoqués sur le Serveur d'administration virtuel ou sur le Serveur d'administration principal. Les CLUF qui ont été acceptés sur un Serveur d'administration principal ne peuvent être révoqués que sur le Serveur d'administration principal.

Pour révoquer un CLUF pour les applications Kaspersky administrées :

1. Ouvrez la fenêtre des propriétés du Serveur d'administration qui s'ouvre et, sous l'onglet **Général**, sélectionnez la section **Contrats de licence utilisateur final**.

   Une liste des CLUF acceptés s'affiche lors de la création des paquets d'installation, lors de l'installation transparente des mises à jour ou lors du déploiement de Kaspersky Security for Mobile.

2. Dans la liste, sélectionnez le CLUF que vous souhaitez révoquer.

   Vous pouvez afficher les propriétés suivantes du CLUF :

   - Date d'acceptation du CLUF
   - Nom de l'utilisateur ayant accepté le CLUF

3. Cliquez sur la date d'acceptation d'un CLUF pour ouvrir la fenêtre de propriétés de celui-ci, qui affiche les données suivantes :

   - Nom de l'utilisateur ayant accepté le CLUF
   - Date d'acceptation du CLUF
   - Identifiant unique (UID) du CLUF
   - Texte intégral du CLUF
   - Liste des objets (paquets d'installation, mises à jour continues, applications mobiles) liés au CLUF et leurs noms et types respectifs

4. Dans la partie inférieure de la fenêtre des propriétés du CLUF, cliquez sur le bouton **Révoquer le Contrat de licence**.

   S'il existe des objets (paquets d'installation et leurs tâches respectives) qui empêchent la révocation du CLUF, la notification correspondante s'affiche. Il est impossible de procéder à la révocation avant d'avoir supprimé ces objets.

   Une fenêtre s'ouvre et vous informe que vous devez d'abord désinstaller l'application de Kaspersky correspondant au CLUF.

5. Cliquez sur le bouton pour confirmer la révocation.

Le CLUF est révoqué. Celui-ci n'est plus affiché dans la liste des Contrats de licence dans la section **Contrats de licence utilisateur final**. La fenêtre des propriétés du CLUF se ferme ; l'application n'est plus installée.

Renouvellement des licences des applications Kaspersky

Vous pouvez renouveler une licence d'application Kaspersky qui a expiré ou est sur le point d'expirer (sous moins de 30 jours).

Pour renouveler une licence expirée ou une licence sur le point d'expirer :

1. Réalisez une des opérations suivantes :

   - Dans le menu principal, accédez à **Opérations → Licence → Licences pour les logiciels de Kaspersky**.
   - Dans le menu principal, accédez à **Surveillance et rapports → Tableau de bord**, puis cliquez sur le lien **Afficher les licences arrivant à expiration** à côté d'une notification.

   La fenêtre **Licences pour les logiciels de Kaspersky** s'ouvre, dans laquelle vous pouvez afficher et renouveler les licences.

2. Cliquez sur le lien **Renouveler la licence** en regard de la licence requise.

   En cliquant sur un lien de renouvellement de licence, vous acceptez de transférer à Kaspersky les informations suivantes concernant Kaspersky Security Center : sa version, la localisation que vous utilisez, l'ID de licence du logiciel (c'est-à-dire l'ID de la licence que vous renouvelez) et si vous avez acheté la licence via une entreprise partenaire ou non.

3. Dans la fenêtre du service de renouvellement de licence qui s'ouvre, suivez les instructions pour renouveler une licence.

   La licence est renouvelée.

Dans Kaspersky Security Center Web Console, les notifications s'affichent lorsqu'une licence est sur le point d'expirer, selon le calendrier suivant :

- 30 jours avant l'expiration
- 7 jours avant l'expiration
- 3 jours avant l'expiration
- 24 heures avant l'expiration
- Lorsqu'une licence a expiré

Utilisation de la place de marché de Kaspersky pour choisir les solutions d'entreprise de Kaspersky

Place de marché est une section du menu principal qui vous permet d'afficher toute la gamme de solutions professionnelles Kaspersky, de sélectionner celles dont vous avez besoin et de passer à l'achat sur le site Web de Kaspersky. Vous pouvez utiliser des filtres pour afficher uniquement les solutions qui correspondent à votre organisation et aux exigences de votre système de sécurité informatique. Lorsque vous sélectionnez une solution, Kaspersky Security Center vous redirige vers la page Web correspondante sur le site Web de Kaspersky pour en savoir plus sur cette solution. Chaque page Web vous permet de procéder à l'achat ou contient des instructions sur le processus d'achat.

Dans la section **Place de marché**, vous pouvez filtrer les solutions Kaspersky en utilisant les critères suivants :

- Nombre d'appareils (terminaux, serveurs et autres types de ressources) que vous souhaitez protéger :
  - 50 – 250
  - 250 – 1000
  - Plus de 1000
- Niveau de maturité de l'équipe de sécurité informatique de votre organisation :
  - **Foundations**

    Ce niveau est typique des entreprises qui n'ont qu'une équipe informatique. Le nombre maximum possible de menaces est bloqué automatiquement.
  - **Optimum**

    Ce niveau est typique des entreprises qui ont une fonction de sécurité informatique particulière au sein de l'équipe informatique. À ce niveau, les entreprises ont besoin de solutions leur permettant de contrer les menaces liées aux produits de base et les menaces qui contournent les mécanismes de prévention existants.
  - **Expert**

    Ce niveau est typique des entreprises avec des environnements informatiques complexes et distribués. L'équipe de sécurité informatique est mature ou l'entreprise dispose d'une équipe SOC (Security Operations Center). Les solutions requises permettent aux entreprises de contrer les menaces complexes et les attaques ciblées.
- Types de ressources que vous souhaitez protéger :
  - **Terminaux :** postes de travail des salariés, machines physiques et virtuelles, systèmes embarqués
  - **Serveurs :** serveurs physiques et virtuels
  - **Cloud :** environnements cloud publics, privés ou hybrides ; services cloud
  - **Réseau :** réseau local, infrastructure informatique
  - **Service :** services liés à la sécurité fournis par Kaspersky

Pour rechercher et acheter une solution d'entreprise Kaspersky, procédez comme suit :

1. Dans le menu principal, accédez à **Place de marché**.

   Par défaut, la section affiche toutes les solutions professionnelles Kaspersky disponibles.

2. Pour afficher uniquement les solutions qui conviennent à votre organisation, sélectionnez les valeurs requises dans les filtres.

3. Cliquez sur la solution que vous souhaitez acheter ou à propos de laquelle vous souhaitez en savoir plus.

Vous serez redirigé vers la page Internet de la solution. Vous pouvez suivre les instructions indiquées à l'écran pour procéder à l'achat.

Configuration de la protection réseau

Cette section fournit des informations sur la configuration manuelle des stratégies et des tâches, sur les rôles des utilisateurs et sur la création d'une structure de groupe d'administration et d'une hiérarchie des tâches.

Scénario : Configuration de la protection réseau

L'Assistant de démarrage rapide de l'application crée des stratégies et des tâches en utilisant les paramètres par défaut. Ces paramètres peuvent s'avérer imparfaits, ou même être interdits par l'organisation. Par conséquent, nous vous recommandons d'adapter ces stratégies et tâches et de créer d'autres stratégies et tâches, si elles sont nécessaires à votre réseau.

Prérequis

Avant de démarrer, assurez-vous que vous avez :

- Installé le Serveur d'administration de Kaspersky Security Center
- Installé Kaspersky Security Center Web Console (facultatif)
- Achevé le scénario d'installation principal de Kaspersky Security Center
- Achevé l'Assistant de configuration initiale de l'application ou créé manuellement les stratégies et tâches suivantes dans le groupe d'administration **Appareils administrés** :
  - La stratégie de Kaspersky Endpoint Security
  - La tâche de groupe de mise à jour de Kaspersky Endpoint Security
  - La stratégie de l'Agent d'administration
  - Tâche *Recherche de vulnérabilités et de mises à jour requises*

La configuration de la protection réseau se fait par étapes :

1. **Configuration et propagation des stratégies et des profils de stratégie de Kaspersky**

Pour configurer et propager les paramètres des applications Kaspersky installées sur les appareils administrés, deux méthodes différentes de gestion de la sécurité sont possibles : centrés sur l'utilisateur ou sur l'appareil. Ces deux méthodes peuvent aussi être associées. Pour mettre en œuvre une gestion de la sécurité centrée sur le périphérique, vous pouvez utiliser les outils fournis dans la console d'administration basée sur Microsoft Management Console ou Kaspersky Security Center Web Console. L'administration de la sécurité centrée sur l'utilisateur ne peut être mise en œuvre par via Kaspersky Security Center Web Console.

2. **Configuration des tâches de gestion à distance des applications Kaspersky**

   Vérifiez les tâches créées avec l'assistant de démarrage rapide de l'application et adaptez si nécessaire.

   Instructions pour :

   - Console d'administration :
     - Paramétrage de la tâche de groupe de mise à jour de Kaspersky Endpoint Security
     - Planification de la tâche Recherche de vulnérabilités et des mises à jour requises
   - Kaspersky Security Center Web Console :
     - Paramétrage de la tâche de groupe de mise à jour de Kaspersky Endpoint Security
     - La tâche Recherche de vulnérabilités et de mises à jour requises est créée

   Le cas échéant, créez des tâches supplémentaires gérer les applications Kaspersky installées sur les machines clientes.

3. **Évaluation et limitation de la charge d'événements sur la base de données**

   Les informations sur les événements qui se produisent pendant le fonctionnement des applications administrées sont transmises de l'appareil client et enregistrées dans la base de données du Serveur d'administration. Pour réduire la charge sur le Serveur d'administration, évaluez et limitez le nombre maximal d'événements stockables dans la base de données.

   Instructions pour :

   - Console d'administration : Définition du nombre maximum d'événements
   - Kaspersky Security Center Web Console : Définition du nombre maximum d'événements

Résultats

À la fin de ce scénario, votre réseau sera protégé par la configuration des applications, tâches et événements de Kaspersky reçus par le serveur d'administration :

- Les applications de Kaspersky sont configurées en fonction des stratégies et des profils de stratégie.
- Les applications sont administrées via un ensemble de tâches.
- Le nombre maximal d'événements pouvant être stockés dans la base de données est défini.

Lorsque la configuration de la protection est terminée, vous pouvez procéder à la configuration des mises à jour régulières des bases de données et des applications Kaspersky.

Pour en savoir plus sur la configuration des réponses automatiques aux menaces détectées par Kaspersky Sandbox, veuillez consulter l'Aide en ligne de Kaspersky Sandbox 2.0.

À propos des méthodes d'administration de la sécurité centrées sur l'appareil et l'utilisateur

Vous pouvez gérer les paramètres de sécurité du point de vue des fonctionnalités de l'appareil et des rôles utilisateurs. La première approche s'appelle *gestion de la sécurité centrée sur l'appareil* et la seconde s'appelle *gestion de la sécurité centrée sur l'utilisateur*. Pour appliquer différents paramètres d'application à différents appareils, vous pouvez utiliser un type d'administration ou les deux types d'administration ensemble. Pour mettre en œuvre une gestion de la sécurité centrée sur l'appareil, vous pouvez utiliser les outils fournis dans la Console d'administration basée sur Microsoft Management Console ou Kaspersky Security Center Web Console. L'administration de la sécurité centrée sur l'utilisateur ne peut être mise en œuvre par via la Kaspersky Security Center Web Console.

La gestion de la sécurité centrée sur l'appareil vous permet d'appliquer différents paramètres d'application de sécurité aux appareils administrés en fonction de leurs caractéristiques. Par exemple, vous pouvez appliquer différents paramètres aux appareils alloués à des groupes d'administration différents. Vous pouvez également différencier les appareils en fonction de leur utilisation dans Active Directory ou de leurs spécifications matérielles.

La gestion de la sécurité centrée sur l'utilisateur vous permet d'appliquer différents paramètres d'application de sécurité à différents rôles d'utilisateur. Vous pouvez créer plusieurs rôles d'utilisateur, attribuer un rôle d'utilisateur approprié à chaque utilisateur et définir différents paramètres d'application pour les appareils appartenant à des utilisateurs dotés de rôles différents. Ainsi, vous souhaitez peut-être appliquer des paramètres des applications divergents pour les appareils des comptables et des collaborateurs des ressources humaines (RH). Par conséquent, lorsque l'administration de la sécurité centrée sur l'utilisateur est mise en œuvre, chaque département (les départements de comptabilité et RH) dispose de sa propre configuration de paramètres pour gérer les applications de Kaspersky. Une configuration de paramètres définit les paramètres d'application pouvant être modifiés par les utilisateurs et ceux définis de manière obligatoire et verrouillés par l'administrateur.

Utilisez une gestion de la sécurité centrée sur l'utilisateur pour pouvoir appliquer des paramètres d'application spécifiques pour des utilisateurs individuels. Cela peut être nécessaire lorsqu'un employé a un rôle unique dans l'entreprise ou lorsque vous souhaitez surveiller les problèmes de sécurité liés aux appareils d'une personne en particulier. Selon le rôle de cet employé dans l'entreprise, vous pouvez étendre ou limiter les droits de cette personne pour modifier les paramètres de l'application. Par exemple, vous souhaiterez peut-être étendre les droits d'un administrateur système qui gère les appareils clients d'une agence locale.

Il est également possible de combiner l'administration de la sécurité centrée sur l'appareil et celle centrée sur l'utilisateur. Par exemple, vous pouvez configurer une stratégie pour une application définie pour chaque groupe d'administration, puis créer des profils des stratégies pour un ou plusieurs rôles d'utilisateurs de votre entreprise. Dans ce cas, les stratégies et les profils de stratégie s'appliquent selon l'ordre suivant :

1. Les stratégies créées pour la gestion de la sécurité centrée sur l'appareil s'appliquent.
2. Elles sont modifiées par les profils de stratégie selon les priorités du profil de stratégie.
3. Les stratégies sont modifiées par les profils de stratégie associés aux rôles d'utilisateur.

Configuration et diffusion des stratégies : approche centrée sur l'appareil

Quand vous aurez terminé ce scénario, les applications seront configurées sur tous les appareils administrés conformément aux stratégies et aux profils de stratégie de l'application que vous avez définis.

Prérequis

Avant de commencer, vérifiez que vous avez installé le Serveur d'administration de Kaspersky Security Center et Kaspersky Security Center Web Console (facultatif). Si vous avez installé la Kaspersky Security Center Web Console, vous pouvez aussi vouloir la gestion de la sécurité centrée sur l'utilisateur comme alternative ou option supplémentaire à l'approche centrée sur l'appareil.

Étapes

Le scénario d'administration des applications de Kaspersky axé sur l'appareil comprend les étapes suivantes :

1. **Configuration des stratégies des applications**

   Configurez les paramètres pour les applications de Kaspersky installées sur les appareils administrés par la création d'une stratégie pour chaque application. L'ensemble de ces stratégies seront propagées sur les appareils clients.

   Si vous configurez la protection de votre réseau dans l'Assistant de configuration initiale de l'application, Kaspersky Security Center crée la stratégie par défaut pour les applications suivantes :

   - Kaspersky Endpoint Security for Windows : pour les appareils clients Windows
   - Kaspersky Endpoint Security for Linux : pour les appareils clients Linux

   Si vous terminez cette procédure de configuration avec l'assistant, vous ne devez pas créer une nouvelle stratégie pour cette application. Continuez vers la configuration manuelle d'une stratégie de Kaspersky Endpoint Security.

   Si vous disposez d'une structure hiérarchique de plusieurs Serveurs d'administration et/ou groupes d'administration, les Serveurs d'administration secondaires et les groupes d'administration enfants héritent des stratégies du Serveur d'administration principal par défaut. Vous pouvez forcer l'héritage par les groupes enfants et les Serveurs d'administration secondaires pour empêcher toute modification des paramètres configurés dans la stratégie en amont. Si vous voulez imposer l'héritage d'une partie uniquement des paramètres, vous pouvez les verrouiller dans la stratégie en amont. Les paramètres qui ne sont pas verrouillés pourront être modifiés dans les stratégies en aval. La hiérarchie de stratégies créée vous permettra d'administrer efficacement les appareils dans les groupes d'administration.

   Instructions pour :

   - Console d'administration : création d'une stratégie
   - Kaspersky Security Center Web Console : création d'une stratégie

2. **Création de profils de stratégie (facultatif)**

   Si vous souhaitez que les appareils au sein d'un même groupe d'administration soient exécutées sous des paramètres de stratégie divergents, créez des profils de stratégie pour ces appareils. Un profil de stratégie est un sous-ensemble nommé de paramètres de stratégie. Un profil de stratégie est un sous-ensemble nommé de paramètres de stratégie qui est diffusé sur les appareils avec la stratégie et qui vient compléter la stratégie quand une condition définie, la *condition d'activation du profil*, est remplie. Les profils contiennent uniquement les paramètres qui se distinguent de la stratégie " de base " en vigueur sur l'appareil administré (ordinateur, appareil mobile).

   Grâce aux conditions d'activation du profil, vous pouvez appliquer différents profils de stratégie, par exemple, aux appareils situés dans une unité ou un groupe de sécurité d'Active Directory défini, avec une configuration matériel particulière ou avec des tags définis. Utilisez les tags pour filtrer les appareils qui répondent aux critères définis. Par exemple, vous pouvez créer un tag *Windows*, l'attribuez à tous les appareils qui tournent sous Windows, puis désignez ce tag comme condition d'activation pour un profil de stratégie. Par conséquent, les applications de Kaspersky installées sur tous les appareils tournant sous Windows seront administrées par leur propre profil de stratégie.

Instructions pour :

- Console d'administration :
  - Création d'un profil de stratégie
  - Création d'une règle d'activation du profil de stratégie
- Kaspersky Security Center Web Console :
  - Création d'un profil de stratégie
  - Création d'une règle d'activation du profil de stratégie

3. **Propagation des stratégies et des profils de stratégie sur les appareils administrés**

   Par défaut, le Serveur d'administration se synchronise automatiquement avec les appareils administrés toutes les 15 minutes. Vous pouvez aussi contourner la synchronisation automatique et exécuter manuellement la synchronisation par la commande Forcer la synchronisation. De plus, la synchronisation est forcée après la création ou la modification d'une stratégie ou d'un profil de stratégie. Lors de la synchronisation, les stratégies et profils de stratégie neufs ou modifiés sont propagés aux appareils administrés.

   Si vous utilisez la Kaspersky Security Center Web Console, vous pouvez vérifier si les stratégies et les profils de stratégie ont été livrés à un appareil. Kaspersky Security Center indique la date et l'heure de remise dans les propriétés de l'appareil.

   Instructions pour :

   - Console d'administration : Synchronisation forcée
   - Kaspersky Security Center Web Console : synchronisation forcée

Résultats

Une fois le scénario centré sur l'appareil terminé, les applications de Kaspersky sont configurées selon les paramètres spécifiés et propagés par la hiérarchie des stratégies.

Les stratégies et les profils de stratégie de l'application configurés sont appliqués automatiquement aux nouveaux appareils ajoutés aux groupes d'administration.

Configuration et diffusion des stratégies : approche centrée sur l'utilisateur

Cette section décrit le scénario d'une approche centrée sur l'utilisateur pour la configuration centralisée des applications de Kaspersky installées sur les appareils administrés. Quand vous aurez terminé ce scénario, les applications seront configurées sur tous les appareils administrés conformément aux stratégies et aux profils de stratégie de l'application que vous avez définis.

Ce scénario peut être mis en œuvre via Kaspersky Security Center Web Console version 13 ou toute version ultérieure.

Prérequis

Avant de débuter, confirmez que vous avez bien installé le Serveur d'administration de Kaspersky Security Center et Kaspersky Security Center Web Console et que vous avez terminé le scénario d'installation principal. Vous pouvez aussi vouloir la gestion de la sécurité centrée sur l'appareil comme alternative ou option supplémentaire à l'approche centrée sur l'utilisateur. En savoir plus sur deux approches de gestion.

Processus

Le scénario de gestion des applications de Kaspersky axé sur l'utilisateur comprend les étapes suivantes :

1. **Configuration des stratégies des applications**

   Configurez les paramètres pour les applications de Kaspersky installées sur les appareils administrés par la création d'une stratégie pour chaque application. L'ensemble de ces stratégies seront propagées sur les appareils clients.

   Si vous configurez la protection de votre réseau dans l'Assistant de configuration initiale de l'application, Kaspersky Security Center crée la stratégie par défaut pour Kaspersky Endpoint Security. Si vous terminez cette procédure de configuration avec l'assistant, vous ne devez pas créer une nouvelle stratégie pour cette application. Continuez vers la configuration manuelle d'une stratégie de Kaspersky Endpoint Security.

   Si vous disposez d'une structure hiérarchique de plusieurs Serveurs d'administration et/ou groupes d'administration, les Serveurs d'administration secondaires et les groupes d'administration enfants héritent des stratégies du Serveur d'administration principal par défaut. Vous pouvez forcer l'héritage par les groupes enfants et les Serveurs d'administration secondaires pour empêcher toute modification des paramètres configurés dans la stratégie en amont. Si vous voulez imposer l'héritage d'une partie uniquement des paramètres, vous pouvez les verrouiller dans la stratégie en amont. Les paramètres qui ne sont pas verrouillés pourront être modifiés dans les stratégies en aval. La hiérarchie de stratégies créée vous permettra d'administrer efficacement les appareils dans les groupes d'administration.

   Instructions pour : Créer une stratégie

2. **Définition des propriétaires des appareils**

   Attribuez les appareils administrés aux utilisateurs correspondants.

   Instructions pour : Désigner un utilisateur comme propriétaire de l'appareil

3. **Définition des rôles d'utilisateurs typiques pour votre entreprise**

   Pensez aux différentes tâches réalisées par les employés de votre entreprise. Vous devez regrouper tous les employés en fonction de leur rôle. Par exemple, vous pouvez les organiser selon les services, les professions ou les positions. Ensuite, il faudra créer un rôle d'utilisateur pour chaque groupe. N'oubliez pas que chaque rôle d'utilisateur possédera son profil de stratégie contenant des paramètres de l'application propres à ce rôle.

4. **Création de rôles d'utilisateurs**

   Créez et configurez un rôle d'utilisateur pour chaque groupe d'employés que vous avez défini à l'étape précédente ou utilisez les rôles d'utilisateurs prédéfinis. Les rôles d'utilisateurs contiendront les ensembles de privilèges d'accès aux fonctions de l'application.

   Instructions pour : Créer un rôle utilisateur

5. **Définition de la zone d'action de chaque rôle d'utilisateur**

   Pour chaque rôle d'utilisateurs créé, définissez les utilisateurs et/ou les groupes de sécurité et les groupes d'administration. Les paramètres associés à un rôle d'utilisateur s'appliquent uniquement aux appareils qui appartiennent aux utilisateurs qui ont ce rôle et uniquement si ces appareils appartiennent aux groupes associés à ce rôle, y compris les groupes enfant.

   Instructions pour : Modification de la zone d'action d'un rôle d'utilisateur

6. **Création de profils de stratégie**

   Créez un profil de stratégie pour chaque rôles d'utilisateurs dans votre entreprise. Les profils de stratégie définissent les paramètres qui seront appliqués aux applications installées sur les appareils des utilisateurs en fonction du rôle de chaque utilisateur.

   Instructions pour : Créer un profil de stratégie

7. **Association de profils de stratégie aux rôles d'utilisateurs**

   Associez les profils de stratégie créés aux rôles d'utilisateurs. Ensuite, le profil de stratégie devient actif pour un utilisateur qui possède le rôle indiqué. Les paramètres configurés dans le profil de stratégie seront appliqués aux applications de Kaspersky installées sur les appareils des utilisateurs.

   Instructions pour : Associer des profils de stratégie aux rôles

8. **Propagation des stratégies et des profils de stratégie sur les appareils administrés**

   Par défaut, le Serveur d'administration se synchronise automatiquement avec les appareils administrés toutes les 15 minutes. Lors de la synchronisation, les stratégies et profils de stratégie neufs ou modifiés sont propagés aux appareils administrés. Vous pouvez aussi contourner la synchronisation automatique et exécuter manuellement la synchronisation par la commande Forcer la synchronisation. Une fois la synchronisation terminée, les stratégies et les profils de stratégie sont remis et appliqués aux applications Kaspersky installées.

   Vous pouvez vérifier si les stratégies et les profils de stratégie ont été livrés à un appareil. Kaspersky Security Center indique la date et l'heure de remise dans les propriétés de l'appareil.

   Instructions pour : Synchronisation forcée

Résultats

Une fois le scénario centré sur l'utilisateur terminé, les applications de Kaspersky sont configurées selon les paramètres spécifiés et propagés par la hiérarchie des stratégies et les profils de stratégie.

Pour un nouvel utilisateur, il faudra créer un compte, attribuer à l'utilisateur un des rôles d'utilisateurs définis et attribuer les appareils à l'utilisateur. Les stratégies et les profils de stratégie de l'application configurés sont appliqués automatiquement aux appareils de cet utilisateur.

Paramètres de la stratégie de l'Agent d'administration

Pour configurer les paramètres de la stratégie de l'Agent d'administration, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Stratégies et profils**.
2. Cliquez sur le nom de la stratégie de l'Agent d'administration.

   La fenêtre des propriétés de la stratégie de l'Agent d'administration s'ouvre.

Consultez le tableau comparatif détaillant comment les paramètres ci-dessous s'appliquent, en fonction du type de système d'exploitation utilisé.

Général

Sur cet onglet, vous avez la possibilité de modifier l'état de la stratégie et de configurer l'héritage des paramètres de la stratégie :

- Sous **État de la stratégie**, vous pouvez sélectionner l'une des options d'action de la stratégie :
  - Active

    Si cette option a été sélectionnée, la stratégie devient active.

    Cette option est sélectionnée par défaut.

  - Inactive

    Si cette option a été sélectionnée, la stratégie devient inactive, mais elle est conservée dans le dossier **Stratégies**. Elle pourra être activée en fonction des besoins.

- Le groupe de paramètres **Héritage des paramètres** permet de configurer l'héritage de la stratégie :
  - Hériter les paramètres de la stratégie parent

    Si cette option est activée, les valeurs des paramètres de la stratégie sont héritées depuis la stratégie du groupe de niveau supérieur et sont verrouillées.

    Cette option est activée par défaut.

  - Imposer l'héritage des paramètres aux stratégies enfants

    Une fois que les modifications dans la stratégie sont appliquées, les opérations suivantes sont exécutées :
    - Les valeurs des paramètres de la stratégie seront diffusées dans les stratégies des sous-groupes d'administration, dans les stratégies enfant.
    - Dans le bloc **Héritage des paramètres** de la section **Général** de la fenêtre des propriétés de chaque stratégie enfant, la case **Hériter des paramètres de la stratégie parent** est automatiquement cochée.

    Quand la case est cochée, les valeurs des paramètres des stratégies enfants sont verrouillées.

    Cette option est Inactif par défaut.

Configuration des événements

Cet onglet permet de configurer l'enregistrement des événements dans le journal et les notifications relatives à ces derniers. Les événements sont répartis par niveau d'importance dans les sections suivantes de l'onglet **Configuration des événements** :

- **Erreur de fonctionnement**
- **Avertissement**
- **Information**

Dans chaque section, la liste de types d'événements reprend les types d'événements et la condition de stockage par défaut sur le Serveur d'administration (en jours). Après avoir cliqué sur un type d'événement vous pouvez définir les paramètres d'enregistrement des événements dans le journal et de notification des événements sélectionnés dans la liste. Par défaut, les paramètres de notification courants spécifiés pour l'ensemble du Serveur d'administration servent pour tous les types d'événements. Cependant, vous pouvez modifier des paramètres spécifiques aux types d'événements requis.

Par exemple, dans la section **Avertissement**, vous pouvez configurer le type d'événement **Un problème de sécurité est survenu**. De tels événements peuvent se produire, par exemple, lorsque le espace disque libre d'un point de distribution est inférieure à 2 Go (au moins 4 Go sont nécessaires pour installer des applications et télécharger des mises à jour à distance). Pour configurer l'événement **Un problème de sécurité est survenu**, cliquez dessus et spécifiez où stocker les événements survenus et comment en informer.

Si l'Agent d'administration a détecté un problème de sécurité, vous pouvez gérer ce problème en utilisant les paramètres d'un appareil administré.

Paramètres de l'application

Paramètres

La section **Paramètres** vous permet de configurer les paramètres de la stratégie de l'Agent d'administration :

- **Distribuer les fichiers uniquement via les points de distribution**

  Si cette option est activée, les agents d'administration sur les Appareils administrés récupèrent les mises à jour à partir des points de distribution uniquement.

  Si cette option est désactivée, les agents d'administration sur les appareils administrés récupèrent les mises à jour des points de distribution ou du Serveur d'administration.

  Notez que les applications de sécurité sur les Appareils administrés récupèrent les mises à jour sur la source définie dans la tâche de mise à jour pour chaque application de sécurité. Si vous activez l'option **Distribuer les fichiers uniquement via les points de distribution**, assurez-vous que Kaspersky Security Center est défini comme source des mises à jour dans les tâches de mise à jour.

  Cette option est Inactif par défaut.

- **Taille maximale de la file d'attente d'événements (Mo)**

  Le champ permet d'indiquer l'espace maximal sur le disque, que la file d'attente d'événements peut occuper.

  La valeur par défaut est égale à 2 Mo.

- **L'application est autorisée à récupérer des données étendues de stratégie sur l'appareil**

  L'Agent d'administration installé sur un appareil administré transfère des informations sur la stratégie d'application de sécurité appliquée à l'application de sécurité (par exemple, Kaspersky Endpoint Security for Windows). Vous pouvez afficher les informations transférées dans l'interface de l'application de sécurité.

  L'Agent d'administration transfère les informations suivantes :

  - Heure de remise de la stratégie à l'appareil administré.
  - Nom de la stratégie active au moment de la remise de la stratégie à l'appareil administré.
  - Nom de la stratégie pour les utilisateurs autonomes au moment de la remise de la stratégie à l'appareil administré (non disponible pour l'Agent d'administration pour Linux).
  - Nom et chemin d'accès complet au groupe d'administration qui contenait l'appareil administré au moment de la remise de la stratégie à l'appareil administré.
  - Liste des profils de stratégie actifs avec leurs noms et priorités au moment de la livraison de la stratégie à l'appareil administré.

  Vous pouvez utiliser les informations pour vous assurer que la bonne stratégie est appliquée à l'appareil et à des fins d'élimination des défaillances. Cette option est Inactif par défaut.

- **Protéger le service de l'Agent d'administration contre la suppression ou l'arrêt non autorisé et empêcher la modification des paramètres**

  Lorsque cette option est activée, après l'installation de l'Agent d'administration sur un appareil administré, le module ne peut pas être supprimé ou reconfiguré sans les privilèges requis. Il est impossible d'arrêter le service de l'Agent d'administration. Cette option n'a aucun effet sur les contrôleurs de domaine.

  Activez cette option pour protéger l'Agent d'administration sur les postes de travail exploités avec des privilèges d'administrateur local.

  Cette option est Inactif par défaut.

- **Utiliser un mot de passe de désinstallation**

  Si cette option est activée, à l'aide du bouton **Modifier** vous pouvez indiquer le mot de passe pour l'utilitaire klmover et la désinstallation à distance de l'Agent d'administration.

  Cette option est Inactif par défaut.

Stockages

La section **Stockages** permet de sélectionner les types des objets dont les informations seront envoyées sur le Serveur d'administration par l'Agent d'administration. Si la stratégie de l'Agent d'administration bloque la modification ce certains paramètres de cette section, vous ne pouvez pas modifier ceux-ci.

- **Détails sur les applications installées**

  Si l'option est activée, les informations sur les applications installées sur les appareils clients sont envoyées au Serveur d'administration.

  Cette option est activée par défaut.

- **Inclut les informations sur les correctifs**

  Les informations sur les correctifs des applications installées sur les appareils clients sont envoyées au Serveur d'administration. L'activation de cette option peut augmenter la charge sur le Serveur d'administration et le SGBD, et causer une augmentation du volume de la base de données.

  Cette option est activée par défaut. Il est disponible uniquement pour Windows.

- **Détails sur les mises à jour Windows Update**

  Si cette option est activée, les informations sur les mises à jour Microsoft Windows qui doivent être installées sur les appareils clients sont envoyées au Serveur d'administration.

  Parfois, même si l'option est désactivée, les mises à jour sont affichées dans les propriétés de l'appareil dans la section **Mises à jour disponibles**. Cela peut se produire si, par exemple, les appareils de l'organisation présentent des vulnérabilités qui pourraient être corrigées par ces mises à jour.

  Cette option est activée par défaut. Il est disponible uniquement pour Windows.

  Les informations sur les mises à jour facultatives de Microsoft Windows Update ne sont pas envoyées au Serveur d'administration.

- **Détails sur les vulnérabilités dans les applications et les mises à jour correspondantes**

  Si cette option est activée, les informations sur les vulnérabilités dans les applications tierces (y compris les logiciels Microsoft), détectées sur les appareils administrés, et sur les mises à jour du logiciel destinées à corriger les vulnérabilités dans les applications tierces (à l'exception des logiciels Microsoft) sont envoyées au Serveur d'administration.

  La sélection de cette option (**Détails sur les vulnérabilités dans les applications et les mises à jour correspondantes**) augmente la charge du réseau, la charge du disque du Serveur d'administration et la consommation des ressources de l'Agent d'administration.

  Cette option est activée par défaut. Il est disponible uniquement pour Windows.

  Pour administrer les mises à jour des logiciels Microsoft, utilisez l'option **Détails sur les mises à jour Windows Update**.

- **Informations sur le registre du matériel**

  L'Agent d'administration installé sur un appareil envoie des informations sur le matériel de l'appareil au Serveur d'administration. Vous pouvez consulter les détails sur le matériel dans les propriétés de l'appareil.

  Assurez-vous que l'utilitaire lshw est installé sur les appareils Linux à partir desquels vous souhaitez récupérer les détails du matériel. Les détails du matériel récupérés depuis les machines virtuelles peuvent être incomplets en fonction de l'hyperviseur utilisé.

Mises à jour et vulnérabilités du logiciel

La section **Mises à jour et vulnérabilités du logiciel** permet de configurer la recherche et la distribution des mises à jour Windows et de rechercher les vulnérabilités parmi les fichiers exécutables :

- **Utiliser le Serveur d'administration comme serveur WSUS**

  Si l'option est activée, les mises à jour Windows sont téléchargées sur le Serveur d'administration. Le Serveur d'administration présente de manière centralisée les mises à jour téléchargées aux services Windows Update sur les appareils clients à l'aide des Agents d'administration.

  Si l'option est désactivée, le Serveur d'administration n'est pas utilisé pour télécharger les mises à jour Windows. Le cas échéant, les appareils clients reçoivent les mises à jour Windows de manière autonome.

  Cette option est Inactif par défaut.

- Vous pouvez limiter les mises à jour que les utilisateurs installer sur leurs appareils manuellement en utilisant Windows Update.

  Sur les appareils exécutés sous Windows 10, si Windows Update a déjà trouvé des mises à jour pour l'appareil, la nouvelle option que vous sélectionnez sous **Autoriser les utilisateurs à gérer l'installation des mises à jour de Windows Update** ne sera appliquée qu'une fois les mises à jour installées.

  Sélectionnez une option dans la liste déroulante :

  - **Autoriser les utilisateurs à installer toutes les mises à jour Windows Update applicables**

    Les utilisateurs peuvent installer toutes les mises à jour Microsoft Windows Update applicables à leurs appareils.

    Sélectionnez cette option si vous ne voulez pas exécuter l'installation de contrôle des mises à jour.

    Lorsque l'utilisateur installe des mises à jour Microsoft Windows Update manuellement, les mises à jour peuvent être téléchargées depuis les serveurs de Microsoft au lieu des Serveurs d'administration. Ceci est possible si le Serveur d'administration n'a pas encore téléchargé ces mises à jour. Le téléchargement des mises à jour depuis les serveurs de Microsoft génère un trafic supplémentaire.

  - **Autoriser les utilisateurs à installer uniquement les mises à jour Windows Update autorisées**

Les utilisateurs peuvent installer toutes les mises à jour Microsoft Windows Update applicables à leurs appareils et que vous avez approuvées.

Par exemple, vous souhaitez d'abord vérifier l'installation des mises à jour dans un environnement d'essai et vous assurer qu'elles ne perturbent pas le fonctionnement des appareils avant d'autoriser l'installation de ces mises à jour confirmées sur les appareils clients.

Lorsque l'utilisateur installe des mises à jour Microsoft Windows Update manuellement, les mises à jour peuvent être téléchargées depuis les serveurs de Microsoft au lieu des Serveurs d'administration. Ceci est possible si le Serveur d'administration n'a pas encore téléchargé ces mises à jour. Le téléchargement des mises à jour depuis les serveurs de Microsoft génère un trafic supplémentaire.

- **Ne pas autoriser les utilisateurs à installer les mises à jour Windows Update**

  Les utilisateurs ne peuvent pas installer manuellement les mises à jour Microsoft Windows Update sur leurs appareils. Toutes les mises à jour applicables sont installées selon votre configuration.

  Choisissez cette option, si vous voulez administrer centralement l'installation des mises à jour.

  Par exemple, il se peut que vous souhaitiez optimiser la programmation des mises à jour afin de ne pas surcharger le réseau. Vous pouvez programmer les mises à jour en dehors des heures de travail afin qu'elles n'interfèrent pas avec la productivité de l'utilisateur.

- Le groupe de paramètres **Mode de recherche des mises à jour Windows Update** permet de sélectionner le mode de recherche des mises à jour :

  - **Actif**

    Si cette option a été sélectionnée, le Serveur d'administration à l'aide de l'Agent d'administration initie la demande de l'Agent de mises à jour Windows sur l'appareil client à la source des mises à jour : Windows Update Servers or WSUS. Ensuite, l'Agent d'administration transmet sur le Serveur d'administration les informations obtenues en provenance de l'Agent de mises à jour Windows.

    L'option ne prend effet que si l'option **Se connecter au serveur de mise à jour pour mettre à jour les données** de la tâche *Recherche de vulnérabilités et de mises à jour requises* est sélectionnée.

    Cette option est sélectionnée par défaut.

  - **Passif**

    Si cette option a été sélectionnée, l'Agent d'administration transmet périodiquement sur le Serveur d'administration les informations sur les mises à jour obtenues lors de la dernières synchronisation de l'Agent de mises à jour Windows avec la source des mises à jour. Si la synchronisation de l'Agent de mises à jour Windows avec la source des mises à jour n'est pas exécutée, les données sur les mises à jour sur le Serveur d'administration vieillissent.

    Sélectionnez cette option si vous souhaitez obtenir des mises à jour à partir du cache mémoire de la source des mises à jour.

  - **Désactivé**

    Si cette option a été sélectionnée, le Serveur d'administration ne formule aucune requête d'informations sur les mises à jour.

    Sélectionnez cette option si, par exemple, vous souhaitez d'abord tester les mises à jour sur votre appareil local.

- **Analyser les fichiers exécutables à la recherche de vulnérabilités lors du lancement**

  Si cette option est activée, lors du lancement des fichiers exécutables, leur analyse sur la présence des vulnérabilités est exécutée.

  Cette option est activée par défaut.

Administration du redémarrage

Dans la section **Administration du redémarrage**, vous pouvez définir l'action à exécuter si le système d'exploitation d'un appareil administré doit être redémarré en vue d'une utilisation, d'une installation ou une désinstallation correctes d'une application :

- **Ne pas redémarrer le système d'exploitation**

  Les appareils clients ne redémarrent pas automatiquement après l'opération. Pour arrêter le fonctionnement, il faut redémarrer l'appareil (par exemple, manuellement ou à l'aide d'une tâche d'administration des appareils). Les informations sur la nécessité du redémarrage sont enregistrées dans les résultats de la tâche et dans l'état de l'appareil. Cette option convient aux tâches d' sur les serveurs et autres appareils pour lesquels la continuité des opérations est critique.

- **Redémarrer le système d'exploitation automatiquement si nécessaire**

  Dans ce cas, le redémarrage des appareils clients est toujours exécuté automatiquement, si celui-ci est requis pour terminer l'opération. Cette option convient aux tâches d' sur des appareils pour lesquels des interruptions périodiques sont admises (débranchement, redémarrage).

- **Confirmer l'action auprès de l'utilisateur**

  Le message qui signale que l'appareil client doit être redémarré manuellement s'affiche sur l'écran de l'appareil. Pour cette option, il est possible de configurer des paramètres avancés : le texte du message pour l'utilisateur, la fréquence du message, ainsi que le délai à l'issue duquel le redémarrage sera forcé (sans confirmation de l'utilisateur). Cette option convient le mieux pour les postes de travail sur lesquels les utilisateurs doivent pouvoir sélectionner l'heure de redémarrage qui leur convient le mieux.

  Cette option est sélectionnée par défaut.

  - **Fréquence de rappel de la nécessité de réaliser l'installation (min.)**

    Quand cette option est activée, l'application invite l'utilisateur à redémarrer le système d'exploitation selon la fréquence indiquée.

    Cette option est activée par défaut. L'intervalle par défaut est de 5 minutes. La valeur peut être comprise entre 1 et 1 440 minutes.

    Si cette option est désactivée, l'invite est affichée une seule fois.

  - **Forcer le redémarrage au bout de (min.)**

    Après avoir averti l'utilisateur, l'application force le redémarrage du système d'exploitation à l'issue de l'intervalle défini.

    Cette option est activée par défaut. Le délai par défaut est de 30 minutes. La valeur peut être comprise entre 1 et 1 440 minutes.

  - **Forcer la fermeture des applications dans les sessions bloquées**

Les applications en cours d'exécution peuvent empêcher le redémarrage de l'appareil client. Par exemple, si un document est en train d'être modifié dans un logiciel de traitement de texte et qu'il n'est pas enregistré, l'application n'autorise pas le redémarrage de l'appareil.

Quand cette option est activée, l'arrêt forcé de ces applications sur un appareil verrouillé doit avoir lieu avant de pouvoir redémarrer l'appareil. Les utilisateurs pourraient perdre toute modification qui n'a pas été enregistrée à ce moment.

Si cette option est désactivée, un appareil verrouillé n'est pas redémarré. L'état de la tâche sur cet appareil indique qu'il faut redémarrer l'appareil. Les utilisateurs doivent quitter manuellement toutes les applications en cours d'exécution sur les appareils verrouillés, puis redémarrer ces appareils.

Cette option est Inactif par défaut.

Partage du bureau Windows

La section **Partage du bureau Windows** permet d'activer et de configurer l'audit des actions de l'administrateur sur un appareil distant quand l'accès au bureau est partagé :

- **Activer l'audit**

  Si cette option est activée, l'audit des actions de l'administrateur sur l'appareil distant est activé. Les enregistrements des actions de l'administrateur sur l'appareil distant sont conservés :

  - Dans le journal des événements de l'appareil distant
  - Dans un fichier .syslog, situé dans le dossier d'installation de l'Agent d'administration sur l'appareil distant
  - Dans la base des événements du Kaspersky Security Center

  L'audit des actions de l'administrateur est accessible lorsque les conditions suivantes sont réunies :

  - La licence pour le fonctionnement de Gestion des vulnérabilités et des correctifs est en cours d'utilisation
  - L'administrateur est autorisé à lancer l'accès partagé au bureau de l'appareil distant

  Si cette option est désactivée, l'audit des actions de l'administrateur sur l'appareil distant est désactivé.

  Cette option est Inactif par défaut.

- **Masques de fichiers à suivre en cas de lecture**

  La liste contient des masques de fichiers. Lorsque l'audit est activé, l'application suit les fichiers lus par l'administrateur qui correspondent à ces masques et elle enregistre les informations relatives aux fichiers lus. La liste n'est accessible que si la case **Activer l'audit** est cochée. Il est possible de modifier les masques de fichiers et d'en ajouter à la liste. Les nouveaux masques de fichiers doivent être ajoutés sur une nouvelle ligne.

  Par défaut, les masques de fichiers indiqués sont : *.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt et *.pdf.

- **Masques de fichiers à suivre en cas de modification**

  La liste contient les masques des fichiers de l'appareil distant. Lorsque l'audit est activé, l'application suit les fichiers modifiés par l'administrateur qui correspondent à ces masques et elle enregistre les informations relatives aux fichiers modifiés. La liste n'est accessible que si la case **Activer l'audit** est cochée. Il est possible de modifier les masques de fichiers et d'en ajouter à la liste. Les nouveaux masques de fichiers doivent être ajoutés sur une nouvelle ligne.

  Par défaut, les masques de fichiers indiqués sont : *.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt et *.pdf.

Administration des correctifs et des mises à jour

Dans la section **Administration des correctifs et des mises à jour**, vous pouvez configurer la réception et la diffusion des mises à jour et l'installation des correctifs vers les appareils administrés :

- **Installer automatiquement les mises à jour et les correctifs nécessaires pour les modules dont l'état est Non défini**

  Si la case est Activé, les correctifs de Kaspersky avec l'état d'approbation *Non défini* s'installent automatiquement sur les appareils administrés juste après avoir été téléchargés depuis les serveurs de mises à jour.

  Si l'option est désactivée, les correctifs de Kaspersky chargés avec l'état *Non défini* sont installés après que l'administrateur a modifié leur état pour qu'il soit *Approuvé*.

  Cette option est activée par défaut.

- **Télécharger au préalable les mises à jour et les bases antivirus depuis le Serveur d'administration (recommandé)**

  Si la case est Activé, le modèle hors ligne de téléchargement des mises à jour est désactivé. Quand le serveur d'administration reçoit des mises à jour, il signale à l'Agent d'administration (sur les appareils où il est installé) les mises à jour qui seront requises pour les applications administrées. Quand l'Agent d'administration reçoit des informations sur les mises à jour, il télécharge les fichiers nécessaires au préalable sur le Serveur d'administration. Lors de la première connexion à Agent d'administration, le Serveur d'administration initialise le téléchargement des mises à jour. Une fois que l'Agent d'administration sur l'appareil client a téléchargé toutes les mises à jour, celles-ci deviennent accessibles aux applications situées sur ce même appareil.

  Lorsque l'application administrée sur l'appareil client s'adresse à l'Agent d'administration pour obtenir des mises à jour, l'Agent vérifie s'il a les mises à jour nécessaires. Si des mises à jour ont été reçues du Serveur d'administration au plus tôt 25 heures après la requête de l'application administrée, l'Agent d'administration ne se connecte pas au Serveur d'administration et fournit à l'application administrée des mises à jour du cache local. Il se peut que la connexion au Serveur d'administration ne soit pas établie lorsque l'Agent d'administration fournit les mises à jour aux applications sur les appareils client, mais la connexion n'est pas requise pour la mise à jour.

  Si l'option est désactivée, le modèle hors ligne de téléchargement des mises à jour n'est pas utilisé. Les mises à jour sont distribuées conformément à la programmation de la tâches de téléchargement des mises à jour.

  Cette option est activée par défaut.

Connectivité

La section **Connectivité** inclut trois sous-sections :

- **Réseau**
- **Profils de connexion**
- **Calendrier de connexion**

Dans la sous-section **Réseau**, vous pouvez configurer la connexion au Serveur d'administration, activer l'utilisation d'un port UDP et spécifier le numéro de port UDP.

- Dans le groupe de paramètres **Se connecter au Serveur d'administration**, vous pouvez configurer les paramètres de connexion au Serveur d'administration et indiquer l'intervalle de synchronisation des appareils clients avec le Serveur d'administration :

  - **Période de synchronisation (min.)**

    L'Agent d'administration synchronise l'appareil administré avec le serveur d'administration. Nous recommandons d'adopter un intervalle de synchronisation (désigné également par le terme battement de cœur) de 15 minutes pour 10 000 appareils administrés.

    Si l'intervalle de synchronisation est défini sur moins de 15 minutes, la synchronisation est effectuée toutes les 15 minutes. Si l'intervalle de synchronisation est défini sur 15 minutes ou plus, la synchronisation est effectuée à l'intervalle de synchronisation spécifié.

  - **Compresser le trafic réseau**

    Si cette option est activée, la vitesse de transfert des données de l'Agent d'administration sera augmentée, le volume des informations transmises sera réduit et la charge sur le Serveur d'administration sera diminuée.

    La charge sur le processeur central de l'ordinateur client peut augmenter.

    Cette case est cochée par défaut.

  - **Ouvrir les ports de l'Agent d'administration dans le pare-feu Microsoft Windows**

    Si l'option est activée, les ports, indispensables au bon fonctionnement de l'Agent d'administration et du Serveur d'administration, sont ajoutés à la liste des exclusions du pare-feu Microsoft Windows.

    Cette option est activée par défaut.

  - **Utiliser une connexion SSL**

    Si l'option est activée, la connexion au Serveur d'administration est établie via le port sécurisé à l'aide du protocole SSL.

    Cette option est activée par défaut.

  - **Utiliser la passerelle de connexion sur le point de distribution (le cas échéant) dans les paramètres de connexion par défaut**

    Si l'option est activée, la passerelle de connexion du point de distribution est utilisée avec les paramètres spécifiés par les propriétés du groupe d'administration.

    Cette option est activée par défaut.

- **Utiliser un port UDP**

Si vous avez besoin que l'Agent d'administration se connecte au Serveur d'administration via un port UDP, activez l'option **Utiliser le port UDP** et indiquez le **Numéro de port UDP**. Cette option est activée par défaut. Par défaut, la connexion au Serveur d'administration est exécutée via le port UDP 15000.

- **Numéro de port UDP**

  Champ à saisir le numéro du port UDP. Le numéro de port par défaut est 15000.

  La forme d'écriture décimale est utilisée.

  Si un appareil client fonctionne sous le système d'exploitation Windows XP Service Pack 2, le pare-feu incorporé verrouillera le port UDP 15000. Ce port doit être ouvert à la main.

- **Utiliser un point de distribution pour forcer la connexion au Serveur d'administration**

  Sélectionnez cette option si vous avez sélectionné l'option **Utiliser ce point de distribution comme serveur push** dans la fenêtre des paramètres du point de distribution. Sinon, le point de distribution n'agira pas comme un serveur push.

La sous-section **Profils de connexion** permet d'indiquer les paramètres d'emplacement réseau et d'activer le mode de l'utilisateur autonome quand le Serveur d'administration n'est pas disponible :

- **Paramètres d'emplacement réseau**

  Les paramètres d'emplacement réseau définissent les caractéristiques du réseau auquel l'appareil client est connecté et spécifient les règles de commutation de l'Agent d'administration d'un profil de connexion du Serveur d'administration sur l'autre en cas de modification des caractéristiques du réseau.

- **Profils de connexion au Serveur d'administration**

  Cette section permet de consulter et d'ajouter des profils de connexion de l'Agent d'administration au Serveur d'administration. Cette section permet également de rédiger des règles de déplacement de l'Agent d'administration vers un autre Serveur d'administration si les événements suivants se produisent :

  - Connexion de l'appareil client à un autre réseau local
  - Déconnexion de l'appareil du réseau local de l'organisation
  - Modification de l'adresse de la passerelle de connexion ou modification de l'adresse du serveur DNS

  Les profils des connexions ne sont pris en charge que pour les appareils fonctionnant sous Windows et macOS.

- **Activer le mode de l'utilisateur autonome quand le Serveur d'administration n'est pas disponible**

  Si l'option est activée, en cas de connexion via ce profil, les applications installées sur l'appareil client vont utiliser les profils de stratégie pour les appareils qui se trouvent en mode de l'utilisateur autonome et les stratégies pour utilisateurs autonomes. Si aucune stratégie pour les utilisateurs autonomes n'est définie pour l'application, c'est la stratégie active qui sera utilisée.

  Si l'option est activée, les applications utiliseront les stratégies actives.

  Cette option est Inactif par défaut.

La sous-section **Calendrier de connexion** vous permet d'indiquer les intervalles de temps pendant lesquels l'Agent d'administration va transférer les données sur le Serveur d'administration :

- **Se connecter en cas de nécessité**

  Si cette option a été sélectionnée, la connexion s'établira quand l'Agent d'administration devra transférer les données sur le Serveur d'administration.

  Cette option est sélectionnée par défaut.

- **Se connecter aux intervalles indiqués**

  Si cette option a été sélectionnée, la connexion de l'Agent d'administration au Serveur d'administration est effectuée dans les intervalles indiqués. Plusieurs périodes de connexions peuvent être ajoutées.

Sondage du réseau par points de distribution

La section **Sondage du réseau par points de distribution** permet de configurer le sondage automatique du réseau. Vous pouvez utiliser les options suivantes pour activer le sondage et définir sa fréquence :

- **Réseau Windows**

  Si l'option est activée, le Serveur d'administration sonde automatiquement le réseau en respectant la planification défini en cliquant sur les liens **Planifier le sondage rapide** et **Planifier le sondage complet**.

  Si cette option est désactivée, le Serveur d'administration sonde le réseau à l'intervalle indiqué dans le champ **Fréquence des sondages du réseau (min.)**.

  L'intervalle de recherche d'appareils pour les versions de l'Agent d'administration antérieures à 10.2 peut être configuré dans les champs **Fréquence des sondages des domaines Windows (min.)** (pour un sondage rapide du réseau Windows) et **Fréquence des sondages du réseau (min.)** (pour un sondage complet du réseau Windows).

  Cette option est Inactif par défaut.

- **Zeroconf**

  Si cette option est activée, le point de distribution sonde automatiquement le réseau avec les appareils IPv6 en utilisant la mise en réseau sans configuration (également appelé *Zeroconf*). Dans ce cas, le sondage de plage IP activé est ignoré, car le point de distribution sonde l'ensemble du réseau.

  Pour commencer à utiliser Zeroconf, les conditions suivantes doivent être remplies :

  - Le point de distribution doit exécuter Linux.
  - Vous devez installer l'utilitaire avahi-browse sur le point de distribution.

  Si cette option est désactivée, le point de distribution ne sonde pas les réseaux avec des appareils IPv6.

  Cette option est Inactif par défaut.

- Plages IP

  Si l'option est activée, le point de distribution sonde automatiquement les plages IP en fonction de planification que vous avez configurée en cliquant sur le bouton **Planifier le sondage**.

  Si cette option est désactivée, le point de distribution ne sonde pas les plages IP.

  La fréquence de sondage des plages IP pour les versions de l'Agent d'administration antérieures à la version 10.2 peut être configurée dans le champ **Période de sondage (min.)**. Le champ est disponible si l'option est activée.

  Cette option est Inactif par défaut.

- Contrôleurs de domaine

  Si l'option est activée, le point de distribution sonde automatiquement Active Directory en fonction de la configuration définie en cliquant sur le lien **Planifier le sondage**.

  Si cette option est désactivée, le Serveur d'administration ne sonde pas Active Directory.

  La fréquence de sondage d'Active Directory pour les versions de l'Agent d'administration antérieures à la version 10.2 est définie dans le champ **Période de sondage (min.)**. Le champ est disponible si l'option est activée.

  Cette option est Inactif par défaut.

  Si l'option est activée, le point de distribution sonde automatiquement les contrôleurs de domaine selon la planification que vous avez configurée en cliquant sur le bouton **Planifier le sondage**.

  Si cette option est désactivée, le point de distribution n'interroge pas les contrôleurs de domaine.

  La fréquence de sondage du contrôleur de domaine pour les versions de l'Agent d'administration antérieures à 10.2 peut être configurée dans le champ **Période de sondage (min.)**. Le champ est disponible si l'option est activée.

  Cette option est Inactif par défaut.

Paramètres du réseau pour les points de distribution

Si vos points de distribution utilisent un serveur proxy pour se connecter à Internet, vous pouvez renseigner les paramètres suivants dans le groupe **Paramètres du réseau pour les points de distribution** :

- **Utiliser un serveur proxy**
- **Adresse**
- **Numéro de port**
- Ne pas utiliser le serveur proxy pour les adresses locales

  Si cette option est activée, le serveur proxy ne sera pas utilisé lors de la connexion aux appareils sur le réseau local.

  Cette option est Inactif par défaut.

- Authentification du serveur proxy

  Si la case est cochée, les champs de saisie permettent d'indiquer les identifiants pour l'authentification sur le serveur proxy.

  Celle-ci est décochée par défaut.

- **Nom d'utilisateur**
- **Mot de passe**

Proxy KSN (Points de distribution)

Dans la section **Proxy KSN (Points de distribution)**, vous pouvez configurer l'application afin qu'elle utilise le point de distribution pour transmettre les requêtes de Kaspersky Security Network depuis les appareils administrés :

- Activer le proxy KSN du côté du point de distribution

  Le service KSN proxy est exécuté sur l'appareil qui est utilisé en tant que points de distribution. Utilisez cette fonction pour rediffuser et optimiser le trafic sur le réseau.

  Le point de distribution envoie les statistiques KSN, lesquelles sont répertoriées dans la Déclaration de Kaspersky Security Network, à Kaspersky. Par défaut, la Déclaration KSN se trouve dans %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\ksneula.

  Cette option est Inactif par défaut. L'activation de cette option prend effet uniquement si les options **Utiliser le Serveur d'administration comme serveur proxy** et **J'accepte les termes du Kaspersky Security Network** sont activées dans la fenêtre Propriétés du Serveur d'administration.

  Vous pouvez affecter un nœud d'un cluster actif-passif à un point de distribution et activer le serveur proxy KSN sur ce nœud.

- Transférer les requêtes KSN au Serveur d'administration

  Le point de distribution transfère les requêtes KSN depuis les appareils administrés vers le Serveur d'administration.

  Cette option est activée par défaut.

- Accéder à KSN Cloud/KPSN directement via Internet

  Le point de distribution transfère les requêtes KSN depuis les appareils administrés vers le Cloud KSN ou KPSN. Les requêtes KSN générées sur le point de distribution lui-même sont également envoyées directement à KSN Cloud ou à KPSN.

  Les points de distribution sur lesquels l'Agent d'administration version 11 (ou antérieure) est installé ne peuvent pas accéder directement à KPSN. Si vous souhaitez reconfigurer les points de distribution pour envoyer des demandes KSN à KPSN, activez l'option **&Transférer les demandes KSN au Serveur d'administration** pour chaque point de distribution.

  Les points de distribution sur lesquels l'Agent d'administration version 12 (ou version ultérieure) est installé peuvent accéder directement à KPSN.

- **Port**

  Le numéro du port TCP que les appareils administrés utilisent pour se connecter au serveur proxy KSN. Le numéro de port par défaut est 13111.

- **Port UDP**

  Si vous avez besoin que l'Agent d'administration se connecte au Serveur d'administration via un port UDP, activez l'option **Utiliser le port UDP** et indiquez le **Numéro de port UDP**. Cette option est activée par défaut. Par défaut, la connexion au Serveur d'administration est exécutée via le port UDP 15000.

Mises à jour (Points de distribution)

Dans la section **Mises à jour (Points de distribution)**, vous pouvez activer la fonctionnalité de téléchargement de fichiers diff, pour que les points de distribution prennent donc les mises à jour sous la forme de fichiers diff à partir des serveurs de mise à jour de Kaspersky.

Gestion des comptes locaux (Linux uniquement)

La section **Gestion des comptes locaux (Linux uniquement)** comprend trois sous-sections :

- **Gestion des certificats utilisateurs**
- **Ajouter ou modifier les groupes d'administration locale applicables**
- **Charger un fichier de référence pour protéger le fichier sudoers sur l'appareil de l'utilisateur contre toute modification**

La sous-section **Gestion des certificats utilisateurs** permet d'indiquer les certificats racines à installer. Ces certificats peuvent servir, par exemple, à vérifier l'authenticité de sites Internet ou de serveurs Internet.

- **Installer les certificats racine**

  Si l'option est activée, les certificats ajoutés au tableau seront installés sur les appareils spécifiés.

  Si cette option est désactivée, aucun certificat ne sera installé sur les appareils spécifiés.

  Cette option est Inactif par défaut.

- **Ajouter**

  Cliquez sur ce bouton pour ouvrir la fenêtre dans laquelle vous pouvez ajouter un certificat.

  La taille du certificat doit être inférieure à 10 Mo.

  Kaspersky Security Center prend en charge les certificats avec les extensions CER, CRT, CERT, PEM et KEY.

Dans la sous-section **Ajouter ou modifier les groupes d'administration locale applicables**, vous pouvez gérer les groupes d'administrateurs locaux. Ces groupes sont utilisés, par exemple, lors de la révocation des droits d'administrateur local. Vous pouvez également consulter la liste des comptes utilisateurs à privilèges à l'aide du **Rapport sur les utilisateurs d'appareils à privilèges (Linux uniquement)**.

- **Ajouter**

  Cliquez sur ce bouton pour ouvrir la fenêtre dans laquelle vous pouvez ajouter un groupe d'administrateurs locaux.

- **Modifier**

  Cliquez sur ce bouton pour ouvrir la fenêtre dans laquelle vous pouvez modifier le groupe des administrateurs locaux.

  Ce bouton est accessible si la case en regard du groupe d'administrateurs local est cochée.

- **Supprimer ;**

  Cliquez sur ce bouton pour supprimer du tableau le groupe d'administrateurs locaux sélectionné.

  Ce bouton est accessible si la case en regard du groupe d'administrateurs local est cochée.

Dans la sous-section **Charger un fichier de référence pour protéger le fichier sudoers sur l'appareil de l'utilisateur contre toute modification**, vous pouvez configurer la gestion du fichier sudoers. Les groupes privilégiés et les utilisateurs d'appareils sont définis dans le fichier sudoers sur l'appareil. Le fichier sudoers se trouve dans `/etc/sudoers`. Vous pouvez charger un fichier sudoers de référence pour protéger le fichier sudoers contre toute modification. Cette mesure empêchera toute modification indésirable du fichier sudoers.

Un fichier de référence sudoers non valide peut entraîner un dysfonctionnement de l'appareil de l'utilisateur.

- **Contrôler le fichier sudoers**

  Si l'option est activée, le fichier sudoers sera remplacé par le fichier sudoers de référence actuel.

  Si l'option est désactivée, le fichier sudoers reste inchangé.

  Cette option est Inactif par défaut.

- **Fichier de référence sudoers**

  Ce champ affiche le nom du fichier sudoers de référence chargé.

- **Charger**

  Cliquez sur ce bouton pour ouvrir la fenêtre dans laquelle vous pouvez charger le fichier de référence sudoers.

- **Fichier sudoers de référence actuel**

  Cliquez sur ce bouton pour afficher le contenu du fichier sudoers actuel.

Historique des révisions

L'onglet vous permet de consulter la liste des révisions de la stratégie et de restaurer les modifications apportées à la stratégie, si nécessaire.

Comparaison des paramètres de stratégie de l'Agent d'administration par système d'exploitation

Le tableau ci-dessous indique les paramètres de stratégie de l'Agent d'administration que vous pouvez utiliser dans la Console d'administration et Kaspersky Security Center Web Console pour configurer l'Agent d'administration avec un système d'exploitation particulier.

Paramètres de stratégie de l'Agent d'administration : comparaison par système d'exploitation

Section Stratégie	Windows	macOS	Linux
Général	✓	✓	✓
Configuration des événements	✓	✓	✓
Paramètres	✓	✓	✓ Les options suivantes sont proposées : • **Distribuer les fichiers uniquement via les points de distribution** • **Taille maximale de la file d'attente d'événements (Mo)** • **&L'application est autorisée à récupérer des données étendues de stratégie sur l'appareil**
Stockages	✓	✓ L'option **Informations sur le registre du matériel** est disponible.	✓ Les options suivantes sont proposées : • **Détails sur les applications installées** • **Informations sur le registre du matériel**
Mises à jour et vulnérabilités du logiciel	✓	—	—
Administration du redémarrage	✓	—	—
Partage du bureau Windows	✓	—	—
Administration des correctifs et des mises à jour	✓	—	—

Section Stratégie	Windows	macOS	Linux
Connectivité → Réseau	✓	✓	✓ Sauf l'option **Ouvrir les ports de l'Agent d'administration dans le pare-feu Microsoft Windows**.
Connectivité → Profils de connexion	✓	✓	—
Connectivité → Calendrier de connexion	✓	✓	✓
Sondage du réseau par points de distribution	✓ Seulement les options **Réseau Windows**, **Plages IP** et **Contrôleurs de domaine** sont disponibles.	—	✓ Les options suivantes sont proposées : • **Zeroconf** • **Plages IP** • **Contrôleurs de domaine**
Paramètres du réseau pour les points de distribution	✓	✓	✓
Proxy KSN (Points de distribution)	✓	—	✓
Mises à jour (Points de distribution)	✓	—	✓
Historique des révisions	✓	✓	✓

Activation et désactivation du mode de faible consommation de ressources pour l'Agent d'administration

Le mode de faible consommation de ressources permet de limiter l'utilisation de la mémoire vive de l'Agent d'administration installé sur l'appareil client. Par défaut, le mode de faible consommation de ressources est désactivé.

En mode de faible consommation de ressources, les fonctionnalités suivantes ne sont pas exécutées :

- L'Agent d'administration ne peut pas être affecté à la fonction de point de distribution (que ce soit manuellement ou automatiquement).
- L'Agent d'administration n'enregistre pas les informations relatives à l'état de l'Agent d'administration dans un fichier texte distinct.
- L'Agent d'administration ne prend pas en charge le modèle hors ligne de téléchargement des mises à jour.
- Les modules et processus suivants sont désactivés :
  - Obtention d'informations sur les mises à jour tierces et les vulnérabilités.
  - Exécution du proxy KSN du côté du point de distribution.
  - Chargement des mises à jour dans le stockage des points de distribution.
  - Contournement du blocage du serveur DNS.
  - Obtention d'informations concernant l'espace libre du disque.

Les modules et les processus reprennent leur fonctionnement après la désactivation du mode de faible consommation de ressources.

Pour activer le mode de faible consommation de ressources, procédez comme suit :

1. Exécutez la commande suivante dans la ligne de commande de l'appareil client :

   ```
   C:\Program files (x86)\Kaspersky Lab\NetworkAgent>klscflag -fset -pv klnagent -n KLNAG_FLAG_TEST_VM_PERF -t d -v 1
   ```

2. Relancez l'Agent d'administration.

3. Pour vérifier que le mode de consommation réduite de ressources est activé, ouvrez l'**Observateur des événements** sous Windows, puis sélectionnez **Journaux des applications et des services → Journal des événements Kaspersky**.

   Assurez-vous que le journal contient des événements tels que **L'Agent d'administration de Kaspersky Security Center fonctionne en mode de consommation réduite de ressources**.

Le mode de faible consommation de ressources est activé.

Pour désactiver le mode de faible consommation de ressources, procédez comme suit :

1. Exécutez la commande suivante dans la ligne de commande de l'appareil client :

   ```
   C:\Program files (x86)\Kaspersky Lab\NetworkAgent>klscflag -fset -pv klnagent -n KLNAG_FLAG_TEST_VM_PERF -t d -v 0
   ```

2. Relancez l'Agent d'administration.

3. Pour vérifier que le mode de consommation réduite de ressources est désactivé, ouvrez l'**Observateur des événements** sous Windows, puis sélectionnez **Journaux des applications et des services → Journal des événements Kaspersky**.

   Assurez-vous que le dernier événement klnagent ne contient pas le message **L'Agent d'administration de Kaspersky Security Center fonctionne en mode de consommation réduite de ressources**.

Le mode de faible consommation de ressources est désactivé.

Vous pouvez aussi activer à distance le mode de faible consommation de ressources à l'aide de la tâche *Exécuter des scripts à distance*.

Configuration manuelle d'une stratégie de Kaspersky Endpoint Security

Cette section fournit des recommandations sur la configuration de la stratégie de Kaspersky Endpoint Security. Vous pouvez effectuer la configuration dans la fenêtre des propriétés de la stratégie. Lorsque vous modifiez un paramètre, cliquez sur l'icône en forme de cadenas à droite du groupe de paramètres concerné pour appliquer les valeurs spécifiées à un poste de travail.

Configuration de Kaspersky Security Network

Kaspersky Security Network (KSN) est l'infrastructure des services cloud qui contient des informations sur la réputation des fichiers, des ressources Internet et des logiciels. Kaspersky Security Network permet à Kaspersky Endpoint Security for Windows de réagir plus rapidement aux différents types de menaces, améliore les performances des modules de protection et réduit le risque de faux positifs. Pour en savoir plus sur Kaspersky Security Network, consultez l'aide de Kaspersky Endpoint Security for Windows.

Pour spécifier les paramètres KSN recommandés :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Stratégies et profils**.
2. Cliquez sur la stratégie de Kaspersky Endpoint Security for Windows.

   La fenêtre des propriétés de la stratégie sélectionnée s'ouvre.
3. Dans les propriétés de la stratégie, accédez à **Paramètres de l'application** → **Protection avancée** → **Kaspersky Security Network**.
4. Assurez-vous que l'option **Kaspersky Security Network** est activée. L'utilisation de cette option aide à rediffuser et optimiser le trafic sur le réseau.

   Si vous utilisez Managed Detection and Response, vous devez activer l'option **Kaspersky Security Network** pour le point de distribution et activer le mode KSN étendu.
5. Activez l'utilisation des serveurs KSN si le service KSN proxy n'est pas disponible. Les serveurs de KSN peuvent se trouver aussi bien du côté de Kaspersky (utilisation du KSN) ou du côté d'un tiers (utilisation du KPSN).
6. Cliquez sur le bouton **OK**.

Les paramètres KSN recommandés sont spécifiés.

Consultation de la liste des réseaux protégés par le Pare-feu

Assurez-vous que le Pare-feu de Kaspersky Endpoint Security for Windows protège tous vos réseaux. Par défaut, le Pare-feu protège les réseaux avec les types de connexion suivants :

- **Réseau public**. Les applications de sécurité, les pare-feu ou les filtres ne protègent pas les appareils dans un tel réseau.
- **Réseau local**. L'accès aux fichiers et aux imprimantes est limité pour les appareils de ce réseau.
- **Réseau de confiance**. Les appareils d'un tel réseau sont protégés contre les attaques et l'accès non autorisé aux fichiers et aux données.

Si vous avez configuré un réseau personnalisé, assurez-vous que le Pare-feu le protège. Pour ce faire, consultez la liste des réseaux dans les propriétés de la stratégie de Kaspersky Endpoint Security for Windows. Il se peut que certains réseaux ne figurent pas dans la liste.

Pour en savoir plus sur le Pare-feu, consultez l'aide de Kaspersky Endpoint Security for Windows.

Pour vérifier la liste des réseaux, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Stratégies et profils**.
2. Cliquez sur la stratégie de Kaspersky Endpoint Security for Windows.

   La fenêtre des propriétés de la stratégie sélectionnée s'ouvre.
3. Dans les propriétés de la stratégie, accédez à **Paramètres de l'application** → **Protection principale** → **Pare-feu**.
4. Sous **Réseaux disponibles**, cliquez sur le lien **Paramètres du réseau**.

   La fenêtre **Connexions réseau** s'ouvre. Cette fenêtre affiche la liste des réseaux.
5. Si la liste contient un réseau manquant, ajoutez-le.

Désactivation de l'analyse des disques réseau

Lorsque Kaspersky Endpoint Security for Windows analyse les disques réseau, ceux-ci peuvent être soumis à une charge importante. Il est préférable de réaliser l'analyse directement sur les serveurs de fichiers.

Vous pouvez désactiver l'analyse des disques réseau dans les propriétés de la stratégie de Kaspersky Endpoint Security for Windows. Pour obtenir une description de ces propriétés de stratégie, consultez l'aide de Kaspersky Endpoint Security for Windows.

Pour désactiver l'analyse des disques réseau, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Stratégies et profils**.
2. Cliquez sur la stratégie de Kaspersky Endpoint Security for Windows.

   La fenêtre des propriétés de la stratégie sélectionnée s'ouvre.
3. Dans les propriétés de la stratégie, accédez à **Paramètres de l'application** → **Protection principale** → **Protection contre les fichiers malicieux**.
4. Sous **Zone de protection**, désactivez l'option **Tous les disques réseau**.
5. Cliquez sur le bouton **OK**.

L'analyse des disques réseau est désactivée.

Exclusion des détails du logiciel de la mémoire du Serveur d'administration

Il est recommandé que le Serveur d'administration n'enregistre pas les informations relatives aux modules logiciels lancés sur les appareils du réseau. Par conséquent, la mémoire du Serveur d'administration n'est pas saturée.

Vous pouvez désactiver l'enregistrement de ces informations dans les propriétés de la stratégie de Kaspersky Endpoint Security for Windows.

Pour désactiver l'enregistrement d'informations sur les modules logiciels installés :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Stratégies et profils**.
2. Cliquez sur la stratégie de Kaspersky Endpoint Security for Windows.

   La fenêtre des propriétés de la stratégie sélectionnée s'ouvre.
3. Dans les propriétés de la stratégie, accédez à **Paramètres de l'application** → **Paramètres généraux** → **Rapports et stockage**.
4. Sous **Transfert des données au Serveur d'administration**, décochez la case **À propos des applications exécutables** si elle est toujours cochée dans la stratégie de niveau supérieur.

   Quand cette case est cochée, la base de données du Serveur d'administration enregistre les informations relatives à toutes les versions de tous les modules logiciels sur les appareils dans le réseau. Les informations indiquées peuvent prendre un espace considérable dans la base de données de Kaspersky Security Center (des dizaines de gigaoctets).

Les informations sur les modules logiciels installés ne sont plus enregistrées dans la base de données du Serveur d'administration.

Configuration de l'accès à l'interface de Kaspersky Endpoint Security for Windows sur les postes de travail

Si la protection contre les menaces sur le réseau de l'organisation doit être administrée en mode centralisé via Kaspersky Security Center, spécifiez les paramètres de l'interface dans les propriétés de la stratégie Kaspersky Endpoint Security for Windows, comme décrit ci-dessous. Par conséquent, vous empêcherez l'accès non autorisé à Kaspersky Endpoint Security for Windows sur les postes de travail et la modification des paramètres de Kaspersky Endpoint Security for Windows.

Pour obtenir une description de ces propriétés de stratégie, consultez l'aide de Kaspersky Endpoint Security for Windows.

Pour spécifier les paramètres d'interface recommandés :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Stratégies et profils**.
2. Cliquez sur la stratégie de Kaspersky Endpoint Security for Windows.

   La fenêtre des propriétés de la stratégie sélectionnée s'ouvre.
3. Dans les propriétés de la stratégie, accédez à **Paramètres de l'application** → **Paramètres généraux** → **Interface**.
4. Sous **Interaction avec l'utilisateur**, sélectionnez l'option **Ne pas afficher**. Cela désactive l'affichage de l'interface utilisateur de Kaspersky Endpoint Security for Windows sur les postes de travail, de sorte que leurs utilisateurs ne peuvent pas modifier les paramètres de Kaspersky Endpoint Security for Windows.
5. Sous **Protection par mot de passe**, activez le commutateur. Cela réduit le risque de modifications non autorisées ou involontaires des paramètres de Kaspersky Endpoint Security for Windows sur les postes de travail.

Les paramètres recommandés pour l'interface de Kaspersky Endpoint Security for Windows sont spécifiées.

Enregistrement des événements de stratégie importants dans la base de données du Serveur d'administration

Pour éviter le débordement de la base de données du Serveur d'administration, nous vous recommandons d'enregistrer uniquement des événements importants dans la base de données.

Pour configurer l'enregistrement d'événements importants dans la base de données du Serveur d'administration :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Stratégies et profils**.
2. Cliquez sur la stratégie de Kaspersky Endpoint Security for Windows.

   La fenêtre des propriétés de la stratégie sélectionnée s'ouvre.
3. Dans les propriétés de la stratégie, ouvrez l'onglet **Configuration des événements**.

4. Dans la section **Critique**, cliquez sur **Ajouter un événement** et cochez les cases en regard des événements suivants uniquement :

   - *Contrat de licence utilisateur final violé*
   - *Le lancement automatique de l'application est désactivé*
   - *Erreur d'activation*
   - *Une menace active a été détectée. Il faut lancer la procédure de désinfection avancée*
   - *Désinfection impossible*
   - *Un lien dangereux ouvert précédemment a été détecté*
   - *Le processus est terminé*
   - *L'activité réseau est interdite*
   - *Une attaque réseau a été détectée*
   - *Le lancement de l'application est interdit*
   - *Accès interdit (bases locales)*
   - *Accès interdit (KSN)*
   - *Erreur locale de mise à jour*
   - *Impossible de lancer deux tâches simultanément*
   - *Erreur d'interaction avec Kaspersky Security Center*
   - *Certains modules n'ont pas été mis à jour*
   - *Erreur d'application des règles de chiffrement/déchiffrement des fichiers*
   - *Erreur d'activation du mode portable*
   - *Erreur de désactivation du mode portable*
   - *Impossible de charger le module de chiffrement*
   - *La stratégie ne peut pas être appliquée*
   - *Erreur de modification de la sélection de modules de l'application*

5. Cliquez sur le bouton **OK**.

6. **Erreur de fonctionnementAjouter un événement***Dans la section Erreur de fonctionnement, cliquez sur Ajouter des événements et cochez la case uniquement à côté de l'événement Paramètres de tâche non valides.*
   Les paramètres de la tâche n'ont pas été appliqués.

7. Cliquez sur le bouton **OK**.

8. Dans la section **Avertissement**, cliquez sur **Ajouter un événement** et cochez les cases en regard des événements suivants uniquement :

    - *L'Autodéfense de l'application est désactivée*
    - *Les modules de la protection sont désactivés*
    - *La clé de réserve est incorrecte*
    - *Un programme légitime qui peut être utilisé par des intrus pour nuire à votre ordinateur ou à vos données personnelles a été détecté (bases locales)*
    - *Un programme légitime qui peut être utilisé par des intrus pour nuire à votre ordinateur ou à vos données personnelles a été détecté (KSN)*
    - *L'objet a été supprimé*
    - *Un objet a été désinfecté*
    - *L'utilisateur a refusé la stratégie de chiffrement*
    - *Un fichier a été restauré à partir de la quarantaine sur le serveur de Kaspersky Anti Targeted Attack Platform par l'administrateur*
    - *Un fichier a été mis en quarantaine sur le serveur de Kaspersky Anti Targeted Attack Platform par l'administrateur*
    - *Message envoyé à l'administrateur sur l'interdiction du lancement de l'application*
    - *Message envoyé à l'administrateur sur l'interdiction de l'accès à l'appareil*
    - *Message envoyé à l'administrateur sur l'interdiction de l'accès à la page Internet*

9. Cliquez sur le bouton **OK**.
10. Dans la section **Information**, cliquez sur **Ajouter un événement** et cochez les cases en regard des événements suivants uniquement :

    - *Une copie de sauvegarde de l'objet a été créée*
    - *Le lancement de l'application est interdit en mode test*

11. Cliquez sur le bouton **OK**.

L'enregistrement des événements importants dans la base de données du Serveur d'administration est configuré.

Configuration manuelle d'une tâche de groupe de mise à jour de Kaspersky Endpoint Security

Pour Kaspersky Endpoint Security, la programmation optimale et recommandée est **Lors du téléchargement des mises à jour dans le stockage** quand la case **Adopter un décalage aléatoire automatique pour les lancements de tâche** est cochée.

Autorisation de l'accès hors ligne à l'appareil externe bloqué par le Contrôle des appareils

Dans le composant Contrôle des appareils de la stratégie de Kaspersky Endpoint Security for Windows, vous pouvez administrer l'accès des utilisateurs aux appareils externes qui sont installés sur l'appareil client ou qui sont connectés à celui-ci (par exemple, les disques durs, les caméras ou les modules Wi-Fi). Cela vous permet de protéger l'appareil client contre les infections lorsque de tels appareils externes sont connectés, et d'éviter les pertes ou les fuites de données.

Si vous devez accorder un accès temporaire à l'appareil externe bloqué par le Contrôle des appareils mais qu'il n'est pas possible d'ajouter l'appareil à la liste des appareils de confiance, vous pouvez accorder un accès temporaire hors ligne à l'appareil externe. L'accès hors ligne signifie que l'appareil client n'a pas accès au réseau.

Vous pouvez accorder l'accès hors ligne à l'appareil externe bloqué par le Contrôle des appareils uniquement si l'option **Autoriser la demande d'accès temporaire** est activée dans les paramètres de la stratégie de Kaspersky Endpoint Security for Windows, dans la section **Paramètres de l'application → Contrôles de sécurité → Contrôle des appareils**.

L'autorisation de l'accès hors ligne à l'appareil externe bloqué par le Contrôle des périphériques comprend les étapes suivantes :

1. Dans la boîte de dialogue de Kaspersky Endpoint Security for Windows, l'utilisateur de l'appareil qui souhaite avoir accès à l'appareil externe bloqué, génère un fichier de demande d'accès et l'envoie à l'administrateur de Kaspersky Security Center.

2. En recevant cette demande, l'administrateur de Kaspersky Security Center crée un fichier clé d'accès et l'envoie à l'utilisateur de l'appareil.

3. Dans la boîte de dialogue de Kaspersky Endpoint Security for Windows, l'utilisateur de l'appareil active le fichier de la clé d'accès et obtient un accès temporaire à l'appareil externe.

Pour accorder un accès temporaire à l'appareil externe bloqué par le Contrôle des appareils :

1. Dans le menu principal, accédez à **Ressources (Appareils) → Appareils administrés**.

   La liste des appareils administrés s'affiche.

2. Dans cette liste, sélectionnez l'appareil de l'utilisateur qui demande l'accès à l'appareil externe bloqué par le Contrôle des appareils.

   Vous ne pouvez sélectionner qu'un appareil.

3. Au-dessus de la liste des appareils administrés, cliquez sur le bouton points de suspension (...), puis cliquez sur le bouton **Autoriser l'accès à l'appareil en mode déconnecté**.

4. Dans la fenêtre **Paramètres de l'application** qui s'ouvre, dans la section **Contrôle des appareils**, cliquez sur le bouton **Parcourir**.

5. Sélectionnez le fichier de demande d'accès que vous avez reçu de l'utilisateur, puis cliquez sur le bouton **Ouvrir**. Le fichier doit être au format AKEY.

   Les détails de l'appareil verrouillé auquel l'utilisateur a demandé l'accès sont affichés.

6. Spécifiez la valeur du paramètre **Durée d'accès**.

   Ce paramètre définit la durée pendant laquelle vous autorisez l'utilisateur à accéder à l'appareil verrouillé. La valeur par défaut est celle qui a été spécifiée par l'utilisateur lors de la création du fichier de demande d'accès.

7. Précisez la période pendant laquelle la clé d'accès peut être activée sur l'appareil.

   Ce paramètre définit la période pendant laquelle l'utilisateur peut activer l'accès à l'appareil bloqué à l'aide de la clé d'accès fournie.

8. Cliquez sur le bouton **Enregistrer**.

   Cette opération ouvre la fenêtre standard de Microsoft Windows **Enregistrement de la clé d'accès**.

9. Sélectionnez le dossier de destination dans lequel vous souhaitez enregistrer le fichier contenant la clé d'accès de l'appareil bloqué.

10. Cliquez sur le bouton **Enregistrer**.

Par conséquent, lorsque vous envoyez à l'utilisateur le fichier de la clé d'accès et que l'utilisateur l'active dans la boîte de dialogue de Kaspersky Endpoint Security for Windows, l'utilisateur dispose d'un accès temporaire à l'appareil bloqué pendant une période en particulier.

Suppression d'applications ou de mises à jour logicielles à distance

Pour supprimer des applications ou des mises à jour logicielles à distance des appareils sélectionnés, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Tâches**.

2. Cliquez sur **Ajouter**.

   Ceci permet de lancer l'assistant de création d'une tâche. Parcourez les étapes de l'Assistant à l'aide du bouton **Suivant**.

3. Pour l'application Kaspersky Security Center, sélectionnez le type de tâche **Désinstallation à distance d'une application**.

4. Spécifiez le nom de la tâche créée.

   Le nom de la tâche ne peut pas contenir plus de 100 symboles et contenir de symboles spéciaux ("*<>?\:|).

5. Sélectionnez les appareils auxquels les tâches seront affectées.

6. Sélectionnez le type de logiciel que vous souhaitez supprimer, puis sélectionnez les applications, les mises à jour ou les correctifs en particulier que vous souhaitez supprimer :

   - **Désinstaller une application administrée**

     Une liste des applications de Kaspersky s'affiche. Sélectionnez l'application que vous souhaitez supprimer.

   - **Supprimer une application incompatible**

     Une liste des applications incompatibles avec les applications de sécurité Kaspersky ou Kaspersky Security Center s'affiche. Cochez les cases en regard de l'application que vous souhaitez supprimer.

   - **Supprimer une application depuis le registre des applications**

Par défaut, les Agents d'administration envoient au Serveur d'administration des informations à propos des applications installées sur les appareils administrés. La liste des applications installées est stockée dans le registre des applications.

Pour sélectionner une application dans le registre des applications :

a. Cliquez sur le champ **Application à désinstaller**, puis sélectionnez l'application que vous souhaitez supprimer.

Si vous sélectionnez l'Agent d'administration de Kaspersky Security Center, lorsque vous exécutez la tâche, l'état *Terminé avec succès* indique que le processus de suppression a démarré. Si l'Agent d'administration de Kaspersky Security Center est supprimé, l'état ne change pas. Si la tâche échoue, l'état passe à *Échec*.

b. Précisez les options de désinstallation :

- **Mode de désinstallation**

Sélectionnez la manière dont vous souhaitez supprimer l'application :

- **Définir automatiquement la commande de désinstallation**

  Si l'application dispose d'une commande de désinstallation définie par le fournisseur de l'application, Kaspersky Security Center utilise cette commande. Il est conseillé de sélectionner cette option.

- **Indiquer la commande de suppression**

  Sélectionnez cette option si vous souhaitez spécifier votre propre commande pour la désinstallation de l'application.

  Il est conseillé d'essayer d'abord de supprimer l'application en utilisant l'option **Définir automatiquement la commande de désinstallation**. Si la désinstallation via la commande définie automatiquement échoue, utilisez votre propre commande.

  Saisissez une commande d'installation dans le champ, puis indiquez l'option suivante :

  Utiliser cette commande pour désinstaller l'application uniquement si la commande par défaut n'a pas été détectée automatiquement

  Kaspersky Security Center vérifie si l'application sélectionnée dispose d'une commande de désinstallation définie par le fournisseur de l'application. Si la commande est trouvée, Kaspersky Security Center l'utilisera à la place de la commande indiquée dans le champ **Commande pour la désinstallation d'applications**.

  Il est conseillé d'activer cette option.

- **Procéder au redémarrage une fois la désinstallation réussie**

Si l'application nécessite le redémarrage du système d'exploitation sur l'appareil administré après une désinstallation réussie, le système d'exploitation est redémarré automatiquement.

- **Désinstaller la mise à jour de l'application, l'application tierce ou le correctif indiqué**

  Une liste des mises à jour, des correctifs et des applications tierces s'affiche. Sélectionnez l'élément que vous souhaitez supprimer.

  La liste affichée est une liste générale des applications et des mises à jour, et elle ne correspond pas aux applications et mises à jour installées sur les appareils administrés. Avant de sélectionner un élément, nous vous recommandons de vous assurer que l'application ou la mise à jour est installée sur les appareils définis dans la zone d'action de la tâche. Vous pouvez afficher la liste des appareils sur lesquels l'application ou la mise à jour est installée via la fenêtre des propriétés.

  Pour afficher la liste des appareils, procédez comme suit :

  a. Cliquez sur le nom de l'application ou de la mise à jour.

     La fenêtre des propriétés s'ouvre.

  b. Ouvrez la section **Appareils**.

     Vous pouvez également afficher la liste des applications installées et des mises à jour dans la fenêtre des propriétés de l'appareil.

7. Indiquez comment les appareils clients téléchargeront l'utilitaire de désinstallation :

- **En utilisant l'Agent d'administration**

  Les fichiers sont livrés aux appareils clients par l'Agent d'administration installé sur ces appareils clients.

  Si cette option est désactivée, les fichiers sont livrés à l'aide des outils Microsoft Windows.

  Il est recommandé d'activer cette option si la tâche concerne des appareils sur lesquels un Agent d'administration est installé.

- **En utilisant les ressources du système d'exploitation via le Serveur d'administration**

  Les fichiers sont transmis aux appareils clients à l'aide des outils du système d'exploitation du Serveur d'administration. Cette option peut être activée si l'Agent d'administration n'est pas installé sur l'appareil client, mais que l'appareil client se trouve sur le même réseau que le Serveur d'administration.

- **En utilisant les ressources du système d'exploitation via les points de distribution**

  Les fichiers sont transmis aux appareils clients à l'aide des outils du système d'exploitation via les points de distribution. Cette option peut être activée si au moins un point de distribution se trouve sur le réseau.

  Si l'option **En utilisant l'Agent d'administration** est activée, les fichiers seront livrés via les outils du système d'exploitation uniquement dans le cas où il n'est pas possible d'utiliser les outils de l'Agent d'administration.

- **Nombre maximal de téléchargements simultanés**

  Nombre maximal autorisé d'appareils clients auxquels le Serveur d'administration peut transmettre simultanément les fichiers. Plus ce nombre est élevé, plus l'application sera désinstallée rapidement, mais plus la charge sur le Serveur d'administration sera élevée.

- **Nombre maximal de tentatives de désinstallation**

Si, lors de l'exécution de la tâche *Désinstallation à distance d'une application*, Kaspersky Security Center ne parvient pas à désinstaller une application sur un appareil administré conformément au nombre d'exécutions du programme d'installation paramétré, Kaspersky Security Center arrête de distribuer l'utilitaire de désinstallation à cet appareil administré et ne démarre plus le programme d'installation sur l'appareil.

Le paramètre **Nombre maximal de tentatives de désinstallation** vous permet d'enregistrer les ressources de l'appareil administré et de réduire le trafic (désinstallation, exécution du fichier MSI et messages d'erreur).

Des tentatives de démarrage de tâches récurrentes peuvent indiquer un problème qui empêche la désinstallation sur l'appareil. L'administrateur doit résoudre le problème dans le nombre de tentatives de désinstallation indiqué, puis redémarrer la tâche (manuellement ou selon une planification).

Si la désinstallation n'est finalement pas réalisée, le problème est considéré comme insoluble et toutes les tâches supplémentaires à entreprendre sont déclarées coûteuses à cause de la consommation inutile de ressources et de bande passante.

Lorsque la tâche est créée, le compteur de tentatives est défini sur `0`. Chaque exécution du programme d'installation qui renvoie une erreur sur l'appareil incrémente la valeur du compteur.

Si le nombre de tentatives paramétré est dépassé et que l'appareil est prêt pour la désinstallation de l'application, vous pouvez augmenter la valeur du paramètre **Nombre maximal de tentatives de désinstallation** et lancer la tâche de désinstallation de l'application. Sinon, vous pouvez aussi créer une nouvelle tâche *Désinstallation à distance d'une application*.

- **Vérifier le type de système d'exploitation avant le téléchargement**

  Avant de transmettre les fichiers aux appareils clients, Kaspersky Security Center vérifie si les paramètres de l'utilitaire d'installation sont applicables au système d'exploitation de l'appareil client. Si les paramètres ne sont pas applicables, Kaspersky Security Center ne transmet pas les fichiers et n'essaie pas d'installer l'application. Par exemple, pour installer une application quelconque sur les appareils d'un groupe d'administration qui comprend des appareils fonctionnant sous divers systèmes d'exploitation, vous pouvez attribuer la tâche d'installation au groupe d'administration, puis activer cette option pour ignorer les appareils qui fonctionnent sous un système d'exploitation autre que celui requis.

- **Utiliser un mot de passe de désinstallation**

  Ce paramètre s'affiche si, à l'étape précédente, vous avez sélectionné **Désinstaller l'application administrée**, puis avez spécifié l'Agent d'administration de Kaspersky Security Center dans le champ **Application à désinstaller**.

  Si vous avez défini auparavant le mot de passe pour la désinstallation à distance de l'Agent d'administration dans les paramètres de stratégie de l'Agent d'administration, cochez la case **Utiliser le mot de passe de désinstallation**, puis saisissez le mot de passe pour la désinstallation dans le champ **Mot de passe**. Si vous n'avez pas défini le mot de passe pour la désinstallation à distance de l'Agent d'administration, ne cochez pas la case.

8. Définissez les paramètres de redémarrage du système d'exploitation :

- **Ne pas redémarrer l'appareil**

  Les appareils clients ne redémarrent pas automatiquement après l'opération. Pour arrêter le fonctionnement, il faut redémarrer l'appareil (par exemple, manuellement ou à l'aide d'une tâche d'administration des appareils). Les informations sur la nécessité du redémarrage sont enregistrées dans les résultats de la tâche et dans l'état de l'appareil. Cette option convient aux tâches d' sur les serveurs et autres appareils pour lesquels la continuité des opérations est critique.

- **Redémarrer l'appareil**

  Dans ce cas, le redémarrage des appareils clients est toujours exécuté automatiquement, si celui-ci est requis pour terminer l'opération. Cette option convient aux tâches d' sur des appareils pour lesquels des interruptions périodiques sont admises (débranchement, redémarrage).

- **Confirmer l'action auprès de l'utilisateur**

  Le message qui signale que l'appareil client doit être redémarré manuellement s'affiche sur l'écran de l'appareil. Pour cette option, il est possible de configurer des paramètres avancés : le texte du message pour l'utilisateur, la fréquence du message, ainsi que le délai à l'issue duquel le redémarrage sera forcé (sans confirmation de l'utilisateur). Cette option convient le mieux pour les postes de travail sur lesquels les utilisateurs doivent pouvoir sélectionner l'heure de redémarrage qui leur convient le mieux.

  Cette option est sélectionnée par défaut.

- **Répéter la demande toutes les (min.)**

  Quand cette option est activée, l'application invite l'utilisateur à redémarrer le système d'exploitation selon la fréquence indiquée.

  Cette option est activée par défaut. L'intervalle par défaut est de 5 minutes. La valeur peut être comprise entre 1 et 1 440 minutes.

  Si cette option est désactivée, l'invite est affichée une seule fois.

- **Redémarrer le système au bout de (min.)**

  Après avoir averti l'utilisateur, l'application force le redémarrage du système d'exploitation à l'issue de l'intervalle défini.

  Cette option est activée par défaut. Le délai par défaut est de 30 minutes. La valeur peut être comprise entre 1 et 1 440 minutes.

- **Forcer la fermeture des applications dans les sessions bloquées**

Les applications en cours d'exécution peuvent empêcher le redémarrage de l'appareil client. Par exemple, si un document est en train d'être modifié dans un logiciel de traitement de texte et qu'il n'est pas enregistré, l'application n'autorise pas le redémarrage de l'appareil.

Quand cette option est activée, l'arrêt forcé de ces applications sur un appareil verrouillé doit avoir lieu avant de pouvoir redémarrer l'appareil. Les utilisateurs pourraient perdre toute modification qui n'a pas été enregistrée à ce moment.

Si cette option est désactivée, un appareil verrouillé n'est pas redémarré. L'état de la tâche sur cet appareil indique qu'il faut redémarrer l'appareil. Les utilisateurs doivent quitter manuellement toutes les applications en cours d'exécution sur les appareils verrouillés, puis redémarrer ces appareils.

Cette option est Inactif par défaut.

9. Si nécessaire, ajoutez les comptes utilisateurs qui seront utilisés pour démarrer la tâche de désinstallation à distance :

- **Compte utilisateur non requis (Agent d'administration installé)**

  Si cette option est sélectionnée, il n'est pas nécessaire d'indiquer le compte utilisateur au nom duquel l'installateur de l'application sera lancé. La tâche est lancée sous le même compte utilisateur que le compte du service du Serveur d'administration.

  Si l'agent d'administration n'est pas installé sur les appareils clients, l'option n'est pas disponible.

- **Compte utilisateur requis (Agent d'administration non utilisé)**

  Sélectionnez cette option si l'Agent d'administration n'est pas installé sur les appareils pour lesquels vous affectez la tâche *Désinstaller l'application à distance*. Dans ce cas, vous pouvez spécifier un compte utilisateur ou un certificat SSH pour désinstaller l'application.

  - **Compte utilisateur local**. Si cette option est sélectionnée, spécifiez le compte utilisateur sous lequel le programme d'installation de l'application sera exécuté. Cliquez sur le bouton **Ajouter**, sélectionnez **Compte utilisateur local**, puis indiquez les informations d'identification du compte utilisateur.

    Vous pouvez désigner plusieurs comptes utilisateurs si aucun d'entre eux ne possède les privilèges nécessaires sur tous les appareils auxquels vous affectez la tâche. Dans ce cas, tous les comptes ajoutés sont utilisés pour exécuter la tâche, dans un ordre consécutif, de haut en bas.

  - **Certificat SSH**. Si vous souhaitez désinstaller l'application à partir d'un appareil client basé sur Linux, vous pouvez indiquer un certificat SSH au lieu d'un compte utilisateur. Cliquez sur le bouton **Ajouter**, sélectionnez **Certificat SSH**, puis indiquez les clés privée et publique du certificat.

    Pour générer une clé privée, vous pouvez utiliser l'utilitaire ssh-keygen. Notez que Kaspersky Security Center prend en charge le format PEM des clés privées, mais que l'utilitaire ssh-keygen génère par défaut des clés SSH au format OPENSSH. Le format OPENSSH n'est pas pris en charge par Kaspersky Security Center. Pour créer une clé privée au format PEM pris en charge, ajoutez l'option -m PEM dans la commande ssh-keygen.

    Par exemple :

    ```
    ssh-keygen -m PEM -t rsa -b 4096 -C "<user email>"
    ```

10. Si vous souhaitez modifier les paramètres de la tâche par défaut, activez l'option **Ouvrir les détails de la tâche à la fin de la création** sur la page **Fin de la création de la tâche**. Si vous n'activez pas cette tâche, la tâche est créée selon les paramètres par défaut. Vous pourrez modifier ces paramètres par défaut plus tard, à tout moment.

11. Cliquez sur le bouton **Terminer**.

    La tâche est créée et s'affiche dans la liste des tâches.

12. Cliquez sur le nom de la tâche créée pour ouvrir la fenêtre de propriétés de la tâche.

13. Dans la fenêtre des propriétés de la tâche, indiquez les paramètres généraux de la tâche.

14. Cliquez sur le bouton **Enregistrer**.

15. Lancez la tâche manuellement ou attendez son lancement conformément à la planification que vous avez indiquée dans les paramètres de la tâche.

    Suite à l'exécution de la tâche de désinstallation à distance, l'application sélectionnée sera supprimée des appareils sélectionnés.

Problèmes de désinstallation à distance

Parfois, lors de la désinstallation à distance d'applications tierces, il se peut que l'avertissement suivant s'affiche : " Désinstallation à distance terminée sur l'appareil avec avertissement : l'application à supprimer n'est pas installée. " Ce problème survient lorsque l'application destinée à être désinstallée a déjà été désinstallée ou a été installée uniquement pour un utilisateur individuel. Les applications installées pour un utilisateur individuel (également appelées applications par utilisateur) deviennent invisibles et ne peuvent pas être désinstallées à distance si l'utilisateur n'est pas connecté.

Ce comportement diffère des applications destinées à être utilisées par plusieurs utilisateurs sur le même appareil (également appelées applications par appareil). Les applications par appareil sont visibles et accessibles à tous les utilisateurs de l'appareil.

Par conséquent, les applications par utilisateur doivent être désinstallées uniquement lorsque l'utilisateur est connecté.

Source d'informations sur les applications installées

L'Agent d'administration récupère des informations sur les logiciels installés sur les appareils Windows à partir des clés de registre suivantes :

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall

  Contient des informations sur les applications installées pour tous les utilisateurs.

- HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall

  Contient des informations sur les applications installées pour tous les utilisateurs.

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall

  Contient des informations sur les applications installées pour l'utilisateur actuel.

- HKEY_USER<...>\Software\Microsoft\Windows\CurrentVersion\Uninstall

  Contient des informations sur les applications installées pour des utilisateurs particuliers.

Tâches

Cette section décrit les tâches utilisées par Kaspersky Security Center.

À propos des tâches

Kaspersky Security Center gère le fonctionnement des protection applications Kaspersky installées sur les appareils par la création et l'exécution des *tâches*. Les tâches permettent d'exécuter l'installation, le lancement et l'arrêt des applications, l'analyse des fichiers, la mise à jour des bases de données et des modules des applications, les autres actions avec les applications.

Les tâches pour une application définie peuvent être créées à l'aide de Kaspersky Security Center Web Console uniquement si le plug-in d'administration de cette application est installé sur le serveur de Kaspersky Security Center Web Console.

Les tâches peuvent être exécutées sur le Sur le Serveur d'administration et sur les appareils.

Les tâches exécutées sur le Serveur d'administration sont les suivantes :

- Diffusion automatique des rapports
- Téléchargement des mises à jour dans le stockage
- Sauvegarde des données du Serveur d'administration
- Maintenance de la base de données

Les types de tâche suivants sont réalisés sur les appareils :

- *Tâches* exécutées sur un appareil particulier

  Les tâches locales peuvent être modifiées non seulement par l'administrateur via la Console d'administration, mais aussi par l'utilisateur de l'appareil distant (par exemple, dans l'interface de l'application de sécurité). Si la tâche locale a été modifiée simultanément par l'administrateur et l'utilisateur sur l'appareil administré, ce sont les modifications introduites par l'administrateur qui sont retenues car elles ont une priorité supérieure.

- *Tâches de groupe* : tâches qui sont réalisées sur tous les appareils d'un groupe particulier

  Sauf indication contraire dans les propriétés de la tâche, une tâche de groupe peut également avoir un impact sur les sous-groupes du groupe sélectionné. Une tâche de groupe agit aussi (de manière facultative) sur les appareils connectés aux Serveurs d'administration virtuels et secondaires placés dans ce groupe et ses sous-groupes.

- *Tâches* — Tâches exécutées sur les appareils un ensemble de peu importe leur inclusion dans les groupes d'administration.

Pour chaque application vous pouvez créer n'importe quel nombre de tâches de groupe, de tâches globales et des tâches locales.

Vous pouvez modifier les paramètres des tâches en l'exécution des tâches, copier, exporter ou importer, ainsi que supprimer les Tâches.

Les tâches ne sont lancées sur un appareil que lorsque l'application pour laquelle les tâches ont été créées est lancée.

Les résultats de l'exécution des tâches sont enregistrés dans le journal des événements du SE sur chaque appareil, dans le journal des événements du SE sur le Serveur d'administration et dans la base de données du Serveur d'administration.

N'incluez pas de données confidentielles dans les paramètres des tâches. Par exemple, le mot de passe de l'administrateur de domaine.

À propos de la zone d'action des tâches

La *zone d'action d'une tâche* est l'ensemble d'appareils sur lesquels la tâche est réalisée. Voici les types de zone d'action :

- Pour une *tâche locale*, la zone d'action est l'appareil en lui-même.
- Pour une *tâche du Serveur d'administration*, la zone d'action est le Serveur d'administration.
- Pour une *tâche de groupe*, la zone d'action est la liste des appareils inclus dans le groupe.

Lors de la création d'une *tâche globale*, vous pouvez utiliser les méthodes suivantes afin de définir la zone d'action :

- Désignation manuelle de certains appareils.

  Vous pouvez utiliser l'adresse IP (ou l'intervalle IP), le nom NetBIOS ou le nom DNS en tant que l'adresse de l'appareil.

- Importer la liste des appareils depuis le fichier au format TXT, contenant la les adresses des appareils ajoutés (chaque adresse doit se trouver dans une ligne séparée).

  Si la liste des appareils est importée depuis le fichier ou formée manuellement et les appareils sont identifiés selon le nom, uniquement les appareils dont les informations sont déjà enregistrées dans la base de données du Serveur d'administration peuvent être ajoutés dans la liste lors de la connexion des appareils ou lors du. De plus, l'information doit avoir été saisie quand ces appareils étaient connectés ou lors de la recherche d'appareils.

- Indiquer une sélection d'appareils.

  Au fil du temps, la zone d'action de la tâche change au fur et à mesure que change la quantité d'appareils qui figurent dans la sélection. La sélection d'appareils peut s'opérer sur la base des attributs des appareils, notamment sur la base du logiciel installé sur l'appareil, ainsi que sur la base des tags attribués à l'appareil. La sélection d'appareils est la méthode la plus flexible pour définir la zone d'action d'une tâche.

  Le Serveur d'administration se charge toujours de la programmation des tâches pour les sélections d'appareils. Ces tâches ne seront pas lancées sur les appareils qui ne communiquent pas avec le Serveur d'administration. Les tâches dont la zone d'action est définie à l'aide d'autres méthodes sont exécutées directement sur les appareils et par conséquent, elles ne dépendent pas de la connexion de l'appareil au Serveur d'administration.

Les tâches pour les sélections d'appareils sont lancées non selon l'heure locale de l'appareil, mais bien selon l'heure locale du Serveur d'administration. Les tâches dont la zone d'action est définie par d'autres méthodes sont exécutées à l'heure locale de l'appareil.

Création d'une tâche

Pour créer une tâche, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Tâches**.
2. Cliquez sur **Ajouter**.

   Ceci permet de lancer l'assistant de création d'une tâche. Suivez-en les instructions.
3. Si vous souhaitez modifier les paramètres de la tâche par défaut, activez l'option **Ouvrir les détails de la tâche à la fin de la création** sur la page **Fin de la création de la tâche**. Si vous n'activez pas cette tâche, la tâche est créée selon les paramètres par défaut. Vous pourrez modifier ces paramètres par défaut plus tard, à tout moment.
4. Cliquez sur le bouton **Terminer**.

La tâche est créée et s'affiche dans la liste des tâches.

Pour créer une tâche attribuée aux appareils sélectionnés, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Appareils administrés**.

   La liste des appareils administrés s'affiche.
2. Dans la liste des appareils administrés, cochez les cases en regard des appareils pour exécuter la tâche à leur place. Vous pouvez utiliser les fonctions de recherche et de filtrage pour trouver les appareils que vous cherchez.
3. Cliquez sur le bouton **Lancer la tâche**, puis sélectionnez **Création d'une tâche**.

   Ceci permet de lancer l'Assistant de création d'une tâche.

   À la première étape de l'Assistant, vous pouvez supprimer les appareils sélectionnés pour les inclure dans la zone d'action de la tâche. Suivez les instructions de l'Assistant.
4. Cliquez sur le bouton **Terminer**.

La tâche pour les appareils sélectionnés est créée.

Lancer une tâche manuellement

L'application démarre les tâches en fonction des paramètres de planification spécifiés dans les propriétés de chaque tâche. Vous pouvez lancer une tâche manuellement à tout moment à partir de la liste des tâches. Vous pouvez également sélectionner des appareils dans la liste **Appareils administrés**, puis démarrer une tâche existante pour eux.

Pour démarrer une tâche manuellement :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Tâches**.
2. Dans la liste des tâches, cochez la case en regard de la tâche que vous souhaitez démarrer.
3. Cliquez sur le bouton **Démarrer**.

La tâche sera lancée. Vous pouvez vérifier l'état de la tâche dans la colonne **État** ou en cliquant sur le bouton **Résultat**.

Affichage de la liste des tâches

Vous pouvez afficher la liste des tâches créées dans Kaspersky Security Center.

Pour afficher la liste des tâches,

Dans le menu principal, accédez à **Ressources (Appareils)** → **Tâches**.

La liste des tâches s'affiche. Les tâches sont regroupées par nom d'application auquel elles sont liées. Par exemple, la tâche *Désinstallation à distance d'une application* est liée au Serveur d'administration et la tâche *Recherche de vulnérabilités et de mises à jour requises* se rapporte à l'Agent d'administration.

Pour afficher les propriétés d'une tâche,

Cliquez sur le nom de la tâche.

La fenêtre des propriétés de la tâche s'affiche avec plusieurs onglets nommés. Par exemple, le **Type de tâche** s'affiche sous l'onglet **Général** et la planification des tâches, sous l'onglet **Programmation**.

Paramètre de la tâche générale

Cette section contient les paramètres que vous pouvez afficher et configurer pour la plupart de vos tâches. La liste des paramètres disponibles dépend de la tâche que vous configurez.

Paramètres définis lors de la création d'une tâche

Vous pouvez définir les paramètres suivants lors de la création d'une tâche. Certains de ces paramètres peuvent également être modifiés dans les propriétés de la tâche créée.

- Paramètres de redémarrage du système d'exploitation :
  - **Ne pas redémarrer l'appareil**

    Les appareils clients ne redémarrent pas automatiquement après l'opération. Pour arrêter le fonctionnement, il faut redémarrer l'appareil (par exemple, manuellement ou à l'aide d'une tâche d'administration des appareils). Les informations sur la nécessité du redémarrage sont enregistrées dans les résultats de la tâche et dans l'état de l'appareil. Cette option convient aux tâches d' sur les serveurs et autres appareils pour lesquels la continuité des opérations est critique.

  - **Redémarrer l'appareil**

    Dans ce cas, le redémarrage des appareils clients est toujours exécuté automatiquement, si celui-ci est requis pour terminer l'opération. Cette option convient aux tâches d' sur des appareils pour lesquels des interruptions périodiques sont admises (débranchement, redémarrage).

  - **Confirmer l'action auprès de l'utilisateur**

    Le message qui signale que l'appareil client doit être redémarré manuellement s'affiche sur l'écran de l'appareil. Pour cette option, il est possible de configurer des paramètres avancés : le texte du message pour l'utilisateur, la fréquence du message, ainsi que le délai à l'issue duquel le redémarrage sera forcé (sans confirmation de l'utilisateur). Cette option convient le mieux pour les postes de travail sur lesquels les utilisateurs doivent pouvoir sélectionner l'heure de redémarrage qui leur convient le mieux.

    Cette option est sélectionnée par défaut.

  - **Répéter la demande toutes les (min.)**

    Quand cette option est activée, l'application invite l'utilisateur à redémarrer le système d'exploitation selon la fréquence indiquée.

    Cette option est activée par défaut. L'intervalle par défaut est de 5 minutes. La valeur peut être comprise entre 1 et 1 440 minutes.

    Si cette option est désactivée, l'invite est affichée une seule fois.

  - **Redémarrer le système au bout de (min.)**

    Après avoir averti l'utilisateur, l'application force le redémarrage du système d'exploitation à l'issue de l'intervalle défini.

    Cette option est activée par défaut. Le délai par défaut est de 30 minutes. La valeur peut être comprise entre 1 et 1 440 minutes.

  - **Forcer la fermeture des applications dans les sessions bloquées**

Les applications en cours d'exécution peuvent empêcher le redémarrage de l'appareil client. Par exemple, si un document est en train d'être modifié dans un logiciel de traitement de texte et qu'il n'est pas enregistré, l'application n'autorise pas le redémarrage de l'appareil.

Quand cette option est activée, l'arrêt forcé de ces applications sur un appareil verrouillé doit avoir lieu avant de pouvoir redémarrer l'appareil. Les utilisateurs pourraient perdre toute modification qui n'a pas été enregistrée à ce moment.

Si cette option est désactivée, un appareil verrouillé n'est pas redémarré. L'état de la tâche sur cet appareil indique qu'il faut redémarrer l'appareil. Les utilisateurs doivent quitter manuellement toutes les applications en cours d'exécution sur les appareils verrouillés, puis redémarrer ces appareils.

Cette option est Inactif par défaut.

- Paramètres du calendrier de la tâche :

  Le type de planification peut varier en fonction de la tâche.

  - **Paramètre Démarrer la tâche :**

    - Toutes les N heures

      La tâche s'exécute régulièrement, selon l'intervalle défini en heures, à partir de la date et heure définis.

      La tâche s'exécute par défaut toutes les six heures à partir de la date et de l'heure actuelles du système.

    - Tous les N jours

      La tâche s'exécute régulièrement, selon l'intervalle défini en jours. En outre, vous pouvez spécifier la date et l'heure de la première exécution de la tâche. Ces options supplémentaires deviennent disponibles si elles sont prises en charge par l'application pour laquelle vous créez la tâche.

      La tâche s'exécute par défaut chaque jour, à partir de la date et de l'heure actuelle du système.

    - Toutes les N minutes

      La tâche s'exécute régulièrement, à l'intervalle défini en minutes, à partir de l'heure indiquée le jour de la création de la tâche.

      La tâche s'exécute par défaut toutes les 30 minutes, à partir de l'heure actuelle du système.

    - Par jours de la semaine

      La tâche s'exécute régulièrement les jours définis de la semaine, à l'heure indiquée.

      Par défaut, la tâche s'exécute chaque vendredi à 18h00.

    - Chaque mois

La tâche s'exécute régulièrement le jour du mois défini, à l'heure indiquée.

Si le jour en question ne figure pas dans le mois, la tâche s'exécute le dernier jour.

La tâche s'exécute par défaut le premier jour de chaque mois, à l'heure système actuelle.

- **Manuel**

  La tâche ne s'exécute pas automatiquement. Vous pouvez uniquement la lancer manuellement.

  Cette option est sélectionnée par défaut.

- **Chaque mois, les jours indiqués des semaines sélectionnées**

  La tâche s'exécute régulièrement les jours du mois définis, à l'heure indiquée.

  Par défaut, aucun jour du mois n'est sélectionné. L'heure de début par défaut est 18:00.

- **Lors du téléchargement des mises à jour dans le stockage**

  La tâche s'exécute après le téléchargement des mises à jour dans le stockage. Par exemple, vous pouvez utiliser cette programmation pour rechercher les vulnérabilités et les mises à jour requises.

- **Lors de la détection d'une attaque de virus**

  La tâche s'exécute après un événement *Attaque de virus* de virus. Sélectionnez les types d'application qui vont surveiller les propagations de virus. Les types suivants de Application sont présent :

  - Antivirus pour postes de travail et serveurs de fichiers
  - Antivirus de protection du périmètre
  - Antivirus pour systèmes de messagerie

  Tous les types d'application sont cochés par défaut.

  Il se peut que vous souhaitiez exécuter différentes tâches en fonction du type d'application de sécurité qui signale une propagation de virus. Dans ce cas, supprimez la sélection des types d'application dont vous n'avez pas besoin.

- **Après l'exécution d'une autre tâche**

La tâche actuelle démarre à la fin d'une autre tâche. Cette option ne fonctionne que si les deux tâches sont affectées aux mêmes appareils. Par exemple, vous pouvez exécuter la tâche *Administration des appareils* avec l'option **&Activer l'appareil** et, une fois celle-ci terminée, exécuter la tâche de *recherche de virus* comme tâche de déclenchement.

Il faut sélectionner la tâche de déclenchement dans le tableau et l'état avec lequel cette tâche doit se terminer (**Terminée avec succès** ou **Échec**).

Si nécessaire, vous pouvez rechercher, trier et filtrer les tâches dans le tableau comme suit :

- Saisissez le nom de la tâche dans le champ de recherche pour rechercher une tâche par son nom.
- Cliquez sur l'icône de tri pour trier les tâches par nom.

  Par défaut, les tâches sont triées par ordre alphabétique croissant.
- Cliquez sur l'icône du filtre, et dans la fenêtre qui s'ouvre, filtrez les tâches par groupe, puis cliquez sur le bouton **Appliquer**.

- **Lancer les tâches non exécutées**

  Cette option détermine le comportement d'une tâche si un appareil client n'est pas visible sur le réseau quand la tâche est sur le point de démarrer.

  Si la case est Activé, lors du lancement suivant de l'application de Kaspersky sur cet appareil client, une tentative de lancement de la tâche sera faite. Si la programmation de la tâche est **Manuel**, **Une fois** ou **Immédiatement**, la tâche est immédiatement lancée dès que l'appareil apparaît sur le réseau ou immédiatement après l'inclusion de l'appareil dans la zone d'action de la tâche.

  Si cette option est désactivée, seules les tâches planifiées s'exécutent sur les appareils clients. Pour les planifications **Manuel**, **Une fois** et **Immédiatement**, les tâches s'exécutent uniquement sur les appareils clients qui sont visibles sur le réseau. Par exemple, vous pouvez désactiver cette option pour une tâche qui consomme des ressources que vous voulez exécuter uniquement en dehors des heures de bureau.

  Cette option est Inactif par défaut.

- **Adopter un décalage aléatoire automatique pour les lancements de tâche**

  Si cette option est activée, la tâche est lancée sur les appareils clients de manière aléatoire au cours d'un intervalle défini. C'est ce qu'on appelle un *lancement échelonné d'une tâche*. Un lancement échelonné de tâche permet d'éviter la communication simultanée d'un nombre important d'appareils clients avec le Serveur d'administration lors du lancement de la tâche programmée.

  Le temps du lancement aléatoire est automatiquement calculée lors de la création d'une tâche selon le nombre d'appareils clients sur lesquels la tâche est diffusée. Par la suite, la tâche démarre toujours à l'heure de lancement calculée. Toutefois, quand les paramètres de la tâche sont modifiés ou si la tâche est lancée manuellement, la valeur calculée de l'heure de lancement de la tâche est modifiée.

  Si la case n'est pas cochée, le lancement de la tâche sur les appareils clients s'opère selon la planification.

- **Décaler aléatoirement et automatiquement le lancement de la tâche dans un intervalle de**

Si cette option est activée, la tâche est lancée sur les appareils clients de manière aléatoire au cours de l'intervalle défini. Un lancement échelonné de tâche permet d'éviter la communication simultanée d'un nombre important d'appareils clients avec le Serveur d'administration lors du lancement de la tâche programmée.

Si la case n'est pas cochée, le lancement de la tâche sur les appareils clients s'opère selon la planification.

Cette option est Inactif par défaut. Par défaut, la valeur de cet intervalle est de une minute.

- Les appareils auxquels les tâches seront affectées :
  - **Sélectionner les appareils détectés sur le réseau par le Serveur d'administration**

    la tâche est affectée à un ensemble d'appareils. L'ensemble d'appareils peut reprendre aussi bien des appareils de groupes d'administration que des appareils non définis.

    Par exemple, vous pourriez utiliser cette option dans une tâche d'installation d'un Agent d'administration sur des appareils non définis.

  - **Définir les adresses des appareils manuellement ou les importer à partir d'une liste**

    Vous pouvez définir les noms NetBIOS, les noms DNS, les adresses IP, ainsi que les plages d'adresses IP auxquels il convient d'affecter la tâche.

    Vous pourriez utiliser cette option pour exécuter une tâche pour un sous-réseau défini. Par exemple, vous pourriez souhaiter installer une certaine application sur les appareils des comptables ou analyser des appareils dans un sous-réseau qui est probablement infecté.

  - **Attribuer la tâche à une sélection d'appareils**

    La tâche est affectée aux appareils qui appartiennent à une sélection d'appareils. Vous pouvez définir une des sélections existantes.

    Par exemple, vous pourriez souhaiter utiliser cette option pour exécuter une tâche sur des appareils dotés d'une version du système d'exploitation spécifique.

  - **Attribuer la tâche à un groupe d'administration**

    La tâche est affectée aux appareils qui appartiennent à un groupe d'administration. Vous pouvez renseigner un des groupes existants ou en créer un.

    Par exemple, vous pourriez souhaiter utiliser cette option pour exécuter une tâche d'envoi de messages pour les utilisateurs si le message est particulier pour les appareils repris dans un groupe d'administration spécifique.

    Si une tâche est attribuée à un groupe d'administration, l'onglet **Sécurité** ne s'affiche pas dans la fenêtre des propriétés de la tâche, car les tâches de groupe sont soumises aux paramètres de sécurité des groupes auxquels elles s'appliquent.

- Paramètres du compte :
  - **Compte par défaut**

    La tâche sera lancée sous le même compte utilisateur sous lequel l'application, exécutant cette tâche, a été installée et lancée.

    Cette option est sélectionnée par défaut.

  - **Indiquer le compte utilisateur**

    Remplissez les champs **Compte utilisateur** et **Mot de passe** pour définir les détails d'un compte à partir duquel la tâche est exécutée. Le compte doit disposer de droits suffisants pour cette tâche.

- **Compte utilisateur**

  Le compte utilisateur au nom duquel la tâche sera lancée.

- **Mot de passe**

  Mot de passe du compte utilisateur au nom duquel la tâche sera lancée.

Paramètres définis après la création de la tâche

Vous pouvez définir les paramètres suivants uniquement après qu'une tâche a été créée.

- Paramètres de la tâche de groupe :
  - **Distribuer aux sous-groupes**

    Cette option est disponible uniquement dans les paramètres des tâches de groupe.

    Lorsque cette option est activée, la zone d'action de la tâche inclut :

    - Le groupe d'administration que vous avez sélectionné lors de la création de la tâche.
    - Les groupes d'administration subordonnés au groupe d'administration sélectionné à n'importe quel niveau inférieur dans la hiérarchie des groupes.

    Lorsque cette option est désactivée, la zone d'action de la tâche inclut uniquement le groupe d'administration que vous avez sélectionné lors de la création de la tâche.

    Cette option est activée par défaut.

  - **Envoyer aux Serveurs d'administration secondaires et virtuels**

    Lorsque cette option est activée, la tâche effective sur le Serveur d'administration principal est également appliquée sur les Serveurs d'administration secondaires (y compris virtuels). Si une tâche du même type existe déjà sur le Serveur d'administration secondaire, les deux tâches sont appliquées sur le Serveur d'administration secondaire, celui existant et celui hérité du Serveur d'administration principal.

    Cette option est disponible uniquement lorsque l'option **Distribuer aux sous-groupes** est activée.

    Cette option est Inactif par défaut.

- Paramètres de programmation avancés :
  - **Allumer les appareils en utilisant la fonctionnalité Wake-on-LAN avant le lancement de la tâche**

    Le système d'exploitation sur l'appareil démarre au délai indiqué avant le lancement de la tâche. Par défaut, la valeur de cet délai de est de une minute.

    Activez cette option si vous souhaitez que la tâche soit exécutée sur tous les appareils clients de la zone d'action de la tâche, y compris pour les appareils éteints alors que la tâche est sur le point de démarrer.

    Si vous souhaitez que l'appareil soit automatiquement éteint une fois la tâche terminée, activez l'option **Arrêter les appareils après la fin de la tâche**. Cette option se trouve dans la même fenêtre.

    Cette option est Inactif par défaut.

  - **Arrêter les appareils après la fin de la tâche**

Par exemple, vous pouvez activer cette option pour une tâche d'installation de mise à jour qui installe les mises à jour sur les appareils client chaque vendredi après la fermeture des bureaux, puis éteint ces appareils pour le week-end.

Cette option est Inactif par défaut.

- **Arrêter la tâche si elle prend plus de**

  A l'issue du délai défini, la tâche s'arrêt automatiquement, qu'elle soit finie ou non.

  Activez cette option si vous souhaitez interrompre (ou arrêter) les tâches dont l'exécution dure trop longtemps.

  Cette option est Inactif par défaut. La durée d'exécution de la tâche par défaut est de 120 minutes.

- Paramètres des notifications :
  - Groupe **Sauvegarder le résultat** :
    - Conserver dans la base de données du Serveur pendant (jours)

      Les événements de l'application en rapport avec l'exécution de la tâche sur tous les appareils clients de la zone d'action de la tâche sont stockés sur le Serveur d'administration pendant le nombre de jours indiqué. A l'issue de cette période, les informations sont supprimées du Serveur d'administration.

      Cette option est activée par défaut.

    - Conserver dans le journal des événements du SE sur l'appareil

      Les événements de l'application en rapport avec l'exécution de la tâche sont stockés localement dans le journal des événements Windows de chaque appareil client.

      Cette option est Inactif par défaut.

    - Dans le journal des événements du SE du Serveur d'administration

      Les événements de l'application en rapport avec l'exécution de la tâche sur tous les appareils clients de la zone d'action de la tâche sont stockés centralement dans le journal des événements Windows du système d'exploitation du Serveur d'administration.

      Cette option est Inactif par défaut.

    - Sauvegarder tous les événements

      Quand cette option est sélectionnée, tous les événements liés à la tâche sont enregistrés dans les journaux des événements.

    - Sauvegarder les événements relatifs à la progression de la tâche

      Quand cette option est sélectionnée, seuls les événements liés à l'exécution de la tâche sont enregistrés dans les journaux des événements.

    - Sauvegarder uniquement le résultat de la tâche

      Quand cette option est sélectionnée, seuls les événements liés aux résultats des tâches sont enregistrés dans les journaux des événements.

  - Notifier les résultats

    Vous pouvez choisir les méthodes selon lesquelles les administrateurs reçoivent des notifications relatives aux résultats de l'exécution de la tâche : par email, par SMS ou via le lancement du fichier exécutable. Pour configurer les notifications, cliquez sur le lien **Paramètres**.

    Par défaut, toutes les méthodes de notification sont désactivées.

  - Notifier uniquement les erreurs

Si cette option est activée, les administrateurs ne sont informés que si l'exécution d'une tâche se termine avec une erreur.

Si cette option est désactivée, les administrateurs sont informés après chaque exécution de la tâche.

Cette option est activée par défaut.

- Paramètres de sécurité.
- Paramètres de la zone d'action de la tâche.

  Selon la définition de la zone d'action de la tâche, les paramètres suivants sont proposés :

  - Appareils

    Si la zone d'action de la tâche est déterminée par un groupe d'administration, vous pouvez voir ce groupe. Aucune modification n'est disponible ici. Cependant, vous pouvez définir **Exclusions de la zone d'action de la tâche**.

    Si la zone d'action d'une tâche est déterminée par une liste d'appareils, vous pouvez modifier cette liste en ajoutant et en supprimant des appareils.

  - Sélection d'appareils

    Vous pouvez modifier la sélection d'appareils à laquelle la tâche est appliquée.

  - Exclusions de la zone d'action de la tâche

    Vous pouvez définir les groupes d'appareils auxquels la tâche n'est pas appliquée. Les groupes à exclure peuvent uniquement être des sous-groupes du groupe d'administration auquel la tâche est appliquée.

- **Historique des révisions**.

Exportation d'une tâche

Kaspersky Security Center permet d'enregistrer une tâche et ses paramètres dans un fichier KLT. Vous pouvez utiliser ce fichier KLT pour importer la tâche enregistrée dans Kaspersky Security Center Windows et Kaspersky Security Center Linux.

Pour exporter une tâche, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Tâches**.
2. Cochez la case en regard de la tâche que vous souhaitez exporter.

   Vous ne pouvez pas exporter plusieurs tâches à la fois. Si vous sélectionnez plusieurs tâches, le bouton **Exporter** sera désactivé. Les tâches du Serveur d'administration ne sont pas non plus disponibles à l'exportation.

3. Cliquez sur le bouton **Exporter**.

4. Dans la fenêtre ouverte **Enregistrer sous**, indiquez le nom du fichier et le chemin d'accès de la tâche. Cliquez sur **Enregistrer**.

   La fenêtre **Enregistrer sous** s'affiche uniquement si vous utilisez Google Chrome, Microsoft Edge ou Opera. Si vous utilisez un autre navigateur, le fichier de la tâche est automatiquement enregistré dans le dossier **Téléchargements**.

Importation d'une tâche

Kaspersky Security Center permet d'importer une tâche depuis un fichier KLT. Le fichier KLT contient la tâche exportée et ses paramètres.

Pour importer une tâche, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Tâches**.

2. Cliquez sur le bouton **Importer**.

3. Cliquez sur le bouton **Parcourir** pour choisir un fichier de tâche à importer.

4. Dans la fenêtre qui s'ouvre, indiquez le chemin d'accès au fichier de la tâche KLT, puis cliquez sur le bouton **Ouvrir**. Notez que vous ne pouvez sélectionner qu'un seul fichier de tâche.

   Le traitement de la tâche démarre.

5. Une fois que la tâche a été traitée avec succès, sélectionnez les appareils auxquels vous souhaitez affecter la tâche. Pour ce faire, sélectionnez une des options suivantes :

   - **Attribuer la tâche à un groupe d'administration**

     La tâche est affectée aux appareils qui appartiennent à un groupe d'administration. Vous pouvez renseigner un des groupes existants ou en créer un.

     Par exemple, vous pourriez souhaiter utiliser cette option pour exécuter une tâche d'envoi de messages pour les utilisateurs si le message est particulier pour les appareils repris dans un groupe d'administration spécifique.

     Si une tâche est attribuée à un groupe d'administration, l'onglet **Sécurité** ne s'affiche pas dans la fenêtre des propriétés de la tâche, car les tâches de groupe sont soumises aux paramètres de sécurité des groupes auxquels elles s'appliquent.

   - **Définir les adresses des appareils manuellement ou les importer à partir d'une liste**

     Vous pouvez définir les noms NetBIOS, les noms DNS, les adresses IP, ainsi que les plages d'adresses IP auxquels il convient d'affecter la tâche.

     Vous pourriez utiliser cette option pour exécuter une tâche pour un sous-réseau défini. Par exemple, vous pourriez souhaiter installer une certaine application sur les appareils des comptables ou analyser des appareils dans un sous-réseau qui est probablement infecté.

   - **Attribuer la tâche à une sélection d'appareils**

     La tâche est affectée aux appareils qui appartiennent à une sélection d'appareils. Vous pouvez définir une des sélections existantes.

     Par exemple, vous pourriez souhaiter utiliser cette option pour exécuter une tâche sur des appareils dotés d'une version du système d'exploitation spécifique.

6. Spécifiez la zone de la tâche.

7. Cliquez sur le bouton **Terminée** pour terminer l'importation de la tâche.

La notification avec les résultats de l'importation s'affiche. Si la tâche est importée avec succès, vous pouvez cliquer sur le lien **En savoir plus** pour afficher les propriétés de la tâche.

Après une importation réussie, la tâche s'affiche dans la liste des tâches. Les paramètres et la planification de la tâche sont également importés. La tâche sera lancée conformément à sa planification.

Si la tâche importée porte le même nom qu'une tâche existante, le nom de la tâche importée est suivi de l'index **(<numéro de séquence suivant>)**, par exemple : **(1)**, **(2)**.

Démarrage de l'Assistant de modification du mot de passe des tâches

Pour une tâche non locale, vous pouvez spécifier un compte sous lequel la tâche doit être exécutée. Vous pouvez spécifier le compte lors de la création de la tâche ou dans les propriétés d'une tâche existante. Si le compte spécifié est utilisé conformément aux instructions de sécurité de l'organisation, ces instructions peuvent nécessiter périodiquement le changement du mot de passe du compte. Lorsque le mot de passe du compte expire et que vous en définissez un nouveau, les tâches ne démarrent pas tant que vous n'avez pas spécifié le nouveau mot de passe valide dans les propriétés de la tâche.

L'Assistant de modification du mot de passe des tâches vous permet de remplacer automatiquement l'ancien mot de passe par le nouveau dans toutes les tâches dans lesquelles le compte est spécifié. Vous pouvez également modifier ce mot de passe manuellement dans les propriétés de chaque tâche.

Pour démarrer l'Assistant de modification du mot de passe des tâches :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Tâches**.
2. Cliquez sur **Administrer les informations d'identification des comptes pour les tâches de démarrage**.

Suivez les instructions de l'assistant.

Étape 1. Spécification des informations d'identification

Indiquez les nouvelles informations d'identification valides dans votre système (par exemple, dans Active Directory). Lorsque vous passez à l'étape suivante de l'assistant, Kaspersky Security Center vérifie si le nom de compte spécifié correspond au nom de compte dans les propriétés de chaque tâche non locale. Si les noms de compte correspondent, le mot de passe dans les propriétés de la tâche sera automatiquement remplacé par le nouveau.

Pour spécifier le nouveau compte, sélectionnez une option :

- **Utiliser le compte actuel**

  L'assistant utilise le nom du compte à partir duquel vous êtes actuellement connecté à Kaspersky Security Center Web Console. Spécifiez ensuite manuellement le mot de passe du compte dans le champ **Mot de passe actuel à utiliser dans les tâches**.

- **Définir un autre compte**

  Spécifiez le nom du compte à partir duquel les tâches doivent être lancées. Spécifiez ensuite le mot de passe du compte dans le champ **Mot de passe actuel à utiliser dans les tâches**.

Si vous remplissez le champ **Mot de passe précédent (facultatif ; pour le remplacer par l'actuel)**, Kaspersky Security Center remplace uniquement le mot de passe pour les tâches dans lesquelles se trouvent le nom de compte et l'ancien mot de passe. Le remplacement est effectué automatiquement. Dans tous les autres cas, vous devez choisir une action à entreprendre à l'étape suivante de l'assistant.

Étape 2. Sélection d'une action à entreprendre

Si vous n'avez pas indiqué le mot de passe précédent à la première étape de l'Assistant ou si l'ancien mot de passe indiqué ne correspond pas aux mots de passe dans les propriétés de la tâche, vous devez choisir une action à entreprendre pour les tâches trouvées.

Pour choisir une action pour une tâche :

1. Cochez la case en regard de la tâche pour laquelle vous souhaitez choisir une action.
2. Réalisez une des actions suivantes :
   - Pour supprimer le mot de passe dans les propriétés de la tâche, cliquez sur **Supprimer les identifiants**.

     La tâche est modifiée pour s'exécuter sous le compte par défaut.
   - Pour remplacer le mot de passe par un nouveau, cliquez sur **Forcer le changement de mot de passe même si l'ancien mot de passe est incorrect ou n'est pas fourni**.
   - Pour annuler la modification du mot de passe, cliquez sur **Aucune action n'est sélectionnée**.

Les actions choisies sont appliquées une fois que vous êtes passé à l'étape suivante de l'assistant.

Étape 3. Affichage des résultats

À la dernière étape de l'Assistant, consultez les résultats pour chacune des tâches trouvées. Cliquez sur **Terminer** pour terminer le travail de l'Assistant.

Création de la tâche Exécuter des scripts à distance

Vous pouvez créer une tâche *Exécuter des scripts à distance* pour exécuter un paquet d'installation sur un appareil client et pour installer une application à distance.

Un paquet d'installation contient une archive ZIP avec un ensemble de scripts à exécuter sur les appareils clients, ainsi qu'un fichier manifest.json. Apprenez-en plus à propos de la création de ce type de paquet d'installation dans cet article.

Cette tâche doit être démarrée uniquement sur les appareils dotés de l'Agent d'administration pour Linux.

Pour démarrer une tâche Exécuter des scripts à distance, procédez comme suit :

1. Accédez à l'**Assistant de création d'une tâche** et sélectionnez le type de tâche **Exécuter des scripts à distance**.
2. Saisissez le nom de la tâche et sélectionnez les appareils auxquels la tâche sera affectée. Cliquez sur le bouton **Suivant**.

3. Sélectionnez un paquet d'installation basé sur une archive ZIP avec un fichier manifest.json pour une exécution à distance.

   Si vous ne souhaitez pas ré-exécuter la tâche sur les appareils où elle est déjà terminée, activez l'option **Ne pas lancer cette tâche sur des appareils sur lesquels elle a déjà été effectuée**.

4. Sélectionnez un compte pour exécuter la tâche.

   Si vous sélectionnez le compte par défaut, la tâche sera exécutée par l'Agent d'administration (compte root).

   > Vous ne pouvez pas modifier le compte qui lui est attribué lorsque la tâche *Exécuter des scripts à distance* démarre. Pour modifier le compte utilisateur auquel la tâche est attribuée, il faut arrêter la tâche dans les paramètres de la tâche et la créer de nouveau avec les bons détails du compte.

5. Si vous souhaitez modifier les paramètres de la tâche par défaut, activez l'option **Ouvrir les détails de la tâche à la fin de la création** sur la page **Fin de la création de la tâche**. Si vous n'activez pas cette tâche, la tâche est créée selon les paramètres par défaut. Vous pourrez modifier ces paramètres par défaut à tout moment.

6. Cliquez sur le bouton **Terminer**.

   La tâche *Exécuter des scripts à distance* est créée et s'affiche dans la liste des tâches.

Après avoir reçu des données de la tâche *Exécuter des scripts à distance*, l'Agent d'administration restreint l'accès aux données reçues pour tous les utilisateurs, sauf pour l'administrateur et pour l'utilisateur spécifié dans les paramètres de la tâche.

Installation à distance d'applications sur les appareils à l'aide de la tâche Exécuter des scripts à distance

La tâche *Exécuter des scripts à distance* peut être utilisée pour installer à distance une application sur un appareil client en créant un paquet d'installation personnalisé.

Découvrez comment préparer une archive pour cette tâche dans cet article.

Pour créer le paquet d'installation en vue de l'installation à distance d'une application sur un appareil client, les fichiers suivants doivent figurer dans l'archive à charger pour cette tâche :

- <nom du paquet>.deb
- install.sh

  ```
  sudo apt-get install <nom du paquet>.deb
  ```

- manifest.json

Schéma JSON pour l'installation à distance d'une application

```
{
  "version": 1,
  "actions": [
    {
      "type": "execute",
      "path": "install.sh",
      "args": "<saisissez les arguments, si nécessaire>",
      "results": [
        {
          "code": 0,
          "next": "continue"
        }
      ],
      "default_next": "break"
    }
  ]
}
```

Description des tableaux

1. `version` : version du fichier manifeste et de la tâche.

   Pour le moment, la seule valeur acceptable est 1.

2. Les éléments du tableau `actions` déterminent la composition et l'ordre des scripts exécutés dans la tâche.

   L'ordre d'exécution du script correspond à l'index (place) de l'élément dans le tableau.

3. Pour chaque élément du tableau `actions`, les éléments suivants sont définis.

   a. `type` : type de la commande exécutable issue des scripts. Pour le moment, la valeur est toujours `execute`.

   b. `path` : chemin d'accès au fichier script dans l'archive.

   c. `args` : arguments transmis au script dans le cadre de l'exécution de la commande.

   d. `results` : tableau qui définit les actions supplémentaires en fonction du résultat de la tâche.

      1. `code` : valeur qui retourne un script.

      2. `next` : action à terminer ensuite. L'action `continue` passe à l'exécution du script suivant (élément du tableau `actions`) ; l'action `break` arrête la tâche.

   e. `default_next` : action si le script renvoie une valeur non contenue dans les `results`.

Au démarrage de la tâche *Exécuter des scripts à distance*, l'Agent d'administration charge le paquet d'installation avec l'application sur l'appareil client. Lorsque l'appareil client reçoit le paquet d'installation, l'Agent d'administration sur cet appareil analyse le fichier manifest.json et définit l'ordre d'exécution des scripts et des actions en fonction du résultat, puis démarre l'exécution.

Lorsque la tâche *Exécuter des scripts à distance* est terminée, l'application est installée sur l'appareil client.

Configuration des notifications et de la surveillance de la tâche Exécuter des scripts à distance

Vous pouvez configurer la surveillance, le comportement d'enregistrement des événements et les notifications pour la tâche *Exécuter des scripts à distance*.

Pour consulter l'état de la tâche Exécuter des scripts à distance, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Tâches**.
   La liste des tâches s'affiche.
2. Sélectionnez la tâche et cliquez sur **Historique de l'appareil**.
   La progression de la tâche s'affiche.

Pour configurer le comportement d'enregistrement des événements, procédez comme suit :

1. Dans la liste des tâches, cliquez sur la tâche et accédez à l'onglet **Paramètres**.
2. Dans la section **Notifications**, cliquez sur le bouton **Paramètres**.
3. Choisissez une des options suivantes en fonction du comportement de l'application à l'issue de la tâche :
   - **Sauvegarder tous les événements**.
   - **Sauvegarder les événements relatifs à la progression de la tâche**.
   - **Sauvegarder uniquement le résultat de la tâche**.
     Les événements sont enregistrés dans l'**Historique de l'appareil** et le **Stockage d'événements**.
     Par défaut, seuls les résultats d'exécution de la tâche sont enregistrés.

     > Si vous sélectionnez **Sauvegarder tous les événements**, seuls les résultats d'exécution de la tâche seront enregistrés.
4. Si vous souhaitez conserver les événements dans la base de données du Serveur d'administration, dans le journal des événements sur le Serveur d'administration ou sur l'appareil, activez l'option correspondante.

Apprenez-en plus à propos de la configuration des notifications dans cet article.

Préparation d'une archive pour la tâche Exécuter des scripts à distance

L'archive pour la tâche *Exécuter des scripts à distance* basée sur un fichier manifest.json doit remplir les conditions suivantes :

- Format d'archive : ZIP.
- Taille totale : pas plus de 1 Go.
- Le nombre de fichiers et de dossiers dans l'archive est illimité.

- Le fichier manifeste de l'archive doit correspondre au schéma ci-dessous et être nommé manifest.json. Le schéma est validé uniquement lors de l'exécution de la tâche sur l'appareil.

  Schéma JSON du fichier manifeste et description des tableaux

Schéma JSON

```
{
 "$schema": "http://json-schema.org/draft-07/schema#",
  "title": "Schema for execute scripts task",
   "type": "object",
    "properties": {
        "version": {
            "type": "integer",
            "enum": [1]
        },
        "actions":{
            "type": "array",
            "items": {
                "type": "object",
                "properties": {
                    "type": {
                        "type": "string",
                        "enum": ["execute"]
                    },
                    "path": {
                        "type": "string"
                    },
                    "args": {
                        "type": "string"
                    },
                    "results":{
                        "type": "array",
                        "items": {
                            "type": "object",
                            "properties": {
                                "code": {
                                    "type": "integer",
                                    "minimum": -255,
                                    "maximum": 255
                                },
                                "next":{
                                    "type": "string",
                                    "enum": ["break", "continue"]
                                }
                            },
                            "required": [
                                "code",
                                "next"
                            ]
                        }
                    },
                    "default_next":{
                        "type": "string",
                        "enum": ["break", "continue"]
                    }
                },
                "required": [
                    "type",
                    "path",
```

```
                    "default_next"
                ]
            }
        }
    },
    "required": [
        "version",
        "actions"
    ]
}
```

Exemple de fichier manifeste

```
{
  "version": 1,
  "actions": [
    {
      "type": "execute",
      "path": "scripts/run1.cmd",
      "args": "testArg",
      "results": [
        {
          "code": 0,
          "next": "continue"
        }
      ],
      "default_next": "break"
    },
    {
      "type": "execute",
      "path": "scripts/run2.cmd",
      "results": [
        {
          "code": 0,
          "next": "continue"
        }
      ],
      "default_next": "break"
    },
    {
      "type": "execute",
      "path": "scripts/run3.cmd",
      "results": [
        {
          "code": 0,
          "next": "continue"
        }
      ],
      "default_next": "break"
    }
  ]
}
```

- L'archive doit être structurée comme suit :

  `manifest.json`

  `<file1>`

<file2>

<folder1>/<file3>

<folder2>/<folder3>/<file4>

...

<fileX>

manifest.json est le fichier manifeste de la tâche.

<file1>, ..., <fileX> est l'ensemble de fichiers avec les scripts à exécuter.

Création d'un paquet d'installation sur la base d'un fichier manifeste

Pour créer un paquet d'installation sur la base d'un fichier manifeste, procédez comme suit :

1. Exécutez une des actions suivantes :

   - Dans le menu principal, accédez à **Découverte et déploiement** → **Déploiement et attribution** → **Paquets d'installation**.
   - Dans le menu principal, accédez à **Opérations** → **Stockages** → **Paquets d'installation**.

   Une liste des paquets d'installation disponibles sur le Serveur d'administration s'affiche.

2. Cliquez sur **Ajouter**.

   L'Assistant de création du paquet d'installation se lance. Parcourez les étapes de l'assistant à l'aide du bouton **Suivant**.

3. Sélectionnez **Créer un paquet d'installation pour la tâche Exécuter des scripts à distance à partir d'une archive ZIP avec un fichier manifest.json**.

4. Définissez le nom du paquet et cliquez sur le bouton **Parcourir**.

   Une fenêtre Windows **Ouvrir** standard s'ouvre dans votre navigateur pour vous permettre de choisir un fichier pour créer le paquet d'installation.

5. Sélectionnez un fichier d'archive situé sur les disques disponibles. Découvrez comment préparer une archive pour cette tâche dans cet article.

   Le chargement du fichier sur le Serveur d'administration Kaspersky Security Center commence.

   Le processus de création du paquet d'installation se lance.

   L'Assistant vous informe lorsque le processus est terminé.

   Si le paquet d'installation n'est pas créé, un message approprié s'affiche.

6. Cliquez sur le bouton **Terminer** pour fermer l'Assistant.

Le paquet d'installation que vous avez créé est téléchargé dans le sous-dossier Paquets du dossier partagé du Serveur d'administration. Après le téléchargement, le paquet d'installation apparaît dans la liste des paquets d'installation.

Dans la liste des paquets d'installation d'un Serveur d'administration, vous pouvez cliquer sur le lien portant le nom d'un paquet d'installation personnalisé pour :

- Afficher les propriétés suivantes d'un paquet d'installation :
  - **Nom.** Nom du paquet d'installation personnalisé.
  - **Source.** Nom du fournisseur de l'application.
  - **Version.** Version de l'application.
  - **Date de création.** Date de création du paquet d'installation.
  - **Date de modification.** Date de modification du paquet d'installation.
  - **Chemin.** Chemin d'accès au paquet d'installation personnalisé sur le Serveur d'administration.
- Modifiez le nom de l'archive et les paramètres de ligne de commande. Cette fonctionnalité n'est disponible que pour les paquets qui ne sont pas créés sur la base des applications Kaspersky.

Administration des appareils clients

Kaspersky Security Center permet de gérer les appareils clients :

- Afficher les paramètres et les états des appareils administrés, y compris les clusters et les groupes de serveurs.
- Configurer les points de distribution.
- Gérer les tâches.

Grâce aux groupes d'administration, les appareils clients peuvent former un ensemble administrable comme une seule unité. Un appareil client ne peut être inclus que dans un seul groupe d'administration. Les appareils peuvent être alloués automatiquement à un groupe en fonction des **Conditions de la règle** :

- Création des règles de déplacement des appareils.
- Copie des règles de déplacement des appareils.
- Conditions d'une règle de déplacement de l'appareil.

Vous pouvez utiliser les sélections d'appareils pour filtrer les appareils en fonction d'une condition. Vous pouvez également taguer les appareils pour créer des sélections, rechercher des appareils et répartir les appareils dans les groupes d'administration.

Paramètres de l'appareil administré

Pour voir les paramètres de l'appareil administré :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Appareils administrés**.
   La liste des appareils administrés s'affiche.
2. Cliquez sur le lien avec le nom de l'appareil requis dans la liste des appareils administrés.

La fenêtre des propriétés de l'appareil sélectionné s'affiche.

Les onglets suivants s'affichent dans la partie supérieure de la fenêtre des propriétés et représentent les principaux groupes de paramètres :

- Général

Cet onglet comprend les sections suivantes :

- La section **Général** contient les informations générales sur l'appareil client. La boîte de dialogue affiche des informations mises à jour lors de la dernière synchronisation de l'appareil client avec le Serveur d'administration :

  - Nom

    Champ à consulter et à modifier le nom de l'appareil client dans le groupe d'administration.

  - Description

    Champ de saisie d'une description complémentaire de l'appareil client.

  - État de l'appareil

    État de l'appareil client formé d'après les critères d'état de la protection antivirus et de l'activité réseau de l'appareil, tels que déterminés par l'administrateur.

  - Nom complet du groupe

    Groupe d'administration contenant l'appareil client.

  - Dernière mise à jour des bases antivirus

    Date de la dernière mise à jour des bases de données antivirus ou des applications sur l'appareil.

  - Connexion au Serveur d'administration

    Date et heure de la dernière connexion de l'Agent d'administration installé sur l'appareil client au Serveur d'administration.

  - Heure de la dernière connexion

    Date et heure où l'appareil a été visible sur le réseau pour la dernière fois.

  - Version de l'Agent d'administration

    Version de l'Agent d'administration installé.

  - Date de création

    Date de création de l'appareil au sein de Kaspersky Security Center.

  - Propriétaire de l'appareil

Nom du propriétaire de l'appareil. Vous pouvez désigner ou supprimer un utilisateur en tant que propriétaire de l'appareil en cliquant sur le lien **Administrer le propriétaire de l'appareil**.

- **Maintenir la connexion au Serveur &d'administration**

  Si cette option est activée, la connectivité continue entre l'appareil administré et le Serveur d'administration est conservée. Vous pouvez utiliser cette option si vous n'utilisez pas des serveurs push, qui fournissent une telle connectivité.

  Si cette option est désactivée et les serveurs push ne sont pas utilisés, l'appareil administré se connecte uniquement au Serveur d'administration pour synchroniser les données ou transmettre des informations.

  Le total des appareils pour lesquels l'option **Maintenir la connexion au Serveur &d'administration** a été sélectionnée ne peut être supérieur à 300.

  Cette option est désactivée par défaut sur les appareils administrés. Cette option est activée par défaut sur l'appareil sur lequel le Serveur d'administration est installé et reste activée même si vous essayez de la désactiver.

- La section **Réseau** affiche les informations suivantes sur les propriétés réseau de l'appareil client :
  - **Adresse IP**

    Adresse IP de l'appareil.

  - **Domaine Windows**

    Domaine Windows ou groupe de travail auquel appartient l'appareil.

  - **Nom DNS**

    Nom du domaine DNS de l'appareil client.

  - **Nom NetBIOS**

    Nom de l'appareil client sur le réseau Windows.

  - **Adresse IPv6**

- La section **Système** reprend les informations relatives au système d'exploitation sur l'appareil client :
  - **Système d'exploitation**
  - **Architecture CPU**
  - **Nom de l'appareil**
  - **Type de machine virtuelle**

    Le fabricant de la machine virtuelle.

- **Machine virtuelle dynamique dans le cadre de VDI**

  Cette ligne indique si l'appareil client est une machine virtuelle dynamique dans le cadre de VDI.

- La section **Protection** affiche des informations relatives à l'état actuel de la protection antivirus sur l'appareil client :

  - **Visible**

    État de visibilité de l'appareil client.

  - **État de l'appareil**

    État de l'appareil client formé d'après les critères d'état de la protection antivirus et de l'activité réseau de l'appareil, tels que déterminés par l'administrateur.

  - **Description de l'état**

    État de la protection de l'appareil client et de la connexion au Serveur d'administration.

  - **État de la protection**

    État actuel de la protection en temps réel de l'appareil client.

    Quand l'état change sur l'appareil, le nouvel état est affiché dans la fenêtre des propriétés des appareils uniquement après la synchronisation de l'appareil client avec le Serveur d'administration.

  - **Dernière analyse complète**

    Date et heure de la dernière recherche de logiciels malveillants sur l'appareil client.

  - **Virus détecté**

    Nombre total de menaces détectées sur l'appareil client depuis l'installation de l'application de sécurité (première analyse de l'appareil) ou depuis la dernière remise à zéro du compteur.

  - **Objets dont la désinfection a échoué**

    Nombre de fichiers non traités sur l'appareil client.

    Ce champ ne tient pas compte du nombre de fichiers non traités pour les appareils mobiles.

  - **État de chiffrement des disques**

    État actuel de chiffrement des fichiers sur les disques locaux de l'appareil. Pour obtenir une description des états, consultez l'aide de Kaspersky Endpoint Security for Windows.

- La section **État de l'appareil défini par l'application** fournit des informations sur l'état de l'appareil défini par l'application administrée installée sur l'appareil. Cet état de l'appareil peut différer de celui défini par Kaspersky Security Center.

- Applications

  Cet onglet dresse la liste de toutes les applications de Kaspersky installées sur l'appareil client. Cet onglet contient les boutons **Démarrer** et **Arrêter** qui permettent de lancer et d'arrêter l'application Kaspersky sélectionnée (à l'exception de l'Agent d'administration). Vous pouvez utiliser ces boutons si le port 15000 UDP est disponible sur l'appareil géré pour recevoir des notifications push du Serveur d'administration. Si l'appareil géré ne peut pas recevoir de notifications push, mais que le mode de connexion permanente au Serveur d'administration est activé (l'option **Maintenir la connexion au Serveur &d'administration** est activée dans la section **Général**), les boutons **Démarrer** et **Arrêter** sont également disponibles. Dans le cas contraire, lorsque vous essayez de démarrer ou d'arrêter l'application, un message d'erreur s'affiche. Vous pouvez également cliquer sur le nom de l'application pour afficher des informations générales sur l'application, une liste des événements qui se sont produits sur l'appareil et les paramètres de l'application.

- Stratégies actives et profils de stratégies

  Cet onglet répertorie les stratégies et les profils de stratégie actuellement attribués à l'appareil administré.

- Tâches

  L'onglet **Tâches** permet d'administrer les tâches de l'appareil client : consulter la liste des tâches existantes, créer des tâches, supprimer, lancer ou suspendre des tâches, modifier leurs paramètres et consulter les résultats de l'exécution. La liste des tâches est fournie sur la base des données réceptionnées pendant la dernière session de synchronisation client avec le serveur d'administration. Le Serveur d'administration questionne l'appareil client au sujet de l'état courant de tâche. Si le port 15000 UDP est disponible sur l'appareil administré pour recevoir les notifications push en provenance du Serveur d'administration, l'état de la tâche est affiché et les boutons d'administration de la tâche sont activés. Si l'appareil géré ne peut pas recevoir de notifications push, mais que le mode de connexion permanente au Serveur d'administration est activé (l'option **Maintenir la connexion au Serveur &d'administration** est activée dans la section **Général**), les actions avec les tâches sont également disponibles.

  Si la connexion n'est pas établie, l'état n'est pas affiché et les boutons sont désactivés.

- Événements

  L'onglet **Événements** affiche les événements enregistrés sur le Serveur d'administration pour l'appareil client sélectionné.

- Problèmes de sécurité

  L'onglet **Problèmes de sécurité** permet de consulter, de modifier et de créer des problèmes de sécurité pour l'appareil client. Les problèmes de sécurité peuvent être créés automatiquement, à l'aide des applications administrées de Kaspersky installées sur l'appareil client, ou manuellement par l'administrateur. Ainsi, si un utilisateur transfère toujours des applications malveillantes de son disque amovible personnel vers d'autres appareils, l'administrateur peut créer un problème de sécurité. L'administrateur peut fournir une brève description du cas et recommandés des actions, (comme des mesures disciplinaires à adopter contre un utilisateur) dans le texte du problème de sécurité et il peut ajouter un lien vers le ou les utilisateurs.

  Un problème de sécurité pour lequel les actions nécessaires ont été exécutées est un problème *traité*. La présence de problèmes de sécurité non traités peut être sélectionnée comme condition pour faire passer l'état de l'appareil à *Critique* ou *Avertissement*.

  La section contient la liste des problèmes de sécurité créés pour l'appareil. Les problèmes de sécurité sont classés par niveau de gravité et par type. C'est l'application Kaspersky qui crée le problème de sécurité qui en définit le type. Les problèmes de sécurité traités peuvent être identifiés dans la liste en cochant la case de la colonne **Traité**.

- Tags

  L'onglet **Tags** permet d'administrer la liste des mots-clés utilisés pour effectuer la recherche d'appareils clients : consulter la liste des tags existants, désigner les tags de la liste, configurer des règles de désignation automatique des tags, ajouter de nouveaux tags, renommer d'anciens tags et supprimer des tags.

- Avancé

Cet onglet comprend les sections suivantes :

- **Registre des applications**. Cette section permet de consulter le registre des applications installées sur l'appareil client, ainsi que leurs mises à jour, et de configurer l'affichage du registre des applications.

  Les informations relatives aux applications installées sont présentées si l'Agent d'administration installé sur l'appareil client transmet les informations nécessaires au Serveur d'administration. Les paramètres de transfert des informations sur le Serveur d'administration peuvent être configurés dans la fenêtre des propriétés de l'Agent d'administration ou de sa stratégie, dans la section **Stockages**.

  Cliquez sur le nom d'une application pour ouvrir une fenêtre contenant les détails de l'application ainsi qu'une liste des paquets de mise à jour installés pour l'application.

- **Fichiers exécutables**. Cette section affiche les fichiers exécutables trouvés sur la machine cliente.

- **Points de distribution**. Cette section présente la liste des points de distribution avec lesquels l'appareil interagit.

  - Exporter dans un fichier

    Le bouton **Exporter dans un fichier** vous permet d'enregistrer dans le fichier la liste des points de distribution avec lesquels l'appareil interagit. Par défaut, l'application exporte la liste des appareils dans un fichier au format CSV.

  - Propriétés

    Le bouton **Propriétés** vous permet de consulter et de configurer les paramètres du point de distribution avec lequel l'appareil interagit.

- **Registre du matériel**. Cette section permet de consulter les informations sur le matériel installé sur l'appareil client.

  Si l'Agent d'administration est installé sur un appareil exécutant Windows, il envoie au Serveur d'administration les informations suivantes sur le matériel de l'appareil :

  - Mémoire vive
  - Appareils de stockage de masse
  - Carte mère
  - Processeur
  - Adaptateurs réseau
  - Surveillance
  - Adaptateur vidéo
  - Carte son

  Si l'Agent d'administration est installé sur un appareil exécutant Linux ou macOS, il envoie au Serveur d'administration les informations suivantes sur le matériel de l'appareil, si ces informations sont fournies par le système d'exploitation :

- Volume total de mémoire vive
- Volume total des appareils de stockage de masse
- Carte mère
- Processeur
- Adaptateurs réseau

- **Mises à jour disponibles**. Cette section permet de consulter la liste des mises à jour du logiciel, non installées détectées sur l'appareil.

- **Vulnérabilités dans les applications**. Cette section permet de consulter les informations relatives aux vulnérabilités d'applications tierces installées sur les appareils clients.

  Pour enregistrer les vulnérabilités dans un fichier, cochez les cases en regard des vulnérabilités que vous souhaitez enregistrer, puis cliquez sur le bouton **Exporter vers un fichier CSV** ou sur le bouton **Exporter vers un fichier TXT**.

  Cette section contient les paramètres suivants :

  - **Afficher uniquement les vulnérabilités qui peuvent être corrigées**

    Si l'option est activée, la section reprend les vulnérabilités qui peuvent être éliminées par un correctif.

    Si l'option est désactivée, la section reprend les vulnérabilités qui peuvent être éliminées par un correctif et celles pour lesquelles il n'existe pas de correctifs.

    Cette option est activée par défaut.

  - **Propriétés de la vulnérabilité**

    Cliquez sur une vulnérabilité logicielle dans la liste pour afficher les propriétés de la vulnérabilité logicielle sélectionnée dans une fenêtre distincte. Dans la fenêtre, vous pouvez effectuer l'une des opérations suivantes :

    - Ignorer la vulnérabilité logicielle sur cet appareil administré (dans la Console d'administration ou dans la Kaspersky Security Center Web Console).
    - Afficher la liste des correctifs recommandés pour la vulnérabilité.
    - Spécifier manuellement les mises à jour logicielles permettant de corriger la vulnérabilité (dans la Console d'administration ou dans la Kaspersky Security Center Web Console).
    - Afficher les instances de vulnérabilité.
    - Afficher la liste des tâches existantes pour corriger la vulnérabilité et créer de nouvelles tâches pour corriger la vulnérabilité.

- **Diagnostic à distance**. Cette section permet d'effectuer un diagnostic à distance des appareils clients.

Si vous utilisez un SGBD PostgreSQL, MariaDB ou MySQL, l'onglet **Événements** peut afficher une liste incomplète des événements pour l'appareil client sélectionné. Cette situation se produit lorsque le SGBD stocke un très grand nombre d'événements. Vous pouvez augmenter le nombre d'événements affichés d'une des manières suivantes :

- Suppression des événements inutiles.
- Réduction de la durée de conservation des événements inutiles.

Pour consulter la liste complète des événements enregistrés sur le Serveur d'administration pour l'appareil, accédez à Rapports.

Création des groupes d'administration

Immédiatement après l'installation de Kaspersky Security Center, la hiérarchie des groupes d'administration ne contient qu'un seul groupe d'administration, appelé **Appareils administrés**. Lors de la création d'une hiérarchie de groupes d'administration, vous pouvez ajouter des appareils, y compris des machines virtuelles, au groupe **Appareils administrés**, ainsi que des groupes imbriqués (cf. ill. ci-après).

Consultation des hiérarchies des groupes d'administration

Pour créer un groupe d'administration, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Hiérarchie des groupes**.
2. Dans la structure du groupe d'administration, sélectionnez le groupe d'administration qui doit inclure le nouveau groupe d'administration.
3. Cliquez sur le bouton **Ajouter**.
4. Dans la fenêtre **Nom du nouveau groupe d'administration** qui s'ouvre, saisissez le nom du groupe et cliquez sur le bouton **Ajouter**.

   Un nouveau groupe d'administration portant le nom spécifié apparaît dans la hiérarchie des groupes d'administration.

L'application permet de créer une structure de groupes d'administration sur la base de la structure d'Active Directory ou de la structure du réseau de domaine. Vous pouvez aussi créer une structure de groupes du fichier texte.

Pour créer une structure de groupes d'administration, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Hiérarchie des groupes**.
2. Cliquez sur le bouton **Importer**.

   Finalement, l'assistant de création de la structure des groupes d'administration se lance. Suivez les instructions de l'assistant.

Ajout manuel d'appareils à un groupe d'administration

Vous pouvez déplacer des appareils vers des groupes d'administration automatiquement en créant des règles de déplacement d'appareils ou manuellement en déplaçant des appareils d'un groupe d'administration vers un autre ou en ajoutant des appareils à un groupe d'administration sélectionné. Cette section décrit comment ajouter manuellement des appareils à un groupe d'administration.

Pour ajouter manuellement un ou plusieurs appareils à un groupe d'administration sélectionné, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Appareils administrés**.
2. Cliquez sur le lien **Chemin d'accès actuel :** `<current path>` au-dessus de la liste.
3. Dans la fenêtre qui s'ouvre, sélectionnez le groupe d'administration auquel vous souhaitez ajouter les appareils.
4. Cliquez sur le bouton **Ajouter des appareils**.

   L'Assistant de déplacement des appareils est ensuite démarré.
5. Dressez une liste des appareils que vous souhaitez ajouter au groupe d'administration.

   > Il est possible d'ajouter uniquement les appareils dont les informations ont été insérées dans la base de données du Serveur d'administration lors de la connexion de l'appareil ou après la recherche d'appareils.

   Sélectionnez la façon dont vous souhaitez ajouter des appareils à la liste :

   - Cliquez sur le bouton **Ajouter des appareils**, puis indiquez les appareils d'une des manières suivantes :
     - Sélectionnez les appareils dans la liste des appareils détectés par le Serveur d'administration.
     - Indiquez une adresse IP ou une plage IP de l'appareil.
     - Indiquez le nom NetBIOS ou le nom DNS d'un appareil.

       > Le champ du nom de l'appareil ne doit pas contenir d'espaces, ni les caractères interdits suivants : \ / * ; : ` ~ ! @ # $ ^ & ( ) = + [ ] { } | , < > %
   - Cliquez sur le bouton **Importer des appareils à partir d'un fichier** pour importer une liste d'appareils à partir d'un fichier .txt. Chaque adresse ou nom d'appareil doit figurer sur une ligne séparée.

     > Le fichier ne doit pas contenir d'espaces, ni les caractères interdits suivants : \ / * ; : ` ~ ! @ # $ ^ & ( ) = + [ ] { } | , < > %
6. Affichez la liste des appareils à ajouter au groupe d'administration. Vous pouvez modifier la liste en ajoutant ou en supprimant des appareils.
7. Une fois que vous vous assurez que la liste est correcte, cliquez sur le bouton **Suivant**.

L'Assistant traite la liste des appareils et affiche le résultat. Les appareils traités correctement sont inclus dans les groupes d'administration et s'affichent dans la liste des appareils sous les noms établis pour eux par le Serveur d'administration.

Déplacement manuel des appareils ou des clusters à un groupe d'administration

Vous pouvez déplacer des appareils d'un groupe d'administration vers un autre ou du groupe d'appareils non définis vers un groupe d'administration.

Vous pouvez également déplacer d'un cluster ou d'un groupe de serveurs d'un groupe d'administration à un autre. Lorsque vous déplacez un cluster ou un groupe de serveurs vers un autre groupe, tous ses nœuds se déplacent avec lui, car un cluster et l'un de ses nœuds appartiennent toujours au même groupe d'administration. Lorsque vous sélectionnez un seul nœud de cluster sous l'onglet **Appareils**, le bouton **Déplacer vers le groupe** devient indisponible.

Pour déplacer un ou plusieurs appareils ou clusters dans un groupe d'administration sélectionné, procédez comme suit :

1. Ouvrez le groupe d'administration à partir duquel vous souhaitez déplacer les appareils. Pour ce faire, réalisez une des opérations suivantes :

   - Pour ouvrir un groupe d'administration, dans le menu principal, accédez à **Ressources (Appareils)** → **Appareils administrés**, cliquez sur le lien du chemin dans le champ **Chemin d'accès actif** et sélectionnez un groupe d'administration dans le volet gauche qui s'ouvre.

   - Pour ouvrir le groupe **Appareils non définis**, dans le menu principale, accédez à **Découverte et déploiement** → **Appareils non définis**.

2. Si le groupe d'administration contient des clusters ou des groupes de serveurs, la section **Appareils administrés** est divisée en deux onglets : l'onglet **Appareils** et l'onglet **Clusters et matrices de serveurs**. Ouvrez l'onglet de l'objet que vous souhaitez déplacer.

3. Cochez les cases en regard des appareils ou des clusters que vous souhaitez déplacer vers un autre groupe.

4. Cliquez sur le bouton **Déplacer vers le groupe**.

5. Dans la hiérarchie des groupes d'administration, cochez la case située à côté du groupe d'administration vers lequel vous souhaitez déplacer les appareils ou les clusters sélectionnés.

6. Cliquez sur le bouton **Déplacer**.

Les appareils ou les clusters sélectionnés sont déplacés vers le groupe d'administration sélectionné.

Création des règles de déplacement des appareils

Vous pouvez configurer les règles de déplacement des appareils qui attribuent automatiquement des appareils à des groupes d'administration.

Pour créer une règle de déplacement, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Règles de déplacement**.
2. Cliquez sur **Ajouter**.
3. Dans la fenêtre qui s'ouvre, précisez les informations suivantes sous l'onglet **Général** :

- Nom de la règle

  Saisissez un nom pour la nouvelle règle.

  Si vous copiez une règle, la nouvelle règle obtient le même nom que la règle de source, mais un index au format () est ajouté au nom, par exemple : (1).

- Groupe d'administration

  Sélectionnez le groupe d'administration dans lequel les appareils seront déplacés automatiquement.

- Règle active

  Si cette option est activée, la règle est activée et commence à s'applique après avoir été enregistrée.

  Si cette option est désactivée, la règle est créée mais pas activée. Elle ne fonctionnera pas jusqu'à ce que vous activiez cette option.

- Déplacer uniquement les appareils non inclus dans un groupe d'administration

  Si cette option est activée, seuls les appareils non définis sont déplacés dans le groupe sélectionné.

  Si cette option est désactivée, les appareils qui appartiennent déjà à d'autres groupes d'administration ainsi que les appareils non définis seront déplacés dans le groupe sélectionné.

- Exécution de la règle

  Vous avez le choix parmi les options suivantes :

  - **Exécuter une fois pour chaque appareil**

    La règle est appliquée une fois pour chaque appareil qui correspond à vos critères.

  - **Exécuter une fois pour chaque appareil, ensuite chaque fois après la réinstallation de l'Agent d'administration**

    La règle est appliquée une fois pour chaque appareil qui corresponde à vos critères, puis uniquement lorsque l'Agent d'administration est réinstallé sur ces appareils.

  - **Appliquer la règle en continu**

    La règle est appliquée selon la programmation que le Serveur d'administration définit automatiquement (généralement à intervalles réguliers de plusieurs heures).

4. Sous l'onglet **Conditions de la règle**, indiquez au moins un critère selon lequel les appareils sont déplacés vers un groupe d'administration.

5. Cliquez sur le bouton **Enregistrer**.

La règle de déplacement est créée. Elle s'affiche dans la liste des règles de déplacement.

Plus la position est élevée dans la liste, plus la priorité de la règle est élevée. Pour augmenter ou diminuer la priorité d'une règle en mouvement, déplacez la règle vers le haut ou vers le bas dans la liste, respectivement, à l'aide de la souris.

> Si l'option **Appliquer la règle en continu** est sélectionnée, la règle de déplacement est appliquée quels que soient les paramètres de priorité. Ces règles sont appliquées selon la planification que le Serveur d'administration configure automatiquement.

Si les attributs de l'appareil satisfont directement à plusieurs règles, l'appareil est placé dans le groupe cible de la règle qui affiche la priorité la plus élevée (la règle qui figure plus haut dans la liste).

Copie des règles de déplacement des appareils

Vous pouvez copier les règles de déplacement par exemple si vous souhaitez avoir plusieurs règles identiques pour différents groupes d'administration cibles.

Pour copier une règle de déplacement existante, procédez comme suit :

1. Exécutez une des actions suivantes :

   - Dans le menu principal, accédez à **Ressources (Appareils)** → **Règles de déplacement**.
   - Dans le menu principal, accédez à **Découverte et déploiement** → **Déploiement et attribution** → **Règles de déplacement**.

   La liste des règles de déplacement s'affiche.

2. Cochez la case en regard de la règle que vous souhaitez copier.

3. Cliquez sur **Copier**.

4. Dans la fenêtre qui s'ouvre, modifiez les informations suivantes sous l'onglet **Général** ou ne changez rien si vous souhaitez uniquement copier la règle sans modifier ses paramètres :

   - **Nom de la règle**

     Saisissez un nom pour la nouvelle règle.

     Si vous copiez une règle, la nouvelle règle obtient le même nom que la règle de source, mais un index au format () est ajouté au nom, par exemple : (1).

   - **Groupe d'administration**

     Sélectionnez le groupe d'administration dans lequel les appareils seront déplacés automatiquement.

   - **Règle active**

     Si cette option est activée, la règle est activée et commence à s'applique après avoir été enregistrée.

     Si cette option est désactivée, la règle est créée mais pas activée. Elle ne fonctionnera pas jusqu'à ce que vous activiez cette option.

   - **Déplacer uniquement les appareils non inclus dans un groupe d'administration**

     Si cette option est activée, seuls les appareils non définis sont déplacés dans le groupe sélectionné.

     Si cette option est désactivée, les appareils qui appartiennent déjà à d'autres groupes d'administration ainsi que les appareils non définis seront déplacés dans le groupe sélectionné.

   - **Exécution de la règle**

     Vous avez le choix parmi les options suivantes :

     - **Exécuter une fois pour chaque appareil**

       La règle est appliquée une fois pour chaque appareil qui correspond à vos critères.

     - **Exécuter une fois pour chaque appareil, ensuite chaque fois après la réinstallation de l'Agent d'administration**

       La règle est appliquée une fois pour chaque appareil qui corresponde à vos critères, puis uniquement lorsque l'Agent d'administration est réinstallé sur ces appareils.

     - **Appliquer la règle en continu**

       La règle est appliquée selon la programmation que le Serveur d'administration définit automatiquement (généralement à intervalles réguliers de plusieurs heures).

5. Sous l'onglet **Conditions de la règle**, indiquez au moins un critère pour les appareils que vous souhaitez déplacer automatiquement.

6. Cliquez sur le bouton **Enregistrer**.

La nouvelle règle de déplacement est créée. Elle s'affiche dans la liste des règles de déplacement.

Conditions d'une règle de déplacement de l'appareil

Lorsque vous créez ou copiez une règle pour déplacer les appareils clients vers des groupes d'administration, sous l'onglet **Conditions de la règle**, vous définissez les conditions de déplacement des appareils. Pour déterminer les appareils à déplacer, vous pouvez utiliser les critères suivants :

- Tags attribués aux appareils clients.
- Paramètres réseau. Par exemple, vous pouvez déplacer des appareils avec des adresses IP à partir d'une plage spécifiée.
- Les applications administrées installées sur les appareils clients, par exemple, l'Agent d'administration ou le Serveur d'administration.
- Les machines virtuelles, qui sont les appareils clients.
- Informations sur l'unité d'organisation (OU) Active Directory avec les appareils clients.
- Informations sur un segment dans le Cloud avec les appareils clients.

Vous trouverez ci-dessous la description de la manière de spécifier ces informations dans une règle de déplacement des appareils.

Si vous spécifiez plusieurs conditions dans la règle, l'opérateur logique ET fonctionne et toutes les conditions s'appliquent en même temps. Si vous ne sélectionnez aucune option ou si vous laissez certains champs vides, ces conditions ne s'appliquent pas.

Onglet Tags

Sur cet onglet, vous pouvez configurer une règle de déplacement de l'appareil basée sur les tags de l'appareil qui ont été précédemment ajoutés aux descriptions des appareils clients. Pour ce faire, sélectionnez les balises requises. Vous pouvez également activer les options suivantes :

- **Appliquer aux appareils sans les tags sélectionnés**

  Si cette option est activée, tous les appareils avec les tags indiqués sont exclus de la règle de déplacement des appareils. Si cette option est désactivée, la règle de déplacement des appareils s'applique aux appareils avec tous les tags sélectionnés.

  Cette option est Inactif par défaut.

- **Appliquer si au moins un tag sélectionné coïncide**

  Si cette option est activée, une règle de déplacement des appareils s'applique aux appareils clients avec au moins une des balises sélectionnées. Si cette option est désactivée, la règle de déplacement des appareils s'applique aux appareils avec tous les tags sélectionnés.

  Cette option est Inactif par défaut.

Onglet Réseau

Sous cet onglet, vous pouvez spécifier les données réseau des appareils pris en compte par une règle de déplacement des appareils :

- **Nom de l'appareil sur le réseau Windows**

  Nom de réseau Windows (nom NetBIOS) de l'appareil ou adresse IPv4 ou IPv6.

- **Domaine Windows**

  Une règle de déplacement des appareils s'applique à tous les appareils inclus dans le domaine Windows indiqué.

- **Nom du DNS de l'appareil**

  Nom de domaine DNS de l'appareil client que vous souhaitez déplacer. Remplissez ce champ si votre réseau comprend un serveur DNS.

  Si le classement sensible à la casse est défini pour la base de données que vous utilisez pour Kaspersky Security Center, respectez la casse lorsque vous indiquez le nom DNS de l'appareil. Sinon, la règle de déplacement de l'appareil ne fonctionnera pas.

- **Domaine DNS**

  Une règle de déplacement des appareils s'applique à tous les appareils inclus dans le suffixe DNS principal indiqué. Remplissez ce champ si votre réseau comprend un serveur DNS.

- **Plage IP**

  Si l'option est activée, vous pouvez saisir les adresses IP de début et de fin de la plage IP à laquelle les appareils concernés doivent appartenir.

  Cette option est Inactif par défaut.

- **Adresse IP de connexion au Serveur d'administration**

  Si cette option est activée, vous pouvez définir les adresses IP par lesquelles les appareils clients sont connectés au Serveur d'administration. Pour ce faire, spécifiez la plage IP qui comprend toutes les adresses IP nécessaires.

  Cette option est Inactif par défaut.

- **L'appareil appartient à la plage IP**

  Si cette option est activée, vous pouvez sélectionner une plage IP que vous avez précédemment ajoutée dans la section **Plages IP**. Les appareils concernés doivent être inclus dans la plage IP sélectionnée.

  Cette option est Inactif par défaut.

- Profil de connexion modifié

  Sélectionnez l'une des valeurs ci-dessous :

  - **Oui**. Une règle de déplacement des appareils s'applique uniquement aux appareils clients dont le profil de connexion a été modifié.
  - **Non**. La règle de déplacement des appareils s'applique uniquement aux appareils clients dont le profil de connexion n'a pas changé.
  - **La valeur n'est pas sélectionnée**. La condition ne s'applique pas.

- Administrés par un autre Serveur d'administration

  Sélectionnez l'une des valeurs ci-dessous :

  - **Oui**. Une règle de déplacement des appareils s'applique uniquement aux appareils clients administrés par d'autres Serveurs d'administration. Ces Serveurs sont différents du Serveur sur lequel vous configurez la règle de déplacement des appareils.
  - **Non**. La règle de déplacement des appareils s'applique uniquement aux appareils clients administrés par le Serveur d'administration actuel.
  - **La valeur n'est pas sélectionnée**. La condition ne s'applique pas.

Onglet Applications

Cet onglet permet de configurer une règle de déplacement des appareils en fonction des applications administrées et des systèmes d'exploitation installés sur les appareils clients :

- L'Agent d'administration est installé

  Sélectionnez l'une des valeurs ci-dessous :

  - **Oui**. Une règle de déplacement des appareils s'applique uniquement aux appareils clients sur lesquels l'Agent d'administration est installé.
  - **Non**. La règle de déplacement des appareils s'applique uniquement aux appareils clients sur lesquels l'Agent d'administration n'est pas installé.
  - **La valeur n'est pas sélectionnée**. La condition ne s'applique pas.

- Applications

  Spécifiez les applications administrées qui doivent être installées sur les appareils clients, de sorte qu'une règle de déplacement des appareils s'applique à ces appareils. Par exemple, vous pouvez sélectionner **Agent d'administration de Kaspersky Security Center 15.1** ou **Serveur d'administration de Kaspersky Security Center 15.1**.

  Si vous ne sélectionnez aucune application administrée, la condition ne s'applique pas.

- Version du système d'exploitation

  Vous pouvez supprimer les appareils clients en fonction de la version du système d'exploitation. Pour ce faire, indiquez les systèmes d'exploitation qui doivent être installés sur les appareils clients. Par conséquent, une règle de déplacement des appareils s'applique aux appareils clients avec les systèmes d'exploitation sélectionnés.

  Si vous n'activez pas cette option, la condition ne s'applique pas. L'option est désactivée par défaut.

- Taille de bit du système d'exploitation

  Vous pouvez sélectionner les appareils clients en fonction de la taille des bits du système d'exploitation. Dans le champ **Taille de bit du système d'exploitation**, vous pouvez sélectionner une des valeurs suivantes :

  - **Inconnu**
  - **x86**
  - **AMD64**
  - **IA64**

  Pour vérifier la taille en bits du système d'exploitation des appareils clients, procédez comme suit :

  1. Dans le menu principal, accédez à la section **Ressources (Appareils)** → **Appareils administrés**.
  2. Cliquez sur le bouton **Paramètres des colonnes** ( ) à droite.
  3. Sélectionnez l'option **Taille de bit du système d'exploitation**, puis cliquez sur le bouton **Enregistrer**.

     Ensuite, la taille en bits du système d'exploitation s'affiche pour chaque appareil administré.

- Version du Service Pack du système d'exploitation

  Dans ce champ, vous pouvez indiquer la version du paquet du système d'exploitation installé (au format X.Y) en présence de laquelle la règle de déplacement s'applique à l'appareil. Par défaut, la version n'est pas indiquée.

- Certificat utilisateur

  Sélectionnez l'une des valeurs ci-dessous :

  - **Installé**. Une règle de déplacement des appareils s'applique uniquement aux appareils mobiles dotés d'un certificat mobile.
  - **Non installé(e)**. La règle de déplacement des appareils s'applique uniquement aux appareils mobiles sans certificat mobile.
  - **La valeur n'est pas sélectionnée**. La condition ne s'applique pas.

- Version du système d'exploitation

  Ce paramètre concerne uniquement les systèmes d'exploitation Windows.

  Vous pouvez indiquer si le système d'exploitation sélectionné doit avoir un numéro de version égal, antérieur ou supérieur. Vous pouvez aussi configurer une règle de déplacement de l'appareil pour tous les numéros de version, à l'exception du numéro indiqué.

- Numéro de version du système d'exploitation

  Ce paramètre concerne uniquement les systèmes d'exploitation Windows.

  Vous pouvez indiquer si le système d'exploitation sélectionné doit avoir un numéro de version égal, antérieur ou supérieur. Vous pouvez également configurer une règle de déplacement des appareils pour tous les numéros de version, à l'exception de celui indiqué.

Onglet Machines virtuelles

Sous cet onglet, vous pouvez configurer une règle de déplacement des appareils selon que les appareils clients sont des machines virtuelles ou font partie d'une infrastructure de bureau virtuel (VDI) :

- Est une machine virtuelle

  Dans la liste déroulante, vous pouvez sélectionner une des options suivantes :
  - **N/A**. La condition ne s'applique pas.
  - **Non**. Déplacez les appareils qui ne sont pas des machines virtuelles.
  - **Oui**. Déplacez les appareils qui sont des machines virtuelles.

- **Type de machine virtuelle**

- Membre d'une Virtual Desktop Infrastructure

  Dans la liste déroulante, vous pouvez sélectionner une des options suivantes :
  - **N/A**. La condition ne s'applique pas.
  - **Non**. Déplacez les appareils qui ne font pas partie de VDI.
  - **Oui**. Déplacez les appareils qui font partie de VDI.

Onglet Contrôleur de domaine

Sous cet onglet, vous pouvez préciser qu'il est nécessaire de déplacer les appareils inclus dans l'unité organisationnelle du domaine. Vous pouvez également déplacer des appareils de toutes les unités organisationnelles enfants de l'unité organisationnelle de domaine spécifiée :

- **L'appareil fait partie de l'unité organisationnelle suivante**

  Si cette option est activée, une règle de déplacement d'appareil s'applique aux appareils de l'unité organisationnelle de domaine spécifiée dans la liste sous l'option.

  Cette option est Inactif par défaut.

- **Inclure les unités d'organisations enfants**

  Si l'option est activée, la sélection inclut les appareils appartenant aux unités organisationnelles enfants de l'unité organisationnelle de domaine spécifiée.

  Cette option est Inactif par défaut.

- **Déplacer les appareils depuis les filiales dans les sous-groupes correspondants**
- **Créer les sous-groupes correspondant aux conteneurs des appareils récemment détectés**
- **Supprimer les sous-groupes inexistants dans le domaine**
- **L'appareil fait partie du groupe de sécurité du domaine suivant**

  Si cette option est activée, une règle de déplacement d'appareil s'applique aux appareils du groupe de sécurité de domaine spécifié dans la liste sous l'option.

  Cette option est Inactif par défaut.

Onglets Segments dans le cloud

Cet onglet vous permet d'indiquer qu'il est nécessaire de déplacer les appareils qui appartiennent à certains segments dans le Cloud :

- **L'appareil se trouve dans un segment dans le cloud**

  Si vous sélectionnez cette option, une règle de déplacement des appareils s'applique aux appareils clients qui appartiennent à un segment dans le Cloud. Vous pouvez sélectionner le segment dans le Cloud requis jusqu'au niveau d'un sous-réseau dans la liste sous l'option.

  L'option est désactivée par défaut.

- **Inclure les objets enfants**

  Si vous sélectionnez cette option, une règle de déplacement d'appareils s'applique non seulement au segment dans le Cloud sélectionné, mais également aux objets enfants de ce segment.

  L'option est désactivée par défaut.

- **Déplacer les appareils des objets enfants vers les sous-groupes correspondants**
- **Créer les sous-groupes correspondant aux conteneurs des appareils récemment détectés**
- **Supprimer les sous-groupes n'ayant pas de correspondance dans les segments dans le cloud**
- **Appareil découvert à l'aide de l'API**

  La liste déroulante permet de choisir s'vous pouvez détecter un appareil à l'aide des outils de l'API :

  - **AWS**. L'appareil est détecté via l'utilisation de l'API AWS, autrement dit, l'appareil est bel et bien dans l'environnement cloud AWS.
  - **Azure**. L'appareil est détecté via l'utilisation de l'API Azure, autrement dit, l'appareil est bel et bien dans l'environnement cloud Azure.
  - **Google Cloud.** L'appareil est détecté via l'utilisation de l'API Google, autrement dit, l'appareil est bel et bien dans le cloud Google.
  - **Non**. L'appareil n'est pas détecté à l'aide de l'API AWS, Azure ou Google, c'est-à-dire qu'il se trouve soit en dehors de l'environnement Cloud, soit dans l'environnement Cloud, mais il ne peut pas être détecté à l'aide d'une API.
  - **Pas de valeur**. Cette condition ne s'applique pas.

À propos des clusters et des groupes des serveurs

Kaspersky Security Center prend en charge la technologie de cluster. Si l'Agent d'administration transmet au Serveur d'administration les informations sur le fait que l'application installée sur l'appareil client est une partie de la matrice du serveur, alors l'appareil client devient le nœud du cluster.

Si un groupe d'administration contient des clusters ou des groupes de serveurs, la page **Appareils administrés** affiche deux onglets, un pour les appareils individuels et un pour les clusters et les groupes de serveurs. Une fois que les appareils administrés ont été détectés en tant que nœuds de cluster, le cluster est ajouté en tant qu'objet individuel à l'onglet **Clusters et matrices de serveurs**.

Les nœuds du cluster ou du groupe de serveurs sont répertoriés sous l'onglet **Appareils**, avec les autres appareils administrés. Vous pouvez afficher les propriétés des nœuds en tant qu'appareils individuels et effectuer d'autres opérations, mais vous ne pouvez pas supprimer un nœud de cluster ou le déplacer vers un autre groupe d'administration séparément de son cluster. Vous pouvez uniquement supprimer ou déplacer un cluster entier.

Vous pouvez effectuer les opérations suivantes avec des clusters ou des groupes de serveurs :

- Afficher les propriétés
- Déplacer le cluster ou le groupe de serveurs vers un autre groupe d'administration

  Lorsque vous déplacez un cluster ou un groupe de serveurs vers un autre groupe, tous ses nœuds se déplacent avec lui, car un cluster et l'un de ses nœuds appartiennent toujours au même groupe d'administration.
- Delete

  Il est raisonnable de supprimer un cluster ou un groupe de serveurs uniquement lorsque le cluster ou le groupe de serveurs n'existe plus dans le réseau de l'organisation. Si un cluster est toujours visible sur votre réseau et que l'Agent d'administration et l'application de sécurité Kaspersky sont toujours installés sur les nœuds du cluster, Kaspersky Security Center remet automatiquement le cluster supprimé et ses nœuds dans la liste des appareils administrés.

Propriétés d'un cluster ou d'un groupe de serveurs

Pour consulter les paramètres d'un cluster ou d'un groupe de serveurs, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Appareils administrés** → **Clusters et matrices de serveurs**.

   La liste des clusters et des groupes de serveurs s'affiche.
2. Cliquez sur le nom du cluster ou du groupe de serveurs requis.

La fenêtre des propriétés du cluster ou du groupe de serveurs sélectionné s'affiche.

Général

La section **Général** affiche des informations générales sur le cluster ou le groupe de serveurs. La boîte de dialogue affiche des informations mises à jour lors de la dernière synchronisation des nœuds du cluster avec le Serveur d'administration :

- **Nom**
- **Description**
- **Domaine Windows**

  Domaine ou groupe de travail Windows, qui contient le cluster ou le groupe de serveurs.
- **Nom NetBIOS**

  Nom de réseau Windows du cluster ou du groupe de serveurs.
- **Nom DNS**

  Nom du domaine DNS du cluster ou du groupe de serveurs.

Tâches

Dans l'onglet **Tâches**, vous pouvez administrer les tâches affectées au cluster ou au groupe de serveurs : afficher la liste des tâches existantes ; en créer de nouveaux ; supprimer, démarrer et arrêter des tâches ; modifier les paramètres de la tâche ; et afficher les résultats d'exécution. Les tâches répertoriées se rapportent à l'application de sécurité Kaspersky installée sur les nœuds du cluster. Kaspersky Security Center reçoit la liste des tâches et les détails de l'état des tâches depuis les nœuds du cluster. Si la connexion échoue, l'état n'est pas affiché.

Nœuds

Cet onglet affiche la liste des nœuds inclus dans le cluster ou le groupe de serveurs. Vous pouvez cliquer sur le nom d'un nœud pour afficher la fenêtre des propriétés de l'appareil.

Application Kaspersky

La fenêtre des propriétés peut également contenir des onglets supplémentaires avec les informations et les paramètres liés à l'application de sécurité Kaspersky installée sur les nœuds du cluster.

Consultation et configuration des actions quand les appareils sont inactifs

Si les appareils client au sein d'un groupe sont inactifs, vous pouvez recevoir des notifications à ce sujet. Vous pouvez également supprimer automatiquement ces appareils.

Pour voir ou configurer les actions lorsque les appareils du groupe sont inactifs :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Hiérarchie des groupes**.
2. Cliquez sur le nom du groupe d'administration concerné.

   La fenêtre des propriétés du groupe d'administration s'ouvre.
3. Dans la fenêtre des propriétés, allez à l'onglet **Paramètres**.
4. Dans la section **Héritage**, activez ou désactivez les options suivantes :

   - **Hériter du groupe parent**

     Les paramètres de cette section sont hérités du groupe parent auquel appartient l'appareil client. Quand cette option est activée, les paramètres du groupe **Activité des appareils sur le réseau** sont verrouillés et ne peuvent être modifiés.

     Cette option est disponible uniquement si le groupe d'administration possède un groupe parent.

     Cette option est activée par défaut.

   - **Imposer l'héritage des paramètres aux groupes enfants**

     Les valeurs des paramètres sont diffusées dans les groupes enfants mais ces paramètres sont verrouillés dans les propriétés des groupes enfants.

     Cette option est Inactif par défaut.

5. Dans la section **Activité des appareils**, activez ou désactivez les options suivantes :

- **Informer l'administrateur si l'appareil n'est pas actif pendant plus de (jours)**

  Quand cette option est activée, l'administrateur reçoit des notifications sur les appareils inactifs. Vous pouvez définir la période à l'issue de laquelle l'événement **L'appareil est resté inactif sur le réseau depuis longtemps** est créé. Par défaut, la valeur de cet intervalle est de 7 jours.

  Cette option est activée par défaut.

- **Supprimer l'appareil du groupe après une inactivité de plus de (jours)**

  Quand cette option est activée, vous pouvez définir la période à l'issue de laquelle un appareil est supprimé automatiquement du groupe. Par défaut, la valeur de cet intervalle est de 60 jours.

  Cette option est activée par défaut.

6. Cliquez sur **Enregistrer**.

Vos modifications sont enregistrées et appliquées.

À propos des états des appareils

Kaspersky Security Center attribue un état à chaque appareil administré. Chaque état dépend du respect des conditions définies par l'utilisateur. Dans certains cas, lors de l'attribution d'un état à un appareil, Kaspersky Security Center prend en compte l'indicateur de visibilité de l'appareil sur le réseau (voir le tableau ci-dessous). Si Kaspersky Security Center ne trouve pas d'appareil sur le réseau dans un délai de deux heures, l'indicateur de visibilité de l'appareil est défini sur *Non visible*.

Les états sont les suivants :

- *Critique* ou *Critique/Visible*
- *Attention* ou *Attention/Visible*
- *OK* ou *OK/Visible*

Le tableau ci-dessous reprend les conditions d'attribution de l'état *Critique* ou *Attention* à l'appareil et ses valeurs possibles.

Conditions d'attribution des états à l'appareil

Condition	Description de la condition	Valeurs possibles
L'application de sécurité n'est pas installée	L'Agent d'administration est installé sur l'appareil mais une application de sécurité n'est pas installée.	• Le bouton radio est allumé. • Le bouton radio est éteint.
Trop de virus ont été détectés	Certains virus ont été retrouvés sur l'appareil par une tâche de détection de virus, par exemple, la tâches de *Analyse des logiciels malveillants*, et le nombre de virus détectés dépasse la valeur spécifiée.	Plus de 0.
Le niveau de la Protection en temps réel diffère de celui défini par l'Administrateur	L'appareil est visible sur le réseau, mais le niveau de protection en temps réel est différent de celui défini par l'administrateur (dans la condition) pour l'état de l'appareil.	• Arrêté. • Suspendu(e). • En cours.

Condition	Description de la condition	Valeurs possibles
La recherche d'applications malveillantes n'a pas été exécutée depuis longtemps	L'appareil est visible sur le réseau et une application de sécurité est installée sur l'appareil, mais ni la tâche d'*Analyse des logiciels malveillants* ni une tâche d'analyse locale n'ont été exécutées dans l'intervalle de temps spécifié. La condition s'applique uniquement aux appareils qui ont été ajoutés à la base de données du Serveur d'administration il y a 7 jours ou avant.	Plus de 1 jour.
Les bases sont dépassées	L'appareil est visible sur le réseau, et une application de sécurité est installée sur l'appareil, mais les bases antivirus n'ont pas été mises à jour sur cet appareil dans la période indiquée. La condition s'applique uniquement aux appareils qui ont été ajoutés à la base de données du Serveur d'administration il y a 1 jour ou avant.	Plus de 1 jour.
Ne s'est pas connecté depuis longtemps	L'Agent d'administration est installé sur l'appareil, mais l'appareil ne s'est pas connecté au Serveur d'administration dans la période indiquée car l'appareil était désactivé.	Plus de 1 jour.
Des menaces actives sont détectées	La quantité d'objets non traités dans le dossier **Menaces actives** dépasse la valeur indiquée.	Plus de 0 pièce.
Redémarrage requis	L'appareil est visible sur le réseau, mais une application nécessite le redémarrage de l'appareil depuis la durée indiquée et pour l'une des raisons sélectionnées.	Plus de 0 minute.
Des applications incompatibles sont installées	L'appareil est visible sur le réseau, mais l'inventaire des applications effectué par l'Agent d'administration a détecté des applications incompatibles installées sur l'appareil.	• Le bouton radio est éteint. • Le bouton radio est allumé.
Vulnérabilités dans les applications	L'appareil est visible sur le réseau, et l'Agent d'administration est installé sur l'appareil, mais la tâche *Recherche de vulnérabilités et de mises à jour requises* a détecté des vulnérabilités avec le niveau de gravité indiqué dans les applications installées sur l'appareil.	• Critique. • Élevé. • Normal. • Ignorer s'il est impossible de fermer la vulnérabilité. • Ignorer si la mise à jour a été désignée à l'installation.
La licence a expiré	L'appareil est visible sur le réseau, mais la licence a expiré.	• Le bouton radio est éteint. • Le bouton radio est allumé.
la licence expire bientôt	L'appareil est visible sur le réseau, mais la licence expirera sur l'appareil dans moins de jours que le nombre indiqué.	Moins de 0 jours.
La vérification de mises à jour Windows Update n'a pas eu lieu depuis longtemps	L'appareil est visible sur le réseau, mais la tâche *Synchronisation des mises à jour Windows Update* n'a plus été exécutée dans la période indiquée.	Plus de 1 jour.
État de chiffrement non valide	L'Agent d'administration est installé sur l'appareil mais le résultat du chiffrement de l'appareil est égal à la valeur indiquée.	• Ne correspond pas à la stratégie à cause du refus de l'utilisateur (uniquement pour les appareils externes). • Ne correspond pas à la stratégie à cause de l'erreur. • Stratégie en cours d'application – le redémarrage est requis. • La stratégie de chiffrement n'est pas définie. • Non pris en charge. • Stratégie en cours d'application.
Les paramètres de l'appareil mobile ne correspondent pas à la stratégie	Les paramètres de l'appareil mobile se distinguent des paramètres définis dans la stratégie Kaspersky Endpoint Security for Android lors de l'analyse des règles de concordance.	• Le bouton radio est éteint. • Le bouton radio est allumé.

Condition	Description de la condition	Valeurs possibles
Problèmes de sécurité non traités détectés	Certains problèmes de sécurité non traités ont été détectés sur l'appareil. Les problèmes de sécurité peuvent être créés automatiquement, à l'aide des applications administrées de Kaspersky installées sur l'appareil client, ou manuellement par l'administrateur.	• Le bouton radio est éteint. • Le bouton radio est allumé.
État de l'appareil défini par l'application	L'état de l'appareil est défini par l'application administrée.	• Le bouton radio est éteint. • Le bouton radio est allumé.
Espace disque épuisé sur l'appareil	L'espace disque disponible est inférieur à la valeur indiquée ou l'appareil n'a pas pu être synchronisé avec le Serveur d'administration. L'état *Critique* ou *Attention* est redéfini sur *OK* lorsque l'appareil est synchronisé avec le Serveur d'administration et que l'espace libre sur l'appareil est supérieur ou égal à la valeur spécifiée.	Plus de 0 Mo.
L'appareil n'est plus administré	Lors de la recherche d'appareils, celui-ci est considéré comme visible sur le réseau, mais plus de trois tentatives ratées de synchronisation avec le Serveur d'administration ont eu lieu.	• Le bouton radio est éteint. • Le bouton radio est allumé.
La protection est désactivée	L'appareil est visible sur le réseau, mais l'application de sécurité sur l'appareil est désactivée depuis plus longtemps que la durée indiquée. Dans ce cas, l'état de l'application de sécurité est *arrêté* ou *échec*, et différent de l'état suivant : *démarrage*, *en cours d'exécution* ou *suspendu*.	Plus de 0 minute.
L'application de sécurité n'est pas en cours d'exécution	L'appareil est visible sur le réseau, et une application de sécurité est installée sur l'appareil, mais n'est pas exécutée.	• Le bouton radio est éteint. • Le bouton radio est allumé.

Kaspersky Security Center permet de configurer la permutation automatique de l'état d'un appareil dans un groupe d'administration quand les conditions définies sont remplies. Quand les conditions définies sont remplies, l'appareil client reçoit un des états suivants : *Critique* ou *Attention*. Lorsque les conditions spécifiées ne sont pas remplies, l'état *OK* est affecté à l'appareil client.

Des différents états peuvent correspondre à des différentes valeurs d'une condition. Par exemple, par défaut, si vous respectez la condition **Les bases sont dépassées** avec la valeur **Plus de 3 jours**, l'appareil client se verra affecter l'état *Avertissement*, et avec la valeur **Plus de 7 jours**, l'état *Critique*.

Si vous mettez à niveau Kaspersky Security Center à partir de la version précédente, les valeurs de **Les bases sont dépassées** la condition d'attribution de l'état à *Critique* ou *Avertissement* ne change pas.

Lorsque Kaspersky Security Center attribue un statut à un appareil, pour certaines conditions (voir la colonne Description de la condition), l'indicateur de visibilité est pris en considération. Par exemple, si un appareil administré a reçu l'état *Critique* parce que la condition Les bases sont dépassées a été remplie, et qu'ensuite l'indicateur de visibilité a été placé pour l'appareil, alors l'appareil reçoit l'état *OK*.

Configuration de la permutation des états des appareils

Vous pouvez modifier les conditions pour attribuer le statut *Critique* ou *Avertissement* à un appareil.

Pour activer le changement d'état de l'appareil sur Critique :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Hiérarchie des groupes**.
2. Dans la liste des groupes qui s'affiche, cliquez sur le lien portant le nom d'un groupe dont vous voulez changer les états de l'appareil.
3. Dans la fenêtre des propriétés qui s'ouvre, sélectionnez l'onglet **État de l'appareil**.

4. Dans le volet de gauche, sélectionnez **Critique**.
5. Dans le volet droit, dans la section **Définir l'état comme "Critique" si les options suivantes sont définies**, activez la condition pour basculer un appareil en état *Critique*.

   Vous pouvez modifier seulement les paramètres qui ne sont pas verrouillés dans la stratégie parent.

6. Sélectionnez le bouton radio à côté de la condition dans la liste.
7. Dans le coin supérieur gauche de la liste, cliquez sur le bouton **Modifier**.
8. Définissez la valeur requise pour la condition sélectionnée.

   Certaines conditions n'acceptent pas de valeurs.

9. Cliquez sur le bouton **OK**.

Lorsque les conditions spécifiées sont remplies, l'appareil administré se voit affecter l'état *Critique*.

Pour activer le changement d'état de l'appareil sur Avertissement :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Hiérarchie des groupes**.
2. Dans la liste des groupes qui s'affiche, cliquez sur le lien portant le nom d'un groupe dont vous voulez changer les états de l'appareil.
3. Dans la fenêtre des propriétés qui s'ouvre, sélectionnez l'onglet **État de l'appareil**.
4. Dans le volet gauche, sélectionnez **Avertissement**.
5. Dans le volet droit, dans la section **Définir l'état comme "Avertissement" si les options suivantes sont définies,** activez la condition pour basculer un appareil en état *Avertissement*.

   Vous pouvez modifier seulement les paramètres qui ne sont pas verrouillés dans la stratégie parent.

6. Sélectionnez le bouton radio à côté de la condition dans la liste.
7. Dans le coin supérieur gauche de la liste, cliquez sur le bouton **Modifier**.
8. Définissez la valeur requise pour la condition sélectionnée.

   Certaines conditions n'acceptent pas de valeurs.

9. Cliquez sur le bouton **OK**.

Lorsque certaines conditions spécifiées sont remplies, l'appareil administré se voit affecter l'état *Avertissement*.

Connexion à distance au bureau de l'appareil client

L'administrateur peut obtenir l'accès au bureau de l'appareil client à l'aide de l'Agent d'administration installé sur l'appareil. La connexion à distance à l'appareil client à l'aide de l'Agent d'administration est même possible dans le cas si les ports TCP et UDP de l'appareil client ne sont pas accessibles.

Après la connexion à l'appareil, l'administrateur obtient l'accès complet aux informations sur cet appareil et peut administrer les applications installées sur celui-ci.

La connexion à distance doit être autorisée dans les paramètres du système d'exploitation de l'appareil administré cible. Par exemple, dans Windows 10, cette option est appelée **Autoriser les connexions d'assistance à distance vers cet ordinateur** (vous pouvez trouver cette option dans **Panneau de configuration → Système et sécurité → Système → Paramètres d'utilisation à distance**). Si vous disposez d'une licence pour la fonctionnalité de la gestion des vulnérabilités et des correctifs, vous pouvez imposer l'activation de cette option lorsque vous établissez une connexion à un appareil administré. Si vous ne disposez pas de la licence, activez cette option localement sur l'appareil administré cible. Si cette option est désactivée, la connexion à distance n'est pas possible.

Pour établir une connexion à distance à un appareil, vous devez disposer de deux utilitaires :

- Utilitaire Kaspersky intitulé klsctunnel. Cet utilitaire doit être stocké sur le poste de travail de l'administrateur. Vous utilisez cet utilitaire pour établir une connexion en tunnel entre un appareil client et le Serveur d'administration.

  Kaspersky Security Center permet d'établir des connexions TPC en tunnel depuis la Console d'administration via le Serveur d'administration et puis via l'Agent d'administration vers le port défini sur l'appareil administré. Le tunnel est utilisé pour connecter une app cliente qui se trouve sur un appareil doté de la Console d'administration au port TCP sur l'appareil administré si la connexion directe de l'appareil avec la Console d'administration et l'appareil n'est pas possible.

  La connexion en tunnel de l'appareil client à distance avec le Serveur d'administration est nécessaire si le port de connexion au Serveur d'administration est inaccessible sur l'appareil. Le port sur l'appareil peut être inaccessible dans les cas suivants :

  - L'appareil à distance est connecté au réseau local avec le mécanisme NAT utilisé.
  - L'appareil à distance fait partie du réseau local du Serveur d'administration, mais son port est fermé par un pare-feu.

- Module standard de Microsoft Windows intitulé " Connexion Bureau à distance ". La connexion au bureau à distance est exécutée à l'aide de l'utilitaire titulaire de Windows mstsc.exe conformément aux paramètres de fonctionnement de cet utilitaire.

  La connexion à la session en cours sur le poste de travail distant de l'utilisateur s'établit sans notification. Une fois l'administrateur connecté à la session, l'utilisateur de l'appareil sera déconnecté sans notification.

Pour se connecter à distance au bureau de l'appareil client, procédez comme suit :

1. Dans la Console d'administration basée sur MMC, dans le menu contextuel du Serveur d'administration, choisissez l'option **Propriétés**.
2. Dans la fenêtre des propriétés du Serveur d'administration qui s'ouvre, accédez à **Paramètres de connexion au Serveur d'administration → Ports de connexion**.
3. Assurez-vous que l'option **Ouvrir le port RDP pour Kaspersky Security Center Web Console** est activée.
4. Dans Kaspersky Security Center Web Console, accédez à **Ressources (Appareils) → Appareils administrés**.
5. Dans le champ **Chemin d'accès actif** au-dessus de la liste des appareils administrés, cliquez sur le lien vers le chemin.
6. Dans le volet de gauche qui s'ouvre, sélectionnez le groupe d'administration qui contient l'appareil auquel vous voulez accéder.

7. Cochez la case en regard du nom de l'appareil auquel vous souhaitez avoir accès.

8. Cliquez sur le bouton **Se connecter au bureau distant**.

   La fenêtre Bureau distant (Windows uniquement) s'ouvre.

9. Activez l'option **Autoriser la Connexion Bureau à distance sur l'appareil administré**. Dans ce cas, la connexion sera établie même si les connexions à distance sont actuellement interdites dans les paramètres du système d'exploitation sur l'appareil administré.

   Cette option n'est disponible que si vous disposez d'une licence pour la fonctionnalité Gestion des vulnérabilités et des correctifs.

10. Cliquez sur le bouton **Télécharger** pour télécharger l'utilitaire klsctunnel.

11. Cliquez sur le bouton **Copier dans le presse-papiers** pour copier le texte du champ de texte. Ce texte est un objet de données binaires (BLOB) qui contient les paramètres requis pour établir la connexion entre le Serveur d'administration et l'appareil administré.

    Un BLOB est valide pendant 3 minutes. Si celui-ci a expiré, ouvrez de nouveau la fenêtre Bureau distant (Windows uniquement) pour générer un nouveau BLOB.

12. Exécutez l'utilitaire klsctunnel.

    La fenêtre de l'utilitaire s'ouvre.

13. Collez le texte copié dans le champ de texte.

14. Si vous utilisez un serveur proxy, cochez la case **Utiliser un serveur proxy**, puis indiquez les paramètres de connexion du serveur proxy.

15. Cliquez sur **Ouvrir le port**.

    La fenêtre Connexion Bureau à distance s'ouvre.

16. Indiquez les informations d'identification du compte à partir duquel vous êtes actuellement connecté à Kaspersky Security Center Web Console.

17. Cliquez sur le bouton **Se connecter**.

Lorsque la connexion à l'appareil client est établie, le bureau de l'appareil client est accessible dans la fenêtre Connexion Bureau à distance de Microsoft Windows.

Connexion aux appareils à l'aide du Partage du bureau Windows

L'administrateur peut obtenir l'accès au bureau de l'appareil client à l'aide de l'Agent d'administration installé sur l'appareil. La connexion à distance à l'appareil client à l'aide de l'Agent d'administration est même possible dans le cas si les ports TCP et UDP de l'appareil client ne sont pas accessibles.

L'administrateur peut se connecter à la séance existante sur l'appareil client sans la déconnexion de l'utilisateur travaillant dans cette séance. Dans ce cas, l'administrateur et l'utilisateur de la session sur l'appareil ont un accès collectif au bureau.

Pour établir une connexion à distance à un appareil, vous devez disposer de deux utilitaires :

- Utilitaire Kaspersky intitulé klsctunnel. Cet utilitaire doit être stocké sur le poste de travail de l'administrateur. Vous utilisez cet utilitaire pour établir une connexion en tunnel entre un appareil client et le Serveur d'administration.

  Kaspersky Security Center permet d'établir des connexions TPC en tunnel depuis la Console d'administration via le Serveur d'administration et puis via l'Agent d'administration vers le port défini sur l'appareil administré. Le tunnel est utilisé pour connecter une app cliente qui se trouve sur un appareil doté de la Console d'administration au port TCP sur l'appareil administré si la connexion directe de l'appareil avec la Console d'administration et l'appareil n'est pas possible.

  La connexion en tunnel de l'appareil client à distance avec le Serveur d'administration est nécessaire si le port de connexion au Serveur d'administration est inaccessible sur l'appareil. Le port sur l'appareil peut être inaccessible dans les cas suivants :

  - L'appareil à distance est connecté au réseau local avec le mécanisme NAT utilisé.
  - L'appareil à distance fait partie du réseau local du Serveur d'administration, mais son port est fermé par un pare-feu.

- Partage du bureau Windows. Lors de la connexion à la séance existante du bureau à distance, l'utilisateur de cette séance sur l'appareil recevra une demande de connexion en provenance de l'administrateur. Les informations sur le processus de l'utilisation à distance de l'appareil et sur les résultats de cette utilisation ne sont pas conservées dans les rapports de Kaspersky Security Center.

  L'administrateur peut configurer l'audit des actions sur l'appareil client distant. Lors de l'audit, l'application enregistre les informations relatives aux fichiers que l'administrateur a ouverts et/ou modifiés sur l'appareil client.

Pour se connecter au bureau d'un appareil client à l'aide du Partage du bureau Windows, les conditions suivantes doivent être remplies :

- Microsoft Windows Vista ou une version plus récente est installée sur le poste de travail de l'administrateur. Le type du système d'exploitation de l'appareil hébergeant le Serveur d'administration ne représente pas une restriction pour la connexion à l'aide de Partage du bureau Windows.

  Pour vérifier si la fonctionnalité de partage de bureau Windows est incluse dans votre édition Windows, assurez-vous qu'il existe une clé CLSID\{32BE5ED2-5C86-480F-A914-0FF8885A1B3F} dans le registre Windows.

- Microsoft Windows Vista ou une version plus récente est installée sur l'appareil client.
- Kaspersky Security Center utilise la licence sur la Gestion des vulnérabilités et des correctifs.

Pour se connecter au bureau de l'appareil client à l'aide de la technologie Partage du bureau Windows, procédez comme suit :

1. Dans la Console d'administration basée sur MMC, dans le menu contextuel du Serveur d'administration, choisissez l'option **Propriétés**.
2. Dans la fenêtre des propriétés du Serveur d'administration qui s'ouvre, accédez à **Paramètres de connexion au Serveur d'administration → Ports de connexion**.
3. Assurez-vous que l'option **Ouvrir le port RDP pour Kaspersky Security Center Web Console** est activée.
4. Dans Kaspersky Security Center Web Console, accédez à **Ressources (Appareils) → Appareils administrés**.

5. Dans le champ **Chemin d'accès actif** au-dessus de la liste des appareils administrés, cliquez sur le lien vers le chemin.

6. Dans le volet de gauche qui s'ouvre, sélectionnez le groupe d'administration qui contient l'appareil auquel vous voulez accéder.

7. Cochez la case en regard du nom de l'appareil auquel vous souhaitez avoir accès.

8. Cliquez sur le bouton **Partage du bureau Windows**.

   L'Assistant Partage du bureau Windows s'ouvre.

9. Cliquez sur le bouton **Télécharger** pour télécharger l'utilitaire klsctunnel et attendez la fin du processus de téléchargement.

   Si vous disposez déjà de l'utilitaire klsctunnel, ignorez cette étape.

10. Cliquez sur le bouton **Suivant**.

11. Sélectionnez la session sur l'appareil auquel vous souhaitez vous connecter, puis cliquez sur le bouton **Suivant**.

12. Sur l'appareil cible, dans la boîte de dialogue qui s'ouvre, l'utilisateur doit autoriser une session de partage de bureau. Dans le cas contraire, il n'est pas possible d'ouvrir une session.

    Une fois que l'utilisateur de l'appareil a confirmé la session de partage de bureau, la page suivante de l'Assistant s'ouvre.

13. Cliquez sur le bouton **Copier dans le presse-papiers** pour copier le texte du champ de texte. Ce texte est un objet de données binaires (BLOB) qui contient les paramètres requis pour établir la connexion entre le Serveur d'administration et l'appareil administré.

    > Un BLOB est valide pendant 3 minutes. Si celui-ci a expiré, générez un nouveau BLOB.

14. Exécutez l'utilitaire klsctunnel.

    La fenêtre de l'utilitaire s'ouvre.

15. Collez le texte copié dans le champ de texte.

16. Si vous utilisez un serveur proxy, cochez la case **Utiliser un serveur proxy**, puis indiquez les paramètres de connexion du serveur proxy.

17. Cliquez sur **Ouvrir le port**.

Le partage du bureau démarre dans une nouvelle fenêtre. Si vous souhaitez interagir avec l'appareil, cliquez sur l'icône du menu ( ) dans le coin supérieur gauche de la fenêtre, puis sélectionnez **Mode interactif**.

Sélections d'appareils

Les *sélections d'appareils* sont un outil conçu pour filtrer les appareils en fonction de certaines conditions. Vous pouvez utiliser les sélections d'appareils pour administrer plusieurs appareils : par exemple, pour voir un rapport uniquement au sujet de ces appareils ou pour déplacer ces appareils vers un autre groupe.

Kaspersky Security Center offre un large éventail de *sélections prédéfinies* (par exemple, **Appareils avec l'état Critique**, **La protection est désactivée**, **Des menaces actives sont détectées**). Il est impossible de supprimer les sélections prédéfinies. Vous pouvez également créer et configurer des *sélections personnalisées*.

Dans les sélections personnalisées, vous pouvez définir la zone d'action de recherche et sélectionner tous les appareils, les appareils administrés ou les appareils non définis. Certains paramètres sont définis dans les conditions. Vous pouvez créer plusieurs conditions avec différents paramètres de recherche dans la sélection d'appareils. Par exemple, vous pouvez créer deux conditions et définir des plages IP différentes pour chacune d'entre elles. Si plusieurs conditions sont définies, une sélection affiche les appareils qui remplissent n'importe quelle condition. Par contraste, les paramètres de recherche au sein d'une condition sont superposés. Si une plage IP et le nom d'une application installée sont définis dans une condition, seuls ces appareils seront affichés lorsque l'application est installée et que l'adresse IP appartient à la plage indiquée.

Consultation de la liste des appareils à partir d'une sélection d'appareils

Kaspersky Security Center vous permet d'afficher la liste des appareils à partir d'une sélection d'appareils.

Pour consulter la liste des appareils à partir de la sélection d'appareils, procédez comme suit :

1. Dans le menu principal, accédez à la section **Ressources (Appareils)** → **Sélections d'appareils** ou **Découverte et déploiement** → **Sélections d'appareils**.

2. Dans la liste de sélection, cliquez sur le nom de la sélection d'appareils.

   La page affiche un tableau avec des informations sur les appareils inclus dans la sélection d'appareils.

3. Vous pouvez regrouper et filtrer les données du tableau des appareils comme suit :

   - Cliquez sur l'icône des paramètres ( ), puis sélectionnez les colonnes à afficher dans le tableau.

   - Cliquez sur l'icône du filtre ( ), puis spécifiez et appliquez le critère de filtre dans le menu appelé.

     Le tableau filtré des appareils s'affiche.

Vous pouvez sélectionner un ou plusieurs appareils dans la sélection d'appareils et cliquer sur le bouton **Nouvelle tâche** pour créer une tâche qui sera appliquée à ces appareils.

Pour déplacer les appareils sélectionnés de la sélection d'appareils vers un autre groupe d'administration, cliquez sur le bouton **Déplacer vers le groupe**, puis sélectionnez le groupe d'administration cible.

Création d'une sélection d'appareils

Pour créer une sélection d'appareils, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Sélections d'appareils**.

   Une page comportant une liste de sélections d'appareils s'affiche.

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

   La fenêtre **Paramètres de sélection d'appareils** s'ouvre.

3. Saisissez le nom de la nouvelle sélection.

4. Indiquez le groupe qui contient les appareils à inclure dans la sélection d'appareils :

   - **Rechercher tous les appareils** : recherche d'appareils qui répondent aux critères de sélection et qui sont inclus dans le groupe **Appareils administrés** ou **Appareils non définis**.
   - **Rechercher les appareils administrés** : recherche d'appareils qui répondent aux critères de sélection et qui sont inclus dans le groupe **Appareils administrés**.
   - **Rechercher les appareils non définis** : recherche d'appareils qui répondent aux critères de sélection et qui sont inclus dans le groupe **Appareils non définis**.

   Vous pouvez cocher la case **Inclure les données des Serveurs d'administration secondaires** pour activer la recherche d'appareils qui répondent aux critères de sélection et qui sont administrés par les Serveurs d'administration secondaires.

5. Cliquez sur le bouton **Ajouter**.
6. Dans la fenêtre qui s'ouvre, spécifiez les conditions à remplir pour inclure les appareils dans cette sélection, puis cliquez sur le bouton **OK**.
7. Cliquez sur le bouton **Enregistrer**.

La sélection d'appareils est créée et ajoutée à la liste des sélections d'appareils.

Configuration d'une sélection d'appareils

Pour configurer la sélection d'appareils, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Sélections d'appareils**.

   Une page comportant une liste de sélections d'appareils s'affiche.

2. Sélectionnez la sélection d'appareils définie par l'utilisateur pertinente, puis cliquez sur le bouton **Propriétés**.

   La fenêtre **Paramètres de sélection d'appareils** s'ouvre.

3. Sous l'onglet **Général**, cliquez sur le lien **Nouvelle condition**.
4. Définissez les conditions à remplir pour inclure les appareils dans cette sélection.
5. Cliquez sur le bouton **Enregistrer**.

Les paramètres sont appliqués et enregistrés.

Les paramètres des conditions d'ajout des appareils à une sélection sont décrits ci-dessous. Les conditions sont combinées à l'aide de l'opérateur logique " ou " : la sélection reprend les appareils qui répondent au moins à une des conditions présentées.

Général

La section **Général** permet de modifier le nom de la condition de la sélection et d'indiquer si cette condition doit être intervertie :

Inverser la condition de sélection

Cette option est Inactif par défaut.

Si vous activez cette option, la condition de sélection définie sera inversée. Tous les appareils qui ne correspondent pas à la condition feront partie de la sélection.

L'exemple suivant montre la logique du travail d'inversion :

- **Condition** : sur votre appareil, il y a un système d'exploitation avec le type Linux et le numéro de build 00.0.000.
- **Condition inversée** : sur votre appareil, il existe un système d'exploitation avec NOT (le type de version Linux et le numéro de build 00.0.000), ce qui équivaut à ce qui suit :

  Il existe un système d'exploitation de type NOT Linux OU numéro de build NOT 00.0.000.

Ainsi, la sélection inclura les appareils équipés d'un système d'exploitation, par exemple, de type Windows et dont le numéro de build est 00.0.000, ou de type Linux et dont le numéro de build est différent de 00.0.000.

Infrastructure réseau

La sous-section **Réseau** permet de configurer les critères d'inclusion des appareils dans une sélection sur la base de leurs données de réseau.

- Nom de l'appareil

  Nom de réseau Windows (nom NetBIOS) de l'appareil ou adresse IPv4 ou IPv6.

- Domaine

  Les appareils faisant partie du domaine Windows indiqué seront affichés.

- Groupe d'administration

  Les appareils faisant partie du groupe d'administration seront affichés.

- Description

Texte apparaissant dans la fenêtre des propriétés de l'appareil : dans le champ **Description** de la section **Général**.

Pour décrire le texte dans le champ **Description**, vous pouvez utiliser les caractères suivants :

- A l'intérieur d'un seul mot :
  - *****. Remplace n'importe quelle ligne quel que soit le nombre de caractères.

  Exemple :

  Pour décrire les mots **Serveur**, **Serveurs** ou de serveur, il est possible d'utiliser la ligne **Serveur***.
  - **?.** Remplace un n'importe quel caractère.

  Exemple :

  Pour décrire les mots **Fenêtre** ou **Fenêtres**, il est possible d'utiliser la ligne **Fenêtr?**.

  Caractère ***** ou **?** ne peut pas être utilisé en tant que premier caractère dans la description du texte.
- Pour lier plusieurs mots :
  - Espace. Affiche l'ensemble des appareils dont la description contient l'un des mots de la liste.

  Exemple :

  Pour décrire la phrase contenant le mot **Secondaire** ou **Virtuel**, il est possible d'utiliser la ligne **Secondaire Virtuel**.
  - **+**. Avant le mot signifie la présence obligatoire du mot dans le texte.

  Exemple :

  Pour décrire la phrase contenant le mot **Secondaire**, et le mot **Virtuel**, il est possible de saisir la demande **+Secondaire+Virtuel**.
  - **-**. Avant le mot signifie l'absence obligatoire du mot dans le texte.

  Exemple :

  Pour décrire la phrase avec le mot **Secondaire** et sans le mot **Virtuel**, il est possible de saisir la demande **+Secondaire-Virtuel**.
  - **"<le texte>"**. Le fragment du texte entre guillemets doit être entièrement présent dans le texte.

  Exemple :

  Pour décrire la phrase contenant le groupe de mots **Serveur secondaire**, il est possible de saisir la demande **"Serveur secondaire"**.

- Plage IP

  Si l'option est activée, vous pouvez saisir les adresses IP de début et de fin de la plage IP à laquelle les appareils concernés doivent appartenir.

  Cette option est Inactif par défaut.

- Administrés par un autre Serveur d'administration

  Sélectionnez l'une des valeurs ci-dessous :

  - **Oui**. Une règle de déplacement des appareils s'applique uniquement aux appareils clients administrés par d'autres Serveurs d'administration. Ces Serveurs sont différents du Serveur sur lequel vous configurez la règle de déplacement des appareils.
  - **Non**. La règle de déplacement des appareils s'applique uniquement aux appareils clients administrés par le Serveur d'administration actuel.
  - **La valeur n'est pas sélectionnée**. La condition ne s'applique pas.

La sous-section **Contrôleur de domaine** permet de configurer les critères pour inclure des appareils dans une sélection basée sur l'appartenance au domaine :

- L'appareil fait partie d'une unité organisationnelle du domaine

  Si cette option est activée, la sélection inclut les appareils de l'unité organisationnelle du domaine spécifiée dans le champ de saisie.

  Cette option est Inactif par défaut.

- Cet appareil est membre du groupe de sécurité du domaine

  Si cette option est activée, la sélection inclut les appareils du groupe de sécurité de domaine spécifié dans le champ de saisie.

  Cette option est Inactif par défaut.

La sous-section **Activité réseau** permet de configurer les critères d'inclusion des appareils dans une sélection sur la base de leur activité réseau :

- Agit comme point de distribution

  La liste déroulante permet de sélectionner les critères d'inclusion des appareils dans la sélection dans le cadre d'une recherche :

  - **Oui**. La sélection contient les appareils qui ne sont pas des points de distribution.
  - **Non**. Les appareils qui sont les points de distribution ne seront pas inclus dans la sélection.
  - **La valeur n'est pas sélectionnée**. Les critères ne sont pas appliqués.

- Maintenir la connexion au Serveur d'administration

  La liste déroulante permet de sélectionner les critères d'inclusion des appareils dans la sélection dans le cadre d'une recherche :

  - **Activé**. La sélection comportera des appareils sur lesquels la case **Maintenir la connexion au Serveur d'administration** est cochée.
  - **Désactivé**. La sélection comprendra des appareils sur lesquels la case **Maintenir la connexion au Serveur d'administration** est décochée.
  - **La valeur n'est pas sélectionnée**. Les critères ne sont pas appliqués.

- Changement du profil de connexion

  La liste déroulante permet de sélectionner les critères d'inclusion des appareils dans la sélection dans le cadre d'une recherche :

  - **Oui**. La sélection inclura les appareils connectés au Serveur d'administration suite au changement du profil de connexion.
  - **Non**. La sélection n'inclura pas les appareils connectés au Serveur d'administration suite au changement du profil de connexion.
  - **La valeur n'est pas sélectionnée**. Les critères ne sont pas appliqués.

- Dernière connexion au Serveur d'administration

  Cette case permet de définir les critères de recherche d'appareils selon la date et l'heure de la dernière connexion au Serveur d'administration.

  Si la case est cochée, le champ de saisie permet d'indiquer les valeurs de l'intervalle de temps (date et heure), durant lequel la dernière connexion de l'Agent d'administration installé sur l'appareil client avec le Serveur d'administration a été effectuée. La sélection contient les appareils qui s'inscrivent dans l'intervalle défini.

  Si la case est décochée, le critère ne sera pas appliqué.

  Celle-ci est décochée par défaut.

- Nouveaux appareils détectés lors d'un sondage du réseau

  Recherche de nouveaux appareils détectés lors du sondage du réseau au cours des derniers jours.

  Si l'option est activée, la sélection inclut seulement les nouveaux appareils détectés lors de la recherche d'appareils au cours du nombre de jours défini dans le champ **Période de détection (jours)**.

  Si l'option est désactivée, la sélection inclut tous les appareils détectés lors de la recherche d'appareils.

  Cette option est Inactif par défaut.

- Appareil visible

  La liste déroulante permet de sélectionner les critères d'inclusion des appareils dans la sélection dans le cadre d'une recherche :

  - **Oui**. L'application est reprise dans la sélection d'appareils visibles sur le réseau à l'heure actuelle.
  - **Non**. L'application est reprise dans la sélection d'appareils qui ne sont pas visibles sur le réseau à l'heure actuelle.
  - **La valeur n'est pas sélectionnée**. Les critères ne sont pas appliqués.

La sous-section **Segments dans le cloud** permet de configurer les critères d'inclusion des appareils dans une sélection sur la base de leur appartenance aux segments dans le Cloud :

- L'appareil se trouve dans un segment dans le cloud

  Si cette option est activée, vous pouvez choisir des appareils dans les segments dans le cloud AWS, Azure et Google.

  Si l'option **Inclure les objets enfants** est également activée, la recherche est exécutée sur l'ensemble des objets enfants du segment sélectionné.

  Seuls les appareils du segment choisi figurent dans les résultats de la recherche.

- Appareil découvert à l'aide de l'API

  La liste déroulante permet de choisir si vous pouvez détecter un appareil à l'aide des outils de l'API :

  - **Oui**. L'appareil est détecté à l'aide de l'API AWS, Azure ou Google.
  - **Non**. L'appareil ne peut pas être détecté à l'aide de l'API AWS, Azure ou Google. C'est-à-dire que l'appareil se trouve soit en dehors de l'environnement cloud, soit dans l'environnement cloud, mais il ne peut pas être détecté à l'aide d'une API.
  - Pas de valeur. Cette condition ne s'applique pas.

États des appareils

La sous-section **État de l'appareil administré** permet de configurer les critères d'inclusion des appareils dans une sélection sur la base de la description de l'état de l'appareil envoyé par une application administrée :

- **État de l'appareil**

  Liste déroulante qui permet de sélectionner l'un des états de l'appareil : *OK*, *Critique* ou *Avertissement*.

- **État de la protection en temps réel**

  Liste déroulante vous permettant de sélectionner l'état de la protection en temps réel. Les appareils avec l'état indiqué de la protection en temps réel seront inclus dans la sélection.

- **Description d'état de l'appareil**

  Ce champ permet de cocher les cases en regard des conditions qui, lorsqu'elles sont remplies, affectent l'un des états suivants à l'appareil : *OK, Critique* ou *Avertissement*.

La sous-section **État des modules des applications administrées** permet de configurer les critères d'inclusion des appareils dans une sélection sur la base de l'état des modules dans les applications administrées :

- **État de la protection contre les fuites de données**

  Recherchez des appareils sur la base de l'état de la Protection contre les fuites de données (*Inconnu, Arrêté(e), En cours de démarrage, Suspendu(e), En cours d'exécution, Échec*).

- **État de la protection des serveurs de collaboration**

  Recherchez des appareils sur la base de l'état de la protection de collaboration du serveur (*Inconnu, Arrêté(e), En cours de démarrage, Suspendu(e), En cours d'exécution, Échec*).

- **État de Endpoint Protection des serveurs de messagerie**

  Recherchez des appareils sur la base de l'état de la protection du Serveur de messagerie (*Inconnu, Arrêté(e), En cours de démarrage, Suspendu(e), En cours d'exécution, Échec*).

- **État de Endpoint Sensor**

  Recherchez des appareils sur la base de l'état du module Endpoint Sensor (*Inconnu, Arrêté(e), En cours de démarrage, Suspendu(e), En cours d'exécution, Échec*).

La sous-section **Problèmes ayant une incidence sur l'état dans les applications administrées** permet de spécifier les critères d'inclusion des appareils dans une sélection sur la base de la liste des problèmes potentiels détectés par une application administrée. Si au moins un des problèmes que vous avez sélectionné existe sur un appareil, l'appareil est repris dans la sélection. Quand vous sélectionnez un problème repris pour plusieurs applications, vous avez la possibilité de sélectionner ce problème dans toutes les listes automatiquement.

Vous pouvez cocher les cases pour les descriptions des états de l'application administrée dont la réception entraînera l'inclusion de l'appareil dans la sélection. Quand vous sélectionnez un état repris pour plusieurs applications, vous avez la possibilité de sélectionner cet état dans toutes les listes automatiquement.

Détails sur le système

La section **Système d'exploitation** permet de configurer les critères d'inclusion d'appareils dans une sélection en fonction du type de système d'exploitation installé.

- Type de plateforme

  Si la case est cochée, la liste permet de sélectionner les systèmes d'exploitation. Les appareils avec les systèmes d'exploitation indiqués installés sont inclus dans les résultats de recherche.

- Version du Service Pack du système d'exploitation

  Dans ce champ, vous pouvez indiquer la version du paquet du système d'exploitation installé (au format X.Y) en présence de laquelle la règle de déplacement s'applique à l'appareil. Par défaut, la version n'est pas indiquée.

- Taille de bit du système d'exploitation

  Dans la liste déroulante, vous pouvez sélectionner l'architecture du système d'exploitation qui détermine la manière dont la règle de déplacement est appliquée à l'appareil (**Inconnu**, **x86**, **AMD64** ou **IA64**). Par défaut, aucune option n'est sélectionnée dans la liste, l'architecture du système d'exploitation n'est pas définie.

- Version du système d'exploitation

  Ce paramètre concerne uniquement les systèmes d'exploitation Windows.

  Le numéro de version du système d'exploitation. Vous pouvez indiquer si le système d'exploitation sélectionné doit avoir un numéro de version égal, antérieur ou supérieur. Vous pouvez également configurer la recherche de tous les numéros de version à l'exception du numéro indiqué.

- Numéro de version du système d'exploitation

  Ce paramètre concerne uniquement les systèmes d'exploitation Windows.

  L'identifiant de version du système d'exploitation. Vous pouvez indiquer si le système d'exploitation sélectionné doit avoir un ID de version égal, antérieur ou supérieur. Vous pouvez également configurer la recherche de tous les ID de version à l'exception du numéro indiqué.

La section **Machines virtuelles** permet de configurer les critères d'inclusion des appareils dans une sélection selon qu'il s'agit de machines virtuelles ou d'appareils inclus dans une infrastructure de type Virtual Desktop Infrastructure (VDI) :

- Est une machine virtuelle

  La liste déroulante permet de sélectionner les éléments suivants :

  - **Non défini**.
  - **Non**. Les appareils recherchés ne doivent pas être des machines virtuelles.
  - **Oui**. Les appareils recherchés doivent être des machines virtuelles.

- Type d'une machine virtuelle

  La liste déroulante permet de sélectionner le fabricant de la machine virtuelle.

  Cette liste déroulante est disponible si les valeurs **Oui** ou **Ignorer** sont sélectionnées dans la liste déroulante **Est une machine virtuelle**.

- Membre d'une Virtual Desktop Infrastructure

  La liste déroulante permet de sélectionner les éléments suivants :

  - **Non défini**.
  - **Non**. Les appareils recherchés ne doivent pas faire partie de Virtual Desktop Infrastructure.
  - **Oui**. Les appareils recherchés doivent faire partie de Virtual Desktop Infrastructure (VDI).

La sous-section **Registre du matériel** permet de configurer les critères d'inclusion des appareils dans une sélection sur la base du matériel installé :

Assurez-vous que l'utilitaire lshw est installé sur les appareils Linux à partir desquels vous souhaitez récupérer les détails du matériel. Les détails du matériel récupérés depuis les machines virtuelles peuvent être incomplets en fonction de l'hyperviseur utilisé.

- Appareil

  La liste déroulante permet de sélectionner le type d'unité. Tous les appareils avec cette unité sont inclus dans les résultats de la recherche.

  Le champ prend en charge la recherche en texte intégral.

- Éditeur

  La liste déroulante permet de sélectionner le fabricant de la machine virtuelle. Tous les appareils avec cette unité sont inclus dans les résultats de la recherche.

  Le champ prend en charge la recherche en texte intégral.

- **Nom de l'appareil**

  Nom de l'appareil dans le réseau Windows. L'appareil portant le nom indiqué est repris dans la sélection.

- **Description**

  Description de l'appareil ou du matériel. Les appareils dont la description figure dans le champ seront inclus dans la sélection.

  La description de l'appareil peut être librement saisie dans la fenêtre des propriétés. Le champ prend en charge la recherche en texte intégral.

- **Fabricant d'appareil**

  Nom du fabricant de l'appareil. Les appareils du fabricant figurant dans le champ seront inclus dans la sélection.

  Le nom du fabricant peut être saisi dans la fenêtre des propriétés de l'appareil.

- **Numéro de série**

  Le matériel dont le numéro de série figure dans le champ sera inclus dans la sélection.

- **Numéro d'inventaire**

  Le matériel dont le numéro d'inventaire figure dans le champ sera inclus dans la sélection.

- **Utilisateur**

  Le matériel de l'utilisateur figurant dans le champ sera inclus dans la sélection.

- **Emplacement**

  Emplacement de l'appareil ou du matériel (par exemple dans le bureau ou dans la filiale). Les ordinateurs ou les autres appareils dont l'emplacement figure dans le champ seront inclus dans la sélection.

  L'emplacement de l'appareil peut être librement saisi dans la fenêtre des propriétés du matériel.

- **Fréquence du processeur, en MHz, à partir de**

  La fréquence d'horloge minimale d'un processeur. Les appareils dont le processeur correspond à la plage de fréquences d'horloge indiquée dans les champs de saisie (inclus) seront inclus dans la sélection.

- **Fréquence du processeur, en MHz, jusqu'à**

  La fréquence d'horloge maximale d'un processeur. Les appareils dont le processeur correspond à la plage de fréquences d'horloge indiquée dans les champs de saisie (inclus) seront inclus dans la sélection.

- Nombre de processeurs virtuels, à partir de

  Nombre minimal de cœurs de processeur virtuel. Les appareils avec un processeur qui correspond à la plage du nombre de cœurs virtuels spécifié dans les champs de saisie (inclus) seront inclus dans la sélection.

- Nombre de processeurs virtuels, jusqu'à

  Nombre maximal de cœurs de processeur virtuel. Les appareils avec un processeur qui correspond à la plage du nombre de cœurs virtuels spécifié dans les champs de saisie (inclus) seront inclus dans la sélection.

- Volume du disque dur (Go)

  Le volume minimal du disque dur de l'appareil. Les appareils avec un disque dur qui correspond à la plage de volume spécifiée dans les champs de saisie (inclus) seront inclus dans la sélection.

- Volume du disque dur (Go)

  Le volume maximal du disque dur de l'appareil. Les appareils avec un disque dur qui correspond à la plage de volume spécifiée dans les champs de saisie (inclus) seront inclus dans la sélection.

- Taille de la RAM (Mo) à partir de

  La taille minimale de la mémoire vive de l'appareil. Les appareils dont la mémoire vive correspond à la plage de tailles indiquée dans les champs de saisie (incluse) seront inclus dans la sélection.

- Taille de la RAM (Mo) jusqu'à

  La taille maximale de la mémoire vive de l'appareil. Les appareils dont la mémoire vive correspond à la plage de tailles indiquée dans les champs de saisie (incluse) seront inclus dans la sélection.

Détails des logiciels tiers

La sous-section **Registre des applications** permet de configurer les critères d'inclusion d'appareils dans une sélection sur la base des applications installées :

- Nom de l'application

  La liste déroulante qui permet de sélectionner l'application. Les appareils avec l'application indiquée installée seront inclus dans la sélection.

- Version de l'application

  Le champ de saisie à indiquer la version de l'application sélectionnée.

- Éditeur

  La liste déroulante qui permet de sélectionner l'éditeur de l'application installée sur l'appareil.

- État de l'application

  La liste déroulante qui permet de sélectionner l'état de l'application (*Installé*, *Non installé*). Les appareils sur lesquels l'application indiquée est installée ou non sont inclus dans la sélection en fonction de l'état sélectionné.

- Rechercher selon la mise à jour

  Si l'option est activée, la recherche sera exécutée selon les informations présentes dans les mises à jour des applications installées sur les appareils concernés. Une fois que vous avez sélectionné la case à cocher, les champs **Nom de l'application**, **Version de l'application** et **État de l'application** se changent respectivement en **Nom de la mise à jour**, **Version de la mise à jour** et **État**.

  Cette option est Inactif par défaut.

- Nom de l'application de sécurité incompatible

  La liste déroulante qui permet de sélectionner les applications antivirus des éditeurs tiers. Les appareils avec l'application sélectionnée installée seront inclus dans la sélection pendant la recherche.

- Tag de l'application

  La liste déroulante permet de sélectionner le tag de l'application. Tous les appareils sur lesquels sont installés des applications dont la description contient le tag sélectionné, sont repris dans la sélection d'appareils.

- Appliquer aux appareils sans les tags sélectionnés

  Si cette option est activée, la sélection inclut des appareils ne contenant aucun des tags sélectionnés.

  Si l'option est désactivée, les critères ne sont pas appliqués.

  Cette option est Inactif par défaut.

La sous-section **Vulnérabilités et mises à jour** permet de définir les critères d'inclusion d'appareils dans une sélection sur la base de leur source de Windows Update :

WUA est transféré sur le Serveur d'administration

Dans la liste déroulante, vous pouvez sélectionner une des options de recherche suivantes :

- **Oui**. Si cette option a été sélectionnée, les appareils qui reçoivent les mises à jour Windows Update depuis le Serveur d'administration sont inclus dans les résultats de recherche.
- **Non**. Si cette option a été sélectionnée, les appareils qui reçoivent les mises à jour Windows Update depuis une autre source sont inclus dans les résultats de recherche.

Détails sur les applications Kaspersky

La sous-section **Applications Kaspersky** permet de configurer les critères d'inclusion des appareils dans une sélection sur la base de l'application administrée sélectionnée :

- Nom de l'application

  Liste déroulante qui permet de sélectionner les critères d'inclusion des appareils dans la sélection dans le cadre d'une recherche selon le nom de l'application de Kaspersky.

  La liste ne fournit que le nom des applications disposant de plug-ins d'administration installés sur le poste de travail de l'administrateur.

  Si l'application n'est pas sélectionnée, les critères ne sont pas appliqués.

- Version de l'application

  Champ qui permet de saisir les critères d'inclusion des appareils dans la sélection lors de la recherche par numéro de version de l'application de Kaspersky.

  Si le numéro de version n'est pas indiqué, les critères ne sont pas appliqués.

- Nom de la mise à jour critique

  La liste déroulante qui permet de sélectionner l'état de l'application (*Installé*, *Non installé*). Les appareils sur lesquels l'application indiquée est installée ou non sont inclus dans la sélection en fonction de l'état sélectionné.

  Champ de saisie qui permet de saisir les critères d'inclusion des appareils dans la sélection lors de la recherche du paquet de mise à jour installé pour l'application par nom ou numéro.

  Si le champ n'est pas rempli, les critères ne sont pas appliqués.

- Sélectionnez la période de la dernière mise à jour des modules

  Cette option permet de définir les critères de recherche d'appareils selon l'heure de la dernière mise à jour des modules des applications installées sur les appareils.

  Si la case est cochée, le champ de saisie permet d'indiquer les valeurs de l'intervalle de temps (date et heure), durant lequel la dernière mise à jour des modules des applications installées sur les appareils a été effectuée.

  Si la case est décochée, le critère ne sera pas appliqué.

  Celle-ci est décochée par défaut.

- L'appareil est administré via le Serveur d'administration

  La liste déroulante permet d'inclure les appareils qui sont administrés via Kaspersky Security Center dans la sélection d'appareils :

  - **Oui**. L'application ajoute les appareils administrés via Kaspersky Security Center à la sélection d'appareils.
  - **Non**. L'application inclut les appareils dans la sélection s'ils ne sont pas administrés via Kaspersky Security Center.
  - **La valeur n'est pas sélectionnée**. Les critères ne sont pas appliqués.

- L'application de sécurité est installée

  La liste déroulante permet d'ajouter à la sélection d'appareils ceux sur lesquels l'application de sécurité est installée :

  - **Oui**. L'application inclut les appareils sur lesquels l'application de sécurité est installée dans la sélection d'appareils.
  - **Non**. L'application inclut les appareils sur lequel l'application de sécurité n'est pas installée dans la sélection d'appareils.
  - **La valeur n'est pas sélectionnée**. Les critères ne sont pas appliqués.

La sous-section **Endpoint Protection** permet de configurer les critères d'inclusion d'appareils dans une sélection sur la base de leur état de la protection :

- Date de publication des bases

  Si l'option est activée, la recherche d'appareils clients s'exécute selon la date de publication des bases antivirus. Les champs de saisies permettent d'indiquer l'intervalle de temps sur la base duquel la recherche aura lieu.

  Cette option est Inactif par défaut.

- Nombre d'enregistrements dans les bases

  Si l'option est activée, la recherche d'appareils clients s'exécute en fonction du nombre d'enregistrements dans la base de données. Les champs de saisie permettent d'indiquer les valeurs inférieures et supérieures du nombre d'enregistrements.

  Cette option est Inactif par défaut.

- **Dernière analyse**

  Si l'option est activée, la recherche d'appareils clients s'exécute en fonction de l'heure de la dernière analyse des logiciels malveillants. Les champs de saisie permettent d'indiquer l'intervalle durant lequel la dernière analyse des logiciels malveillants a été exécutée.

  Cette option est Inactif par défaut.

- **Menaces détectées**

  Si l'option est activée, la recherche d'appareils clients s'exécute en fonction du nombre de virus sélectionné. Les champs de saisie permettent d'indiquer les valeurs inférieures et supérieures du nombre de virus découverts.

  Cette option est Inactif par défaut.

La sous-section **Chiffrement** vous permet de configurer le critère d'inclusion des appareils dans une sélection en fonction de l'algorithme de chiffrement sélectionné :

Algorithme de chiffrement

Standard d'algorithme de chiffrement symétrique par bloc Advanced Encryption Standard (AES). La liste déroulante permet de sélectionner la taille de la clé de chiffrement (56, 128, 192 ou 256 bits).

Les valeurs possibles sont *AES56*, *AES128*, *AES192*, *AES256*.

La sous-section **Modules de l'application** contient la liste des modules des applications pour lesquelles les plug-ins d'administration correspondants sont installés dans Kaspersky Security Center Cloud Console.

La sous-section **Modules de l'application** permet de définir les critères d'inclusion des appareils dans une sélection sur la base des états et des numéros de version des modules faisant référence à l'application que vous avez sélectionnée :

- **État**

  Recherchez les appareils selon les états des modules renvoyés par une application au Serveur d'administration. Vous pouvez sélectionner l'un des états suivants : *N/A, Arrêté*, *En pause*, *Lancement*, *En cours d'exécution, Échec*, *Non installé, Non pris en charge par la licence*. Si le module sélectionné de l'application installée sur un appareil administré possède l'état indiqué, l'appareil est repris dans la sélection d'appareils.

  États envoyés par les applications :

  - *Arrêté* : le module est désactivé et ne fonctionne pas pour l'instant.
  - *Suspendu* : le module est suspendu, par exemple, après que l'utilisateur a suspendu la protection dans l'application administrée.
  - *En cours de démarrage* : l'initialisation du module est actuellement en cours.
  - *En cours d'exécution* : le module est activé et fonctionne correctement.
  - *Échec* : une erreur s'est produite lors de l'opération du module.
  - *Non installé* : l'utilisateur n'a pas sélectionné le module en vue de l'installer lors de la configuration de l'installation personnalisée de l'application.
  - *Non pris en charge par la licence* : la licence ne couvre pas le module sélectionné.

  À la différence des autres états, l'état *N/A* n'est pas envoyé par les applications. Cette option indique que les applications n'ont aucune information sur l'état du module sélectionné. Cela peut se produire, par exemple, quand le module sélectionné n'appartient à aucune des applications installées sur l'appareil ou quand l'appareil est éteint.

- **Version**

  Recherchez les appareils en fonction du numéro de version du module que vous avez sélectionné dans la liste. Vous pouvez taper un numéro de version, par exemple `3.4.1.0`, puis indiquez si le numéro de version du module sélectionné doit être égal, antérieur ou postérieur. Vous pouvez également configurer la recherche de toutes les versions à l'exception du numéro indiqué.

Tags

La section **Tags** permet de configurer les critères d'inclusion des appareils dans une sélection sur la base des mots clés (tags) ajoutés au préalable aux descriptions des appareils administrés :

Appliquer si au moins un tag sélectionné coïncide

Si l'option est activée, les appareils dont la description contient au moins l'un des tags sélectionnés figureront dans les résultats de la recherche.

Si l'option est désactivée, seuls les appareils dont la description contient l'ensemble des tags sélectionnés figureront dans les résultats de la recherche.

Cette option est Inactif par défaut.

Pour ajouter des tags au critère, cliquez sur le bouton **Ajouter** et sélectionnez les tags en cliquant dans le champ de saisie **Tag**. Indiquez s'il faut inclure ou exclure les appareils avec les tags sélectionnés dans la sélection d'appareils.

- **Tous les appareils qui présentent ce tag**

  Si vous avez choisi cette option, les résultats de la recherche reprennent les appareils dont la description contient le tag sélectionné. Dans le cadre de la recherche d'appareils, vous pouvez utiliser le caractère * qui remplace n'importe quelle chaîne quel que soit le nombre de caractères.

  Cette option est sélectionnée par défaut.

- **Tous les appareils qui ne présentent pas ce tag**

  Si vous avez choisi cette option, les résultats de la recherche reprennent les appareils dont la description ne contient pas le tag sélectionné. Dans le cadre de la recherche d'appareils, vous pouvez utiliser le caractère * qui remplace n'importe quelle chaîne quel que soit le nombre de caractères.

Utilisateurs

La section **Utilisateurs** permet de configurer les critères d'inclusion des appareils dans une sélection sur la base des comptes utilisateurs utilisés pour ouvrir la session dans le système d'exploitation.

- **Dernier utilisateur ayant accédé au système**

  Si cette option est activée, vous pouvez sélectionner le compte pour configurer le critère. Les résultats de la recherche incluent les appareils sur lesquels l'utilisateur sélectionné a effectué la dernière connexion au système.

- **Utilisateur ayant accédé au moins une fois au système**

  Si l'option est activée, cliquez sur le bouton **Parcourir** pour définir un compte utilisateur. Les résultats de recherche comprennent les appareils sur lesquels l'utilisateur indiqué a déjà accédé au système.

Exportation de la liste des appareils à partir d'une sélection d'appareils

Kaspersky Security Center vous permet d'enregistrer des informations sur les appareils à partir d'une sélection d'appareils et de les exporter sous forme de fichier CSV ou TXT.

Pour exporter la liste des appareils à partir de la sélection d'appareils, procédez comme suit :

1. Ouvrez le tableau avec les appareils de la sélection d'appareils.
2. Choisissez un des moyens suivants les appareils que vous souhaitez exporter :
   - Pour sélectionner certains appareils, cochez la case en regard de celui-ci.
   - Pour sélectionner tous les appareils à partir de la page actuelle du tableau, cochez la case dans l'en-tête du tableau des appareils, puis cochez la case **Tout sélectionner sur la page actuelle**.
   - Pour sélectionner tous les appareils dans le tableau, cochez la case dans l'en-tête du tableau des appareils, puis cochez la case **Tout sélectionner**.
3. Cliquez sur le bouton **Exporter vers un fichier CSV** ou **Exporter vers un fichier TXT**. Toutes les informations sur les appareils sélectionnés inclus dans le tableau seront exportées.

Notez que si vous avez appliqué un critère de filtre à la table des appareils, seules les données filtrées des colonnes affichées seront exportées.

Suppression des appareils depuis les groupes d'administration dans la sélection

Lors de l'utilisation de la sélection d'appareils, vous pouvez supprimer les appareils des groupes d'administration directement dans la sélection sans avoir à supprimer les appareils des groupes d'administration.

Pour supprimer les appareils depuis les groupes d'administration, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Sélections d'appareils** ou **Découverte et déploiement** → **Sélections d'appareils**.
2. Dans la liste de sélection, cliquez sur le nom de la sélection d'appareils.

   La page affiche un tableau avec des informations sur les appareils inclus dans la sélection d'appareils.
3. Sélectionnez les appareils que vous souhaitez supprimer, puis cliquez sur **Supprimer**.

   Finalement, les appareils sélectionnés seront supprimés depuis les groupes d'administration dont ils faisaient partie.

Tags de l'appareil

Kaspersky Security Center permet de désigner les *tags* pour les appareils. Un tag est un identificateur de l'appareil et il peut être utilisé pour regrouper, décrire ou rechercher des appareils. Les tags désignés pour les appareils peuvent être utilisés lors de la création de sélections d'appareils, lors de la recherche d'appareils et lors de la répartition d'appareils en groupes d'administration.

Les tags peuvent être désignés pour les appareils manuellement ou automatiquement. Si vous souhaitez attribuer un tag à un seul appareil, vous pouvez utiliser un tag manuel. L'attribution automatique de tags est exécutée par Kaspersky Security Center d'une des manières suivantes :

- Conformément aux règles définies d'attribution des tags.
- Par une application.

Il est déconseillé d'utiliser différents tags pour attribuer un même tag. Par exemple, si le tag est attribué par la règle, il n'est pas recommandé d'attribuer manuellement ce tag aux appareils.

Si les tags sont attribués par des règles, des tags sont automatiquement attribués aux appareils lorsque les règles spécifiées sont remplies. A chaque tag correspond une règle distincte. Les règles peuvent être appliquées aux propriétés réseau de l'appareil, au système d'exploitation de l'appareil, aux applications installées sur l'appareil ou à d'autres propriétés de l'appareil. Admettons que vous disposiez d'une structure hybride composée de machines physiques, d'instances Amazon EC2 et de machines virtuelles Microsoft Azure, vous pouvez créer une règle qui attribuera le tag `[Azure]` à toutes les machines virtuelles Microsoft Azure. Vous pouvez utiliser ensuite ce tag dans la création d'une sélection d'appareils et cela vous aidera à trier toutes les machines virtuelles Microsoft Azure et à leur attribuer une tâche.

Vous ne pouvez ajouter qu'une seule règle de balisage automatique par balise. Si vous créez une nouvelle règle pour la même balise, la règle précédente sera remplacée.

Un tag est automatiquement supprimé d'un appareil dans les cas suivants :

- Dès que l'appareil cesse de remplir les conditions de la règle qui attribue le tag.
- Lorsque la règle qui attribue la balise est désactivée ou supprimée.

La liste des tags et la liste des règles sur chaque Serveur d'administration sont indépendantes de tous les autres Serveurs d'administration, y compris du Serveur d'administration principal ou des Serveurs d'administration secondaires virtuels. Une règle est appliquée uniquement aux appareils du même Serveur d'administration sur lequel la règle est créée.

Création d'un tag de l'appareil

Pour créer un tag de l'appareil, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Tags** → **Tags de l'appareil**.
2. Cliquez sur **Ajouter**.

   Une fenêtre de nouveau tag s'ouvre.
3. Dans le champ **Tag**, saisissez le nom du tag.
4. Cliquez sur le bouton **Enregistrer** afin d'enregistrer les modifications.

   Le nouveau tag apparaît dans la liste des tags de l'appareil.

Renommage d'un tag de l'appareil

Pour renommer un tag de l'appareil, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Tags** → **Tags de l'appareil**.
2. Cliquez le nom du tag que vous souhaitez modifier.

   Une fenêtre de propriété du tag s'ouvre.
3. Dans le champ **Tag**, modifiez le nom du tag.
4. Cliquez sur le bouton **Enregistrer** afin d'enregistrer les modifications.

Le tag mis à jour apparaît dans la liste des tags de l'appareil.

Suppression d'un tag de l'appareil

Pour supprimer un tag de l'appareil, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Tags** → **Tags de l'appareil**.
2. Dans la liste, sélectionnez le tag de l'appareil que vous souhaitez supprimer.
3. Cliquez sur le bouton **Supprimer**.
4. Dans la fenêtre qui s'ouvre, cliquez sur **Oui**.

Le tag de l'appareil est supprimé. Le tag supprimé est automatiquement retiré de tous les appareils auxquels il était attribué.

Le tag que vous avez supprimé n'est pas automatiquement supprimé des règles d'attribution automatique de tags. Une fois le tag supprimé, il est attribué à un nouvel appareil seulement lorsque l'appareil répond tout d'abord aux conditions d'une règle qui attribue le tag.

Le tag supprimé n'est pas supprimé automatiquement de l'appareil si ce tag est attribué à l'appareil par une application ou un Agent d'administration. Pour supprimer le tag de votre appareil, utilisez l'utilitaire klscflag.

Affichage des appareils ayant reçu un tag

Pour voir les appareils auxquels un tag a été attribué, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Tags** → **Tags de l'appareil**.
2. Cliquez sur le lien **Consulter les appareils** en regard du tag pour lequel vous souhaitez voir les appareils associés.

   Vous serez redirigé vers la section **Appareils administrés** du menu principal, avec les appareils filtrés en fonction du tag pour lequel vous avez cliqué sur le lien **Consulter les appareils**.
3. Pour revenir à la liste des tags de l'appareil, cliquez sur le bouton **Retour** de votre navigateur.

Après avoir consulté les appareils auxquels le tag est attribué, vous pouvez créer et attribuer un nouveau tag ou attribuer le tag existant à d'autres appareils. Dans ce cas, vous devez supprimer le filtre par tag, sélectionner les appareils, puis attribuer le tag.

Consultation des tags attribués à un appareil

Pour voir les tags attribués à un appareil :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Appareils administrés**.
2. Cliquez sur le nom de l'appareil dont vous souhaitez voir les tags.
3. Dans la fenêtre des propriétés de l'appareil qui s'ouvre, sélectionnez l'onglet **Tags**.

   La liste des tags attribués à l'appareil sélectionné s'affiche. La colonne **Tag défini** permet de consulter la manière dont le tag a été attribué.

Dans la barre d'outils, vous pouvez effectuer l'une des opérations suivantes :

- Attribuez un autre tag à l'appareil.
- Supprimez un tag déjà attribué.
- Affichez tous les tags de l'appareil qui existent sur le Serveur d'administration.

Vous ne pouvez pas afficher les tags attribués localement sur l'appareil.

Attribution manuelle d'un tag à un appareil

Pour attribuer un tag manuellement à un appareil, procédez comme suit :

1. Consultez les tags attribués à l'appareil auquel vous souhaitez attribuer un autre tag.
2. Cliquez sur **Ajouter**.

3. Dans la fenêtre qui s'ouvre, réalisez une des opérations suivantes :

   - Pour créer un tag et l'attribuer, sélectionnez **Créer un tag**, puis renseignez le nom du nouveau tag.
   - Pour sélectionner un tag existant, sélectionnez **Attribuer un tag existant**, puis sélectionnez le tag nécessaire dans la liste déroulante.

4. Cliquez sur le bouton **OK** pour appliquer les modifications.
5. Cliquez sur le bouton **Enregistrer** afin d'enregistrer les modifications.

Le tag sélectionné est attribué à l'appareil.

Suppression d'un tag attribué à un appareil

Pour supprimer un tag attribué à un appareil, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Appareils administrés**.
2. Cliquez sur le nom de l'appareil dont vous souhaitez voir les tags.
3. Dans la fenêtre des propriétés de l'appareil qui s'ouvre, sélectionnez l'onglet **Tags**.
4. Cochez la case en regard du tag que vous souhaitez supprimer.
5. En haut de la liste, cliquez sur le bouton **Désattribuer un tag ?**.
6. Dans la fenêtre qui s'ouvre, cliquez sur **Oui**.

Le tag est supprimé de l'appareil.

Le tag de l'appareil non défini n'est pas supprimé. Si vous le voulez, vous pouvez le supprimer manuellement.

Vous ne pouvez pas supprimer manuellement les tags attribués à l'appareil par les applications ou l'Agent d'administration. Pour supprimer ces tags, utilisez l'utilitaire klscflag.

Consultation des règles pour l'attribution automatique de tags aux appareils

Pour consulter les règles d'attribution automatique de tags aux appareils, procédez comme suit :

Réalisez une des opérations suivantes :

- Dans le menu principal, accédez à **Ressources (Appareils)** → **Tags** → **Règles d'attribution automatique de tags**.
- Dans le menu principal, accédez à **Ressources (Appareils)** → **Tags** → **Tags de l'appareil**, puis cliquez sur le lien **Configurer les règles d'attribution automatique de tags**.
- Consultez les tags attribués à un appareil, puis cliquez sur le bouton **Paramètres**.

La liste des règles d'attribution automatique de tags aux appareils s'affiche.

Modification d'une règle d'attribution automatique de tags aux appareils

Pour éditer une règle d'attribution automatique de tags aux appareils, procédez comme suit :

1. Consultez les règles pour l'attribution automatique de tags aux appareils.
2. Cliquez sur le nom de la règle que vous souhaitez modifier.

   Une fenêtre de paramètres de la règle s'ouvre.
3. Modifiez les propriétés générales de la règle :

   a. Dans le champ **Nom de la règle**, modifiez le nom de la règle.

   Le nom ne peut pas contenir plus de 256 caractères.

   b. Réalisez une des opérations suivantes :

   - Activez la règle en basculant le commutateur sur **Règle activée**.
   - Désactivez la règle en basculant le commutateur sur **Règle désactivée**.
4. Réalisez une des opérations suivantes :

   - Si vous souhaitez ajouter une nouvelle condition, cliquez sur le bouton **Ajouter** et définissez les paramètres de la nouvelle condition dans la fenêtre qui s'ouvre.
   - Si vous souhaitez modifier une condition existante, cliquez sur le nom de la condition que vous voulez modifier, puis modifiez les paramètres de la condition.
   - Si vous souhaitez supprimer une condition, cochez la case en regard du nom de la condition que vous souhaitez supprimer, puis cliquez sur **Supprimer**.
5. Cliquez sur **OK** dans la fenêtre des paramètres de conditions.
6. Cliquez sur le bouton **Enregistrer** afin d'enregistrer les modifications.

La règle modifiée apparaît dans la liste.

Création d'une règle d'attribution automatique de tags aux appareils

Pour créer une règle d'attribution automatique de tags aux appareils, procédez comme suit :

1. Consultez les règles pour l'attribution automatique de tags aux appareils.
2. Cliquez sur **Ajouter**.

   Une fenêtre de paramètres de nouvelle règle s'ouvre.

3. Configurez les propriétés générales de la règle :

   a. Dans le champ **Nom de la règle**, saisissez le nom de la règle.

      Le nom ne peut pas contenir plus de 256 caractères.

   b. Exécutez une des actions suivantes :

      - Activez la règle en basculant le commutateur sur **Règle activée**.
      - Désactivez la règle en basculant le commutateur sur **Règle désactivée**.

   c. Dans le champ **Tag**, saisissez le nouveau nom du tag de l'appareil ou sélectionnez un tag parmi ceux de la liste.

      Le nom ne peut pas contenir plus de 256 caractères.

4. Dans la section des conditions, cliquez sur le bouton **Ajouter** pour ajouter une nouvelle condition.

   La fenêtre des paramètres de la nouvelle condition s'ouvre.

5. Saisissez le nom de la condition.

   Le nom ne peut pas contenir plus de 256 caractères. Le nom doit être unique au sein d'une règle.

6. Configurez le déclenchement de la règle d'appareils selon les conditions suivantes . Il est possible de choisir plusieurs conditions.

   - **Réseau** : propriétés réseau des appareils (par exemple, nom de l'appareil sur le réseau Windows, appartenance de l'appareil au domaine, à un sous-réseau IP).

     Si le classement sensible à la casse est défini pour la base de données que vous utilisez pour Kaspersky Security Center, respectez la casse lorsque vous indiquez le nom DNS de l'appareil. Sinon, la règle de marquage automatique ne fonctionnera pas.

   - **Applications** : présence sur l'appareil de l'Agent d'administration, le type, la version et l'architecture du système d'exploitation.
   - **Machines virtuelles** : l'appareil appartient à un type particulier de machine virtuelle.
   - **Contrôleur de domaine** : présence de l'appareil dans la sous-section Active Directory et appartenance de l'appareil au groupe Active Directory.
   - **Registre des applications** : présence sur l'appareil d'applications de différents éditeurs.

7. Cliquez sur le bouton **OK** afin d'enregistrer les modifications.

   Le cas échéant, il est possible d'attribuer plusieurs catégories à une règle. Dans ce cas, le tag est attribué aux appareils quand au moins une des conditions est remplie.

8. Cliquez sur le bouton **Enregistrer** afin d'enregistrer les modifications.

La règle nouvellement créée est exécutée sur les appareils administrés par le Serveur d'administration sélectionné. Si les paramètres de l'appareil correspondent aux conditions de la règle, cet appareil reçoit ce tag.

Plus tard, la règle est appliquée dans les cas suivants :

- Automatiquement et de manière périodique en fonction de la charge de travail du serveur
- Après que vous avez modifié la règle
- Quand vous exécutez la règle manuellement
- Une fois que le serveur d'administration a détecté une modification des paramètres d'un appareil qui remplit les conditions de la règle ou des paramètres d'un groupe qui contient cet appareil

Vous pouvez créer plusieurs règles d'attribution des tags. Plusieurs tags peuvent être attribués à un appareil si vous aviez créé plusieurs règles et que les conditions d'exécution de ces règles sont remplies simultanément. Vous pouvez consulter la liste de tous les tags attribués dans les propriétés de l'appareil.

Règles d'exécution pour l'attribution automatique de tags aux appareils

Quand une règle est appliquée, le tag défini dans les propriétés de cette règle est attribué aux appareils qui remplissent les conditions définies dans les propriétés de la même règle. Vous pouvez exécuter uniquement des règles actives.

Pour exécuter des règles d'attribution automatique de tags aux appareils, procédez comme suit :

1. Consultez les règles pour l'attribution automatique de tags aux appareils.
2. Cochez les cases en regard des règles activez que vous souhaitez exécuter.
3. Cliquez sur le bouton **Exécuter la règle**.

Les règles sélectionnées s'exécutent.

Suppression d'une règle d'attribution automatique de tags aux appareils

Pour supprimer une règle d'attribution automatique de tags aux appareils, procédez comme suit :

1. Consultez les règles pour l'attribution automatique de tags aux appareils.
2. Cochez les cases en regard de la règle que vous souhaitez supprimer.
3. Cliquez sur **Supprimer**.
4. Dans la fenêtre qui s'ouvre, cliquez une nouvelle fois sur **Supprimer**.

La règle sélectionnée est supprimée. Le tag défini dans les propriétés de cette règle est retiré de tous les appareils auxquels il avait été attribué.

Le tag de l'appareil non défini n'est pas supprimé. Si vous le voulez, vous pouvez le supprimer manuellement.

Gestion des tags d'appareil à l'aide de l'utilitaire klscflag

Pour attribuer un ensemble de balises à un appareil, vous devez exécuter l'utilitaire klscflag sur l'appareil client auquel vous souhaitez attribuer des balises.

L'utilitaire klscflag écrase les balises existantes attribuées à l'appareil. Cela signifie que vous pouvez ajouter ou supprimer des balises en spécifiant l'ensemble de balises souhaité dans la commande. L'utilitaire ne dispose pas de commandes distinctes pour ajouter ou supprimer des balises individuelles. Au lieu de cela, vous modifiez l'ensemble des balises.

Lorsque vous spécifiez des noms de balises dans des commandes telles que klscflag, il est recommandé d'utiliser une approche cohérente de la casse, comme les majuscules. L'utilisation de majuscules permet d'éviter les problèmes potentiels liés à des étiquettes qui ne diffèrent que par la casse, en fonction de la configuration du SGBD.

Pour attribuer des tags à votre appareil à l'aide de l'utilitaire klscflag, procédez comme suit :

1. Exécutez l'invite de commande Windows en utilisant les droits d'administrateur, puis remplacez votre répertoire actuel par celui contenant l'utilitaire klscflag. L'utilitaire klsclag se trouve dans le dossier dans lequel l'Agent d'administration est installé. Chemin d'installation par défaut est <Disk>:\Program Files (x86)\Kaspersky Lab\NetworkAgent.

2. Saisissez l'une des commandes suivantes :

   - Pour attribuer un ensemble de balises :

     ```
     klscflag -ssvset -pv 1103/1.0.0.0 -s KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "[\"TAG NAME 1\",\"TAG NAME 2\",\"TAG NAME 3\"]" -svt ARRAY_T -ss "|ss_type = \"SS_PRODINFO\";"
     ```

     où `[\"TAG NAME 1\",\"TAG NAME 2\",\"TAG NAME 3\"]` est la liste des tags que vous souhaitez attribuer à votre appareil.

     Si vous laissez les crochets vides, cela supprimera toutes les balises de l'appareil :

     ```
     klscflag -ssvset -pv 1103/1.0.0.0 -s KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "[]" -svt ARRAY_T -ss "|ss_type = \"SS_PRODINFO\";"
     ```

   - Pour attribuer une nouvelle balise à un ensemble de balises existant :

     ```
     klscflag -ssvset -pv 1103/1.0.0.0 -s KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "[\"NEW TAG NAME\",\"TAG NAME 1\",\"TAG NAME 2\",\"TAG NAME 3\"]" -svt ARRAY_T -ss "|ss_type = \"SS_PRODINFO\";"
     ```

     où `NEW TAG NAME` est le nom de la balise que vous souhaitez attribuer à votre appareil et `TAG NAME 1`, `TAG NAME 2`, `TAG NAME 3` sont les noms des balises déjà attribuées à l'appareil.

   - Pour supprimer une balise spécifique sans supprimer les autres balises déjà attribuées à l'appareil, exécutez la commande avec l'ensemble de balises mis à jour.

     Par exemple, si vos balises actuelles sont `TAG NAME 1`, `TAG NAME 2`, `TAG NAME 3` et que vous souhaitez supprimer `TAG NAME 2`, exécutez la commande suivante :

     ```
     klscflag -ssvset -pv 1103/1.0.0.0 -s KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "[\"TAG NAME 1\",\"TAG NAME 3\"]" -svt ARRAY_T -ss "|ss_type = \"SS_PRODINFO\";"
     ```

3. Relancez le service de l'Agent d'administration.

   L'utilitaire klscflag attribue les tags définis à votre appareil.

4. Si vous souhaitez vous assurer que l'utilitaire klscflag a bien attribué les tags définis, affichez les tags attribués à l'appareil.

Vous pouvez également attribuer des tags d'appareil manuellement.

Stratégies et profils de stratégie

Kaspersky Security Center Web Console permet de créer des stratégies pour des applications de Kaspersky. Cette section décrit les stratégies et les profils de stratégie et explique comment les créer et les modifier.

Stratégies et profils de stratégies

Une *stratégie* est un ensemble de paramètres d'application Kaspersky qui sont appliqués à un groupe d'administration et à ses sous-groupes. Vous pouvez installer plusieurs applications Kaspersky sur les appareils d'un groupe d'administration. Kaspersky Security Center fournit une stratégie propre à chaque application Kaspersky d'un groupe d'administration. La stratégie possède un des états suivants (voir le tableau ci-dessous) :

L'état de la stratégie

État	Description
Actif	La stratégie actuelle appliquée à l'appareil. Une seule stratégie peut être active pour une application Kaspersky dans chaque groupe d'administration. Les appareils appliquent les valeurs de paramètres d'une stratégie active pour une application Kaspersky.
Inactive	Une stratégie qui n'est actuellement pas appliquée à un appareil.
Pour les utilisateurs itinérants	Si cette option a été sélectionnée, la stratégie agit lorsque l'appareil est déconnecté du réseau de l'entreprise.

Le fonctionnement des stratégies obéit aux règles suivantes :

- Il est possible de configurer plusieurs stratégies avec différentes valeurs pour une seule application.
- Une seule stratégie peut être active pour l'application actuelle.
- Vous pouvez activer une stratégie inactive lorsqu'un événement en particulier se produit. Par exemple, vous pouvez mettre en œuvre des paramètres d'Endpoint Protection plus stricts en cas de propagation de virus.
- Une stratégie peut comporter des stratégies enfants.

En règle générale, vous pouvez utiliser des stratégies pour vous préparer aux situations d'urgence, telles qu'une propagation de virus. Par exemple, en cas d'attaque via les clés USB, vous pouvez activer une stratégie bloquant l'accès aux clés USB. Dans ce cas, la stratégie active actuelle devient automatiquement inactive.

Afin d'éviter une multiplicité de stratégies, par exemple, lorsque des circonstances diverses impliquent la seule modification de plusieurs paramètres, vous pouvez utiliser des profils de stratégie.

Un *profil de stratégie* est un sous-ensemble nommément désigné de valeurs de paramètres de stratégie qui remplace les valeurs de paramètres d'une stratégie. Un profil de stratégie affecte la formation effective des paramètres sur un appareil administré. *Les paramètres effectifs* sont un ensemble de paramètres de stratégie, de paramètres de profil de stratégie et de paramètres d'application locale actuellement appliqués à l'appareil.

Les profils de stratégie fonctionnent conformément aux règles suivantes :

- Un profil de stratégie prend effet lorsqu'une condition d'activation particulière est réalisée.
- Les profils de stratégie contiennent des valeurs de paramètres qui diffèrent des paramètres de stratégie.
- L'activation d'un profil de stratégie modifie les paramètres effectifs de l'appareil administré.
- Une stratégie ne peut pas compter plus de 100 profils de stratégie.

À propos du cadenas et des paramètres verrouillés

Chaque paramètre de stratégie est associé à une icône de bouton de verrouillage (). Le tableau ci-dessous montre les états des boutons de verrouillage :

États de bouton de verrouillage

État	Description
Indéfini	Si une icône de cadenas ouvert s'affiche en regard d'un paramètre alors que le commutateur est désactivé, le paramètre n'est pas spécifié dans la stratégie. Un utilisateur peut modifier ces paramètres dans l'interface de l'application administrée. Les paramètres de ce type sont dits *déverrouillés*.
Verrouillé	Si un cadenas verrouillé s'affiche à côté d'un paramètre et si le commutateur est désactivé, le paramètre est appliqué aux appareils sur lesquels la stratégie est appliquée. Un utilisateur ne peut pas modifier les valeurs de ces paramètres dans l'interface de l'application administrée. Les paramètres de ce type sont dits *verrouillés*.

Nous vous recommandons fortement de fermer les verrous pour les paramètres de stratégie que vous souhaitez appliquer sur les appareils administrés. Les paramètres de stratégie déverrouillés peuvent être réattribués par les paramètres de l'application Kaspersky sur un appareil administré.

Vous pouvez utiliser un bouton de verrouillage pour effectuer les actions suivantes :

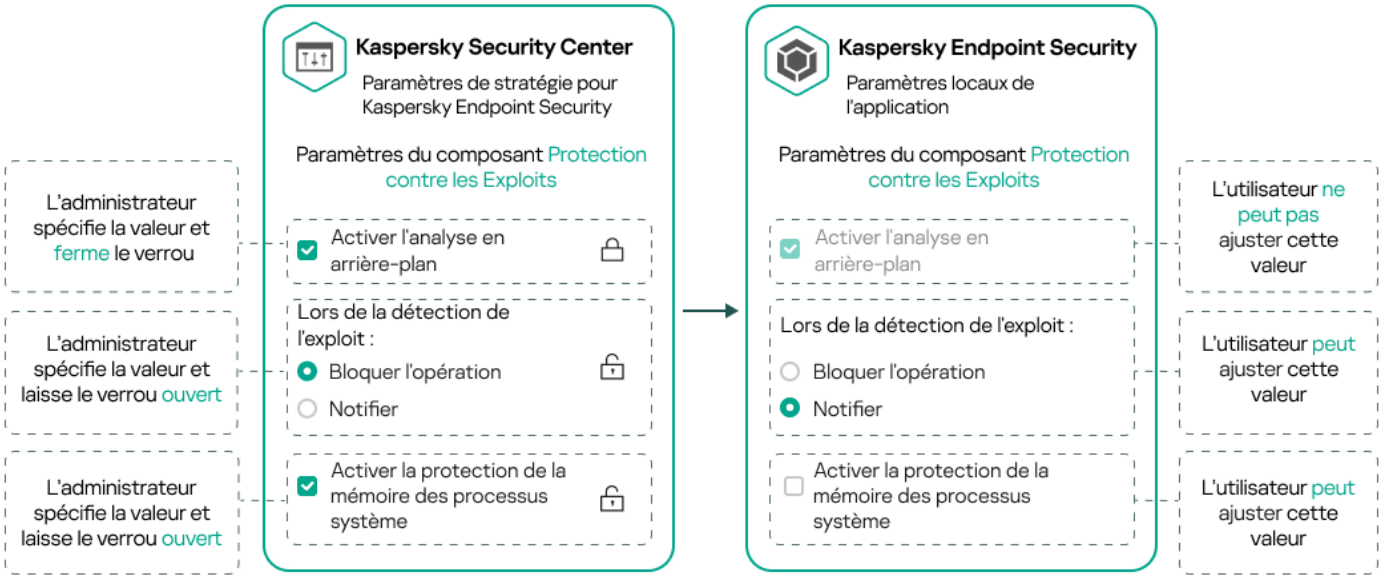
- Paramètres de verrouillage pour une stratégie de sous-groupe d'administration
- Paramètres de verrouillage d'une application Kaspersky sur un appareil administré

Un paramètre verrouillé est ainsi utilisé pour mettre en œuvre des paramètres efficaces sur un appareil administré.

Un processus de mise en œuvre efficace des paramètres comprend les actions suivantes :

- L'appareil administré applique les valeurs des paramètres de l'application Kaspersky.
- L'appareil administré applique les valeurs des paramètres verrouillés d'une stratégie.

Une stratégie et une application Kaspersky administrée contiennent le même ensemble de paramètres. Lorsque vous configurez des paramètres de stratégie, les paramètres de l'application Kaspersky modifient les valeurs sur un appareil administré. Vous ne pouvez pas ajuster les paramètres verrouillés sur un appareil administré (voir le schéma ci-dessous) :



Verrous et paramètres de l'application Kaspersky

Héritage des stratégies, utilisation des profils des stratégies

Cette section comporte des informations sur la hiérarchie et l'héritage des stratégies et des profils de stratégie.

Hiérarchie des stratégies

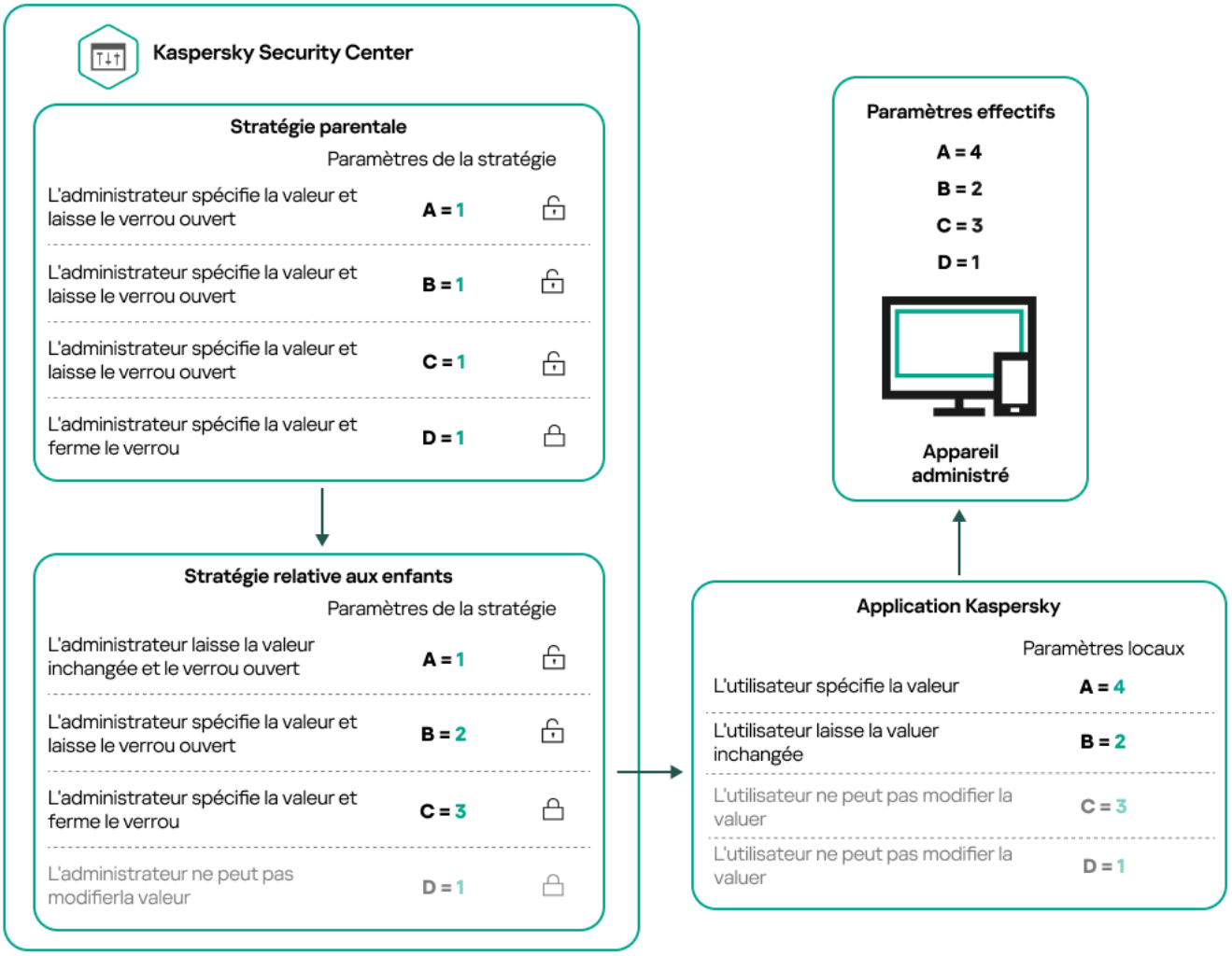
Si des appareils différents requièrent des paramètres différents, vous pouvez organiser les appareils en groupes d'administration.

Vous pouvez spécifier une stratégie pour un seul groupe d'administration. Les paramètres de stratégie peuvent être *hérités*. L'héritage signifie recevoir des valeurs de paramètres de stratégie dans des sous-groupes (groupes enfants) d'une stratégie d'un groupe d'administration de niveau supérieur (parent).

Par la suite, une stratégie pour un groupe parent est également désignée par l'expression *stratégie parent*. Une stratégie pour un sous-groupe (groupe enfant) est également désignée par l'expression *stratégie enfant*.

Par défaut, il existe au moins un groupe d'appareils administrés existe sur le Serveur d'administration. Si vous souhaitez créer des groupes personnalisés, ils sont créés sous forme de sous-groupes (groupes enfants) dans le groupe d'appareils administrés.

Les stratégies d'une même application agissent les unes sur les autres sur la base d'une hiérarchie de groupes d'administration. Les paramètres verrouillés d'une stratégie d'un groupe d'administration de niveau supérieur (parent) réaffecteront les valeurs des paramètres de stratégie d'un sous-groupe (voir la figure ci-dessous).



Hiérarchie des stratégies

Profils de stratégie dans une hiérarchie de stratégies

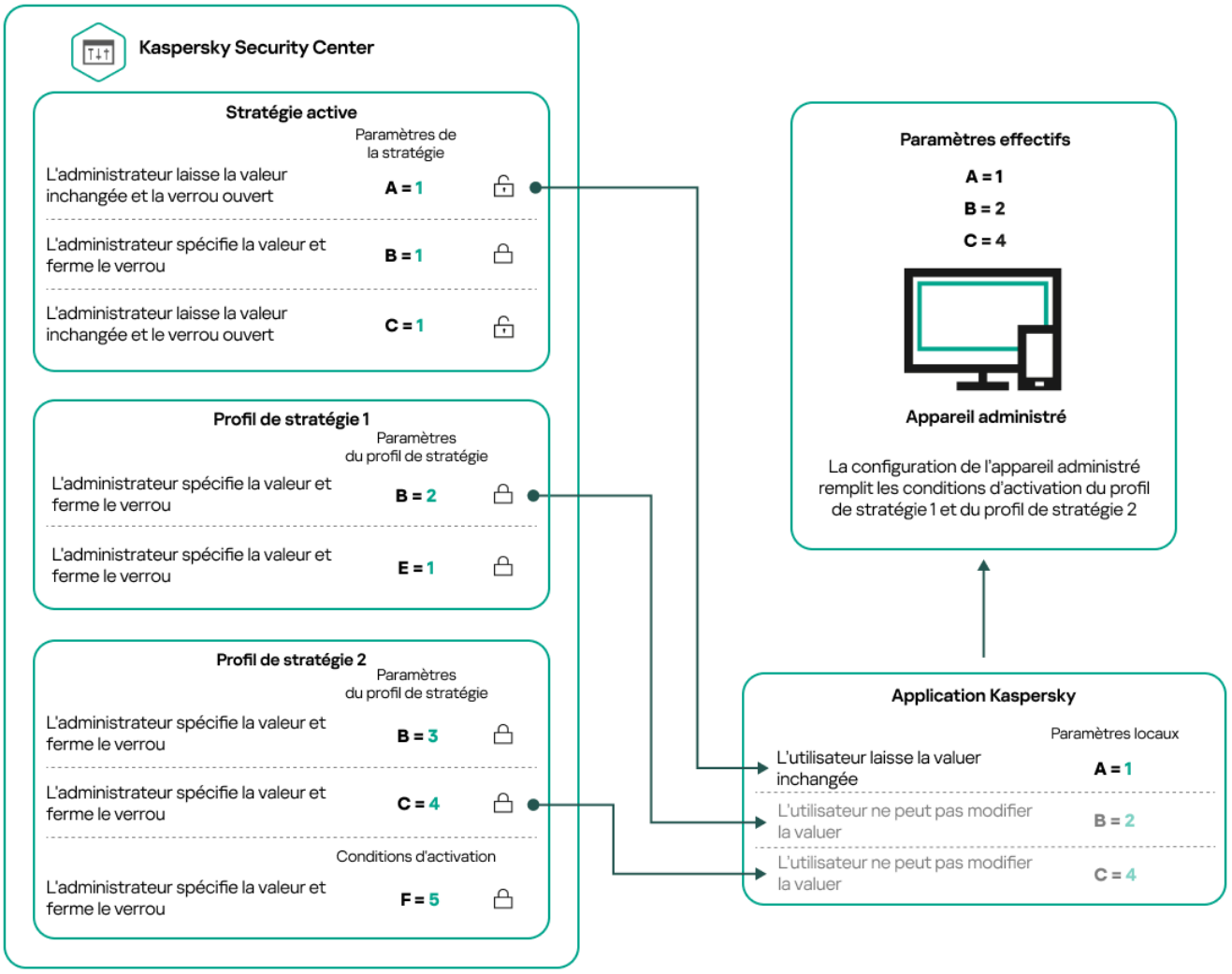
Les conditions d'attribution de priorité des profils de stratégie sont les suivantes :

- la position d'un profil dans une liste de profils de stratégie indique son degré de priorité. Vous pouvez modifier la priorité d'un profil de stratégie. La position la plus élevée dans une liste indique le degré de priorité le plus élevé (voir la figure ci-dessous).

Définition prioritaire d'un profil de stratégie

- Les conditions d'activation des profils de stratégie ne dépendent pas les unes des autres. Plusieurs profils de stratégie peuvent être activés simultanément. Si plusieurs profils de stratégie affectent le même paramètre,

l'appareil sélectionne la valeur de paramètre du profil de stratégie dont la priorité est la plus élevée (voir la figure ci-dessous).

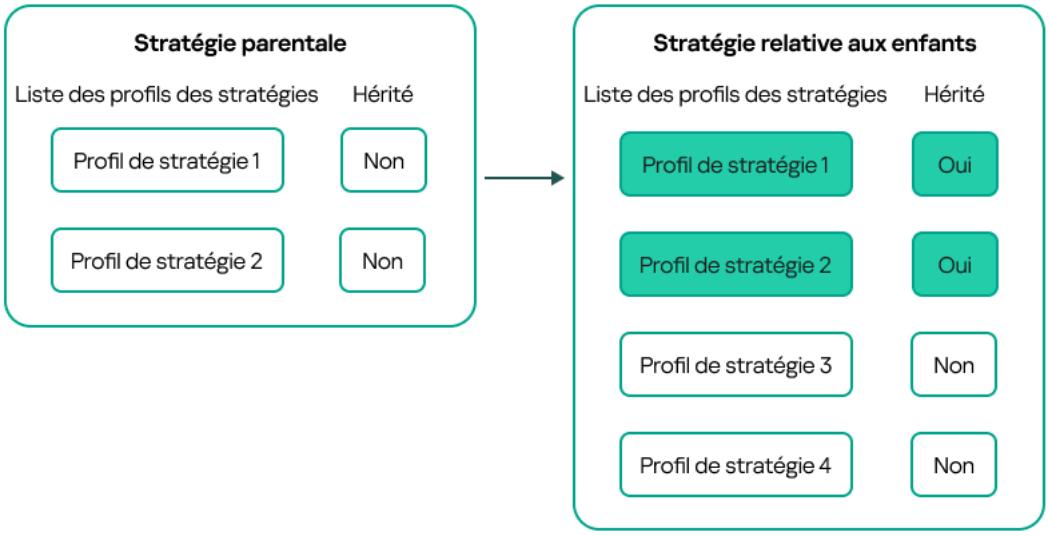


La configuration de l'appareil administré satisfait aux conditions d'activation de plusieurs profils de stratégie

Profils de stratégie dans une hiérarchie d'héritage

Les profils de stratégie de différentes stratégies de niveau hiérarchique sont conformes aux conditions suivantes :

- une stratégie de niveau inférieur hérite des profils de stratégie d'une stratégie de niveau supérieur. Un profil de stratégie hérité d'une stratégie de niveau supérieur obtient une priorité plus élevée que le niveau du profil de stratégie d'origine.
- Vous ne pouvez pas modifier la priorité d'un profil de stratégie hérité (voir la figure ci-dessous).

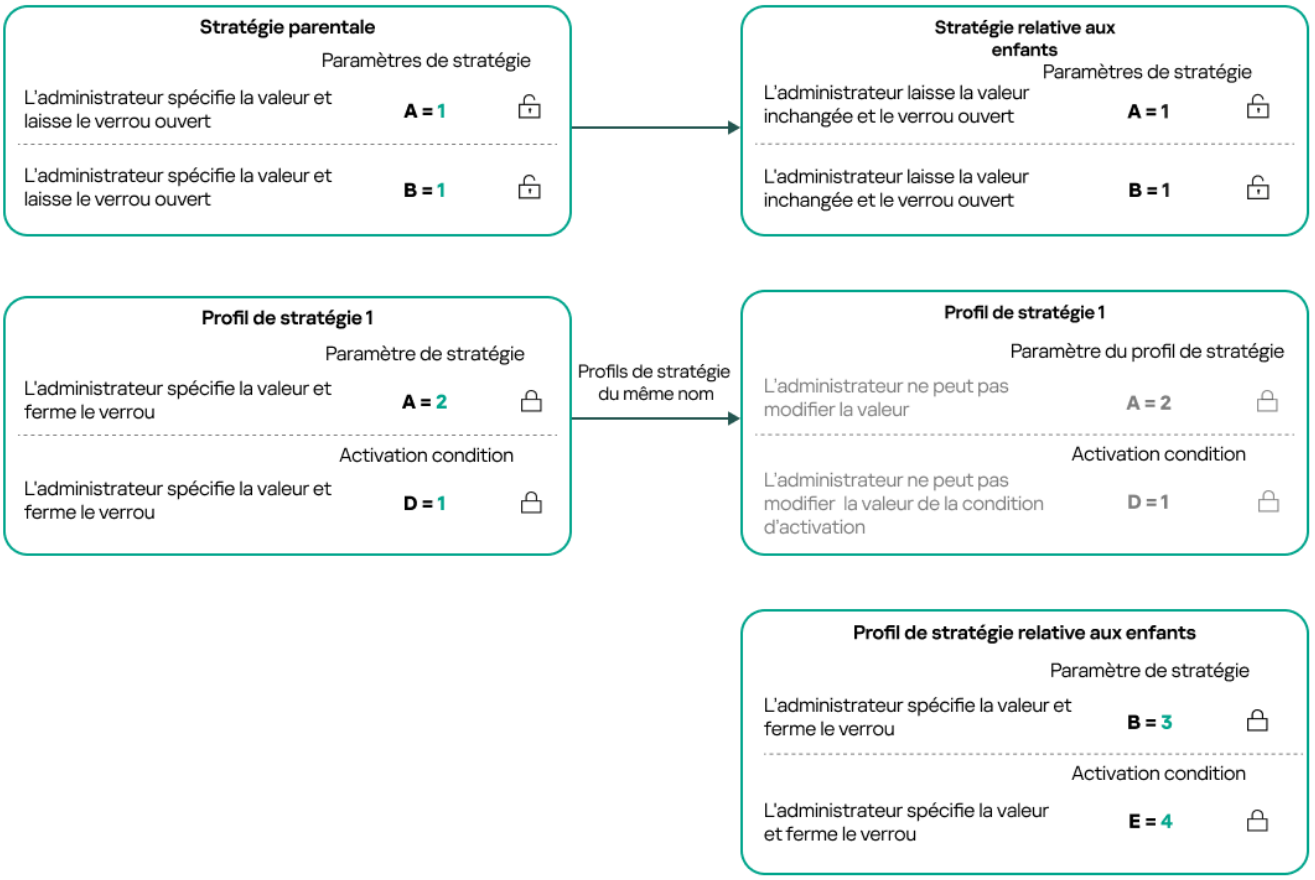


Héritage des profils de stratégie

Profils de stratégie du même nom

S'il existe, à des niveaux hiérarchiques différents, deux stratégies portant le même nom, leur fonctionnement est régi par les règles suivantes :

- Les paramètres verrouillés et la condition d'activation du profil d'un profil de stratégie de niveau supérieur modifient les paramètres et la condition d'activation de profil d'un profil de stratégie de niveau inférieur (voir la figure ci-dessous).



Le profil enfant hérite des valeurs de paramètres d'un profil de stratégie parent

- Les paramètres déverrouillés et la condition d'activation de profil d'un profil de stratégie de niveau supérieur ne modifient pas les paramètres et la condition d'activation de profil d'un profil de stratégie de niveau inférieur.

Comment les paramètres sont mis en œuvre sur un appareil administré

La mise en œuvre des paramètres effectifs sur un appareil administré peut être décrite comme suit :

- les valeurs de tous les paramètres qui n'ont pas été verrouillés sont tirées de la stratégie.
- Ils sont ensuite remplacés par les valeurs des paramètres de l'application administrée.
- Les valeurs des paramètres verrouillés de la stratégie effective sont ensuite appliquées. Les valeurs des paramètres verrouillés modifient celles des paramètres effectifs déverrouillés.

Administration des stratégies

Cette section décrit l'administration des stratégies et comporte des informations sur l'affichage de la liste des stratégies, l'élaboration d'une stratégie, sa modification, sa copie et son déplacement, la synchronisation forcée, l'affichage du graphique d'état de diffusion des stratégies et la suppression de stratégie.

Affichage de la liste des stratégies

Vous pouvez afficher la liste des stratégies créées pour le Serveur d'administration ou pour un groupe d'administration.

Pour consulter la liste des stratégies, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Hiérarchie des groupes**.
2. Dans la structure du groupe d'administration, sélectionnez le groupe d'administration dont vous voulez voir la liste des stratégies.

La liste des stratégies s'affiche dans un tableau. S'il n'y a pas de stratégies, le tableau est vide. Vous pouvez afficher ou masquer les colonnes du tableau, modifier leur ordre, afficher uniquement les lignes qui contiennent une valeur que vous définissez, ou utiliser la recherche.

Création d'une stratégie

Vous pouvez créer des stratégies ; vous pouvez également modifier et supprimer des stratégies existantes.

Pour créer un de stratégie, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Stratégies et profils**.
2. Sélectionnez le groupe d'administration pour lequel la stratégie doit être créée :
   - Pour le groupe racine.

     Dans ce cas, vous pouvez passer à l'étape suivante.
   - Pour un sous-groupe :
     a. Cliquez sur le lien du chemin d'accès actuel dans la partie supérieure de la fenêtre.
     b. Dans le panneau qui s'ouvre, cliquez sur le lien portant le nom du sous-groupe requis.

     Le chemin d'accès actuel change pour refléter le sous-groupe sélectionné.
3. Cliquez sur **Ajouter**.

   La fenêtre **Sélectionnez l'application** s'ouvre.
4. Sélectionnez l'application pour laquelle vous souhaitez créer une stratégie.

5. Cliquez sur **Suivant**.

   La fenêtre des paramètres de la nouvelle stratégie s'ouvre à l'onglet **Général**.

6. Si vous le souhaitez, modifiez le nom par défaut, l'état par défaut et les paramètres d'héritage par défaut pour la stratégie.

7. Sélectionnez l'onglet **Paramètres de l'application**.

   Ou vous pouvez cliquer sur **Enregistrer** et quitter. La stratégie apparaît dans la liste des stratégies et vous pouvez modifier ses paramètres ultérieurement.

8. Sous l'onglet **Paramètres de l'application**, sélectionnez dans le volet de gauche la catégorie que vous souhaitez, puis dans le panneau des résultats à droite, modifiez les paramètres de la stratégie. Vous pouvez modifier les paramètres de la stratégie dans chaque catégorie (section).

   L'ensemble des paramètres dépend de l'application pour laquelle vous créez une stratégie. Pour plus de détails, reportez-vous à ce qui suit :

   - Configuration du Serveur d'administration
   - Paramètres de la stratégie de l'Agent d'administration
   - Documentation de Kaspersky Endpoint Security for Windows

   Pour plus de détails sur les paramètres des autres programmes de protection, consultez la documentation du programme correspondant.

   Pendant la modification des paramètres, vous pouvez cliquer sur **Annuler** pour annuler la dernière opération.

9. Cliquez sur **Enregistrer** afin d'enregistrer la stratégie.

Finalement, la stratégie ajoutée s'affiche dans la liste des stratégies.

Modification d'une stratégie

Pour modifier une stratégie, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Stratégies et profils**.

2. Cliquez sur la stratégie que vous souhaitez modifier.

   La fenêtre des paramètres de la stratégie s'ouvre.

3. Spécifiez les paramètres généraux et les paramètres de l'application pour laquelle vous créez une stratégie. Pour plus de détails, reportez-vous à ce qui suit :

   - Configuration du Serveur d'administration
   - Paramètres de la stratégie de l'Agent d'administration
   - Documentation de Kaspersky Endpoint Security for Windows

   Pour plus de détails sur les paramètres des autres applications de sécurité, consultez la documentation de l'application concernée.

4. Cliquez sur **Enregistrer**.

Les modifications de la stratégie seront enregistrées dans les propriétés de la stratégie et seront affichées dans la section **Historique des révisions**.

Paramètres généraux de la stratégie

Général

Sous l'onglet **Général**, vous pouvez modifier l'état de la stratégie et configurer l'héritage des paramètres de la stratégie :

- Le groupe **État de la stratégie** permet de sélectionner l'un des modes de stratégie :
  - **Active**

    Si cette option a été sélectionnée, la stratégie devient active.

    Cette option est sélectionnée par défaut.

  - **Pour les utilisateurs itinérants**

    Si cette option a été sélectionnée, la stratégie agit lorsque l'appareil est déconnecté du réseau de l'entreprise.

  - **Inactive**

    Si cette option a été sélectionnée, la stratégie devient inactive, mais elle est conservée dans le dossier **Stratégies**. Elle pourra être activée en fonction des besoins.

- Le groupe de paramètres **Héritage des paramètres** permet de configurer l'héritage de la stratégie :
  - **Hériter les paramètres de la stratégie parent**

    Si cette option est activée, les valeurs des paramètres de la stratégie sont héritées depuis la stratégie du groupe de niveau supérieur et sont verrouillées.

    Cette option est activée par défaut.

  - **Imposer l'héritage des paramètres aux stratégies enfants**

    Une fois que les modifications dans la stratégie sont appliquées, les opérations suivantes sont exécutées :
    - Les valeurs des paramètres de la stratégie seront diffusées dans les stratégies des sous-groupes d'administration, dans les stratégies enfant.
    - Dans le bloc **Héritage des paramètres** de la section **Général** de la fenêtre des propriétés de chaque stratégie enfant, la case **Hériter des paramètres de la stratégie parent** est automatiquement cochée.

    Quand la case est cochée, les valeurs des paramètres des stratégies enfants sont verrouillées.

    Cette option est Inactif par défaut.

Configuration des événements

Sous l'onglet **Configuration des événements**, vous pouvez configurer l'enregistrement des événements dans le journal et les notifications relatives à ceux-ci. Les événements sont répartis par niveau d'importance sur différents onglets :

- **Critique**

  La section **Critique** ne s'affiche pas dans les propriétés de la stratégie de l'Agent d'administration.

- **Erreur de fonctionnement**
- **Avertissement**
- **Information**

Dans chaque section, la liste reprend les types d'événements et la condition de stockage sur le serveur d'administration par défaut (en jours). Cliquez sur un type d'événement pour définir les paramètres suivants :

- **Enregistrement des événements**

  Vous pouvez spécifier le nombre de jours de stockage de l'événement et sélectionner l'emplacement du stockage de l'événement :

  - **Exporter dans le système SIEM selon le protocole Syslog**
  - **Conserver dans le journal des événements du SE sur l'appareil**
  - **Dans le journal des événements du SE du Serveur d'administration**

- **Notifications d'événement**

  Vous pouvez choisir si vous souhaitez être averti de l'événement de l'une des manières suivantes :

  - **Notifier par email**
  - **Notifier par SMS**
  - **Notifier via le lancement d'un fichier exécutable ou d'un script**
  - **Notifier via SNMP**

  Par défaut, ce sont les paramètres de notification spécifiés dans l'onglet Propriétés du serveur d'administration (comme l'adresse du destinataire) qui sont utilisés. Si vous le souhaitez, vous pouvez modifier ces paramètres sous les onglets **Email**, **SMS**, et **Fichier exécutable à exécuter**.

Historique des révisions

L'onglet **Historique des révisions** vous permet de consulter la liste des révisions de la stratégie et de restaurer les modifications apportées à la stratégie, si nécessaire.

Activation et désactivation d'une option d'héritage de stratégie

Pour activer ou désactiver l'option d'héritage dans une stratégie :

1. ouvrez la stratégie concernée.
2. Ouvrez l'onglet **Général**.
3. Activez ou désactivez l'héritage de la stratégie :
   - si vous activez l'option **Hériter les paramètres de la stratégie parent** pour une stratégie enfant et si un administrateur verrouille certains paramètres dans la stratégie parent, vous ne pouvez pas modifier ces paramètres dans la stratégie enfant.
   - Si vous désactivez l'option **Hériter les paramètres de la stratégie parent** pour une stratégie enfant, vous pouvez modifier tous les paramètres de la stratégie enfant, même si certains sont verrouillés dans la stratégie parent.
   - Si vous activez l'option **Imposer l'héritage des paramètres aux stratégies enfants** dans le groupe parent, l'option **Hériter les paramètres de la stratégie parent** est également activée pour chaque stratégie enfant. Dans ce cas, vous ne pouvez désactiver cette option pour aucune stratégie enfant. Tous les paramètres verrouillés dans la stratégie parent sont hérités par force dans les groupes enfants et ne sont plus modifiables.
4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications ou sur le bouton **Annuler** pour refuser les modifications.

Par défaut, l'option **Hériter les paramètres de la stratégie parent** est activée pour une nouvelle stratégie.

Si une stratégie possède des profils, toutes les stratégies enfants héritent de ces profils.

Copie d'une stratégie

Vous pouvez copier les stratégies d'un groupe d'administration vers un autre.

Pour copier une stratégie vers une autre groupe d'administration, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Stratégies et profils**.
2. Cochez la case en regard de la stratégie (ou des stratégies) que vous souhaitez copier.
3. Cliquez sur le bouton **Copier**.

   A droite de l'écran, l'arborescence des groupes d'administration s'affiche.
4. Dans l'arborescence, sélectionnez le groupe cible, à savoir le groupe dans lequel vous souhaitez copier la stratégie (ou les stratégies).
5. Cliquez sur le bouton **Copier** en bas de l'écran.
6. Cliquez sur le bouton **OK** pour confirmer l'opération.

La stratégie (les stratégies) sera (seront) copiée(s) dans le groupe cible avec tous ses profils. L'état de chaque stratégie copiée dans le groupe cible est **Inactive**. Vous pouvez remplacer l'état par **Active** à tout moment.

Si, dans le groupe cible, une stratégie présentant un nom similaire à la stratégie déplacée existe déjà, le suffixe de type (<numéro d'ordre>) est ajouté au nom de la stratégie déplacée, par exemple : (1).

Déplacement d'une stratégie

Vous pouvez déplacer les stratégies d'un groupe d'administration vers un autre. Par exemple, vous souhaitez supprimer un groupe mais vous souhaitez utiliser ses stratégies pour un autre groupe. Dans ce cas, vous pourriez vouloir déplacer la stratégie de l'ancien groupe vers le nouveau avant de supprimer l'ancien groupe.

Pour déplacer une stratégie vers un autre groupe d'administration, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Stratégies et profils**.
2. Cochez les cases en regard de la stratégie (ou des stratégies) que vous souhaitez déplacer.
3. Cliquez sur le bouton **Déplacer**.

   A droite de l'écran, l'arborescence des groupes d'administration s'affiche.
4. Dans l'arborescence, sélectionnez le groupe cible, à savoir le groupe dans lequel vous souhaitez déplacer la stratégie (ou les stratégies).
5. Cliquez sur le bouton **Déplacer** en bas de l'écran.
6. Cliquez sur le bouton **OK** pour confirmer l'opération.

   Si une stratégie n'est pas héritée du groupe source, elle est déplacée vers le groupe cible avec tous ses profils. L'état de la stratégie dans le groupe cible est **Inactive**. Vous pouvez remplacer l'état par **Active** à tout moment.

   Si une stratégie est héritée du groupe source, elle reste dans le groupe source. Elle est copiée dans le groupe cible avec tous ses profils. L'état de la stratégie dans le groupe cible est **Inactive**. Vous pouvez remplacer l'état par **Active** à tout moment.

Si, dans le groupe cible, une stratégie présentant un nom similaire à la stratégie déplacée existe déjà, le suffixe de type (<numéro d'ordre>) est ajouté au nom de la stratégie déplacée, par exemple : (1).

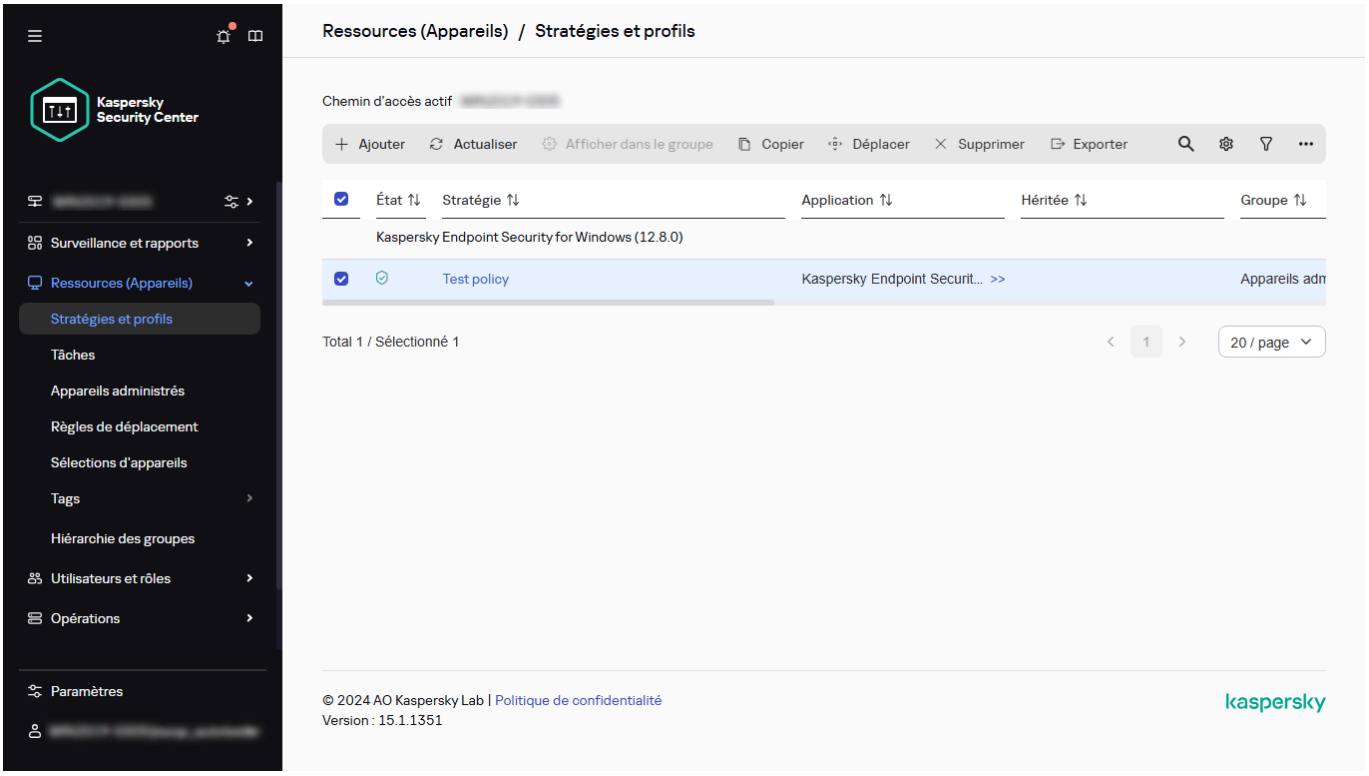
Exportation d'une stratégie

Kaspersky Security Center permet d'enregistrer une tâche, ses paramètres et les profils de stratégie dans un fichier KLP. Vous pouvez utiliser ce fichier KLP pour importer la stratégie enregistrée dans Kaspersky Security Center Windows et Kaspersky Security Center Linux.

Pour exporter une stratégie, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Stratégies et profils**.
2. Cochez la case en regard de la stratégie que vous souhaitez corriger.

   Vous ne pouvez pas exporter plusieurs stratégies à la fois. Si vous sélectionnez plusieurs stratégies, le bouton **Exporter** sera désactivé.



3. Cliquez sur le bouton **Exporter**.
4. Dans la fenêtre ouverte **Enregistrer sous**, indiquez le nom et le chemin du fichier de stratégie. Cliquez sur **Enregistrer**.

   La fenêtre **Enregistrer sous** s'affiche uniquement si vous utilisez Google Chrome, Microsoft Edge ou Opera. Si vous utilisez un autre navigateur, le fichier de stratégie est automatiquement enregistré dans le dossier **Téléchargements**.

Importation d'une stratégie

Kaspersky Security Center permet d'importer une stratégie depuis un fichier KLP. Le fichier KLP contient la stratégie exportée, ses paramètres et les profils de stratégie.

Pour importer une stratégie, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Stratégies et profils**.
2. Cliquez sur le bouton **Importer**.
3. Cliquez sur le bouton **Parcourir** pour choisir le fichier de stratégie à importer.
4. Dans la fenêtre qui s'ouvre, indiquez le chemin d'accès au fichier de stratégie KLP, puis cliquez sur le bouton **Ouvrir**. Notez que vous ne pouvez sélectionner qu'un seul fichier de stratégie.

   Le traitement de la stratégie démarre.

5. Une fois que la stratégie a été traitée avec succès, sélectionnez le groupe d'administration auquel vous souhaitez appliquer la stratégie.

6. Cliquez sur le bouton **Terminée** pour terminer l'importation de la stratégie.

La notification avec les résultats de l'importation s'affiche. Si la stratégie est importée avec succès, vous pouvez cliquer sur le lien **En savoir plus** pour afficher les propriétés de la stratégie.

Après une importation réussie, la stratégie s'affiche dans la liste des stratégies. Les paramètres et les profils de la stratégie sont également importés. Quel que soit l'état de la stratégie sélectionné lors de l'exportation, la stratégie importée est inactive. Vous pouvez modifier l'état de la stratégie dans les propriétés de la stratégie.

Si la stratégie importée porte le même nom que la stratégie existante, le nom de la stratégie importée est suivi de l'index **(<numéro de séquence suivant>)**, par exemple : **(1)**, **(2)**.

Affichage du graphique de l'état de la distribution des stratégies

Dans Kaspersky Security Center, vous pouvez afficher l'état de l'application de la stratégie sur chaque appareil dans un graphique de l'état de distribution des stratégies.

Pour afficher l'état de la distribution des stratégies sur chaque appareil, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Stratégies et profils**.

2. Cochez la case située à côté du nom de la stratégie dont vous souhaitez consulter l'état de la distribution sur les appareils.

3. Dans le menu qui s'affiche, sélectionnez le lien **Distribution**.

   La fenêtre **Résultats de distribution de la stratégie <Nom de la stratégie>** s'ouvre.

4. Dans la fenêtre **Résultats de distribution de la stratégie <Nom de la stratégie>** qui s'ouvre, la **description de l'état** de la stratégie s'affiche.

Vous pouvez modifier le nombre de résultats affichés dans la liste avec la distribution des stratégies. Le nombre d'appareils maximal est égal à 100 000.

Pour modifier le nombre d'appareils affichés dans la liste avec les résultats de la distribution des stratégies, procédez comme suit :

1. Dans le menu principal, allez dans les paramètres de votre compte et puis sélectionnez **Options d'interface**.

2. Dans la fenêtre **Limite du nombre d'appareils affichés dans les résultats de la distribution des stratégies**, indiquez le nombre d'appareils (jusqu'à 100 000).

   Par défaut, le nombre est de 5 000.

3. Cliquez sur **Enregistrer**.

   Les paramètres sont enregistrés et appliqués.

Suppression d'une stratégie

Vous pouvez supprimer une stratégie si vous n'en avez plus besoin. Vous pouvez supprimer uniquement une stratégie qui n'est pas héritée dans le groupe d'administration indiqué. Si une stratégie est héritée, vous ne pouvez la supprimer que dans le groupe de niveau supérieur pour lequel elle a été créée.

Pour supprimer une stratégie, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Stratégies et profils**.
2. Cochez la case en regard de la stratégie que vous voulez supprimer, puis cliquez sur **Supprimer**.

   Le bouton **Supprimer** devient indisponible (grisé) si vous sélectionnez une stratégie héritée.
3. Cliquez sur le bouton **OK** pour confirmer l'opération.

La stratégie est supprimée ainsi que tous ses profils.

Administration des profils de stratégies

Cette section décrit la gestion des profils de stratégie et comporte des informations sur l'affichage des profils d'une stratégie, le changement, la création, la modification ou la copie d'un profil de stratégie, la création d'une règle d'activation de profil de stratégie et la suppression de profil de stratégie.

Consultation des profils d'une stratégie

Pour consulter les profils d'une stratégie, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Stratégies et profils**.
2. Cliquez sur le nom de la stratégie dont vous souhaitez voir les profils.

   La fenêtre des propriétés de la stratégie s'ouvre à l'onglet **Général**.
3. Ouvrez l'onglet **Profils de stratégie**.

La liste des profils des stratégies s'affiche dans un tableau. Si la stratégie n'a pas de profils, un tableau vide s'affiche.

Modification de la priorité d'un profil de stratégie

Pour modifier la priorité d'un profil de stratégie, procédez comme suit :

1. Passez à la liste des profils d'une stratégie que vous voulez.

   La liste des profils de la stratégie s'ouvre.
2. Sous l'onglet **Profils de stratégie**, cochez la case en regard du profil de stratégie dont vous souhaitez modifier la priorité.

3. Définissez une nouvelle position du profil de stratégie dans la liste en cliquant sur **Augmenter la priorité** ou **Réduire la priorité**.

   Plus un profil de stratégie se trouve haut dans la liste, plus sa priorité est élevée.

4. Cliquez sur le bouton **Enregistrer**.

La priorité du profil de stratégie sélectionné est modifiée et appliquée.

Création d'un profil de stratégie

Pour créer un profil de stratégie, procédez comme suit :

1. Passez à la liste des profils d'une stratégie que vous voulez.

   La liste des profils de la stratégie s'ouvre. Si la stratégie n'a pas de profils, un tableau vide s'affiche.

2. Cliquez sur **Ajouter**.

3. Si vous le souhaitez, modifiez le nom par défaut et les paramètres d'héritage par défaut pour le profil.

4. Sélectionnez l'onglet **Paramètres de l'application**.

   Ou vous pouvez cliquer sur **Enregistrer** et quitter. Le profil que vous avez créé apparaît dans la liste des profils des stratégies et vous pouvez modifier ses paramètres ultérieurement.

5. Sous l'onglet **Paramètres de l'application**, sélectionnez dans le volet de gauche la catégorie que vous souhaitez, puis dans le panneau des résultats à droite, modifiez les paramètres du profil. Vous pouvez modifier les paramètres du profil de stratégie dans chaque catégorie (section).

   Pendant la modification des paramètres, vous pouvez cliquer sur **Annuler** pour annuler la dernière opération.

6. Cliquez sur le bouton **Enregistrer** afin d'enregistrer le profil.

Le profil apparaît dans la liste des profils des stratégies.

Modification du profil de stratégie

La modification d'un profil de stratégie est uniquement possible pour les stratégies de Kaspersky Endpoint Security for Windows.

Pour modifier un profil de stratégie, procédez comme suit :

1. Passez à la liste des profils d'une stratégie que vous voulez.

   La liste des profils de la stratégie s'ouvre.

2. Sous l'onglet **Profils de stratégie**, cliquez sur le profil de stratégie que vous souhaitez modifier.

   Cette action entraîne l'ouverture de la fenêtre des propriétés du profil de stratégie.

3. Configurez les paramètres du profil dans la fenêtre des propriétés :

   - Si nécessaire, sous l'onglet **Général**, modifiez le nom du profil et activez ou désactivez le profil.
   - Modifiez les règles d'activation du profil.
   - Modifiez les paramètres de l'application.

   Pour plus de détails sur les applications de sécurité, veuillez consulter la documentation de l'application correspondante.

4. Cliquez sur **Enregistrer**.

Les paramètres modifiés entrent en vigueur après la synchronisation de l'appareil avec le Serveur d'administration (si le profil de stratégie est actif), ou après l'exécution de la règle d'activation (si le profil de stratégie est inactif).

Copie d'un profil de stratégie

Vous pouvez copier un profil de stratégie dans la stratégie actuelle ou une autre, par exemple, si vous souhaitez avoir des profils identiques pour les différentes stratégies. Vous pouvez également utiliser la copie si vous avez deux ou plusieurs profils qui diffèrent seulement sur un petit nombre de paramètres.

Pour copier un profil de stratégie, procédez comme suit :

1. Passez à la liste des profils d'une stratégie que vous voulez.

   La liste des profils de la stratégie s'ouvre. Si la stratégie n'a pas de profils, un tableau vide s'affiche.

2. Sous l'onglet **Profils de stratégie**, cliquez sur le profil de stratégie que vous souhaitez copier.
3. Cliquez sur **Copier**.
4. Dans la fenêtre qui s'ouvre, sélectionnez la stratégie dans laquelle vous souhaitez copier le profil.

   Vous pouvez copier un profil de stratégie dans la même stratégie ou dans une stratégie que vous précisez.

5. Cliquez sur **Copier**.

   Le profil de stratégie est copié dans la stratégie que vous avez sélectionnée. Le profil récemment copié obtient la priorité la plus basse. Si vous copiez le profil dans la même stratégie, la nom de la stratégie récemment copiée, le suffixe (), par exemple : (1), (2) est ajouté au profil récemment copié.

Ensuite, vous pouvez modifier les paramètres du profil, y compris son nom et sa priorité ; le profil de stratégie ne sera pas modifié dans ce cas.

Création d'une règle d'activation du profil de stratégie

Pour créer une règle d'activation du profil de stratégie, procédez comme suit :

1. Passez à la liste des profils d'une stratégie que vous voulez.

   La liste des profils de la stratégie s'ouvre.

2. Sous l'onglet **Profils de stratégie**, cliquez sur le profil de stratégie pour lequel vous devez créer une règle d'activation.

   Si la liste des profils de stratégie est vide, vous pouvez créer le profil de stratégie.

3. Sous l'onglet **Règles d'activation**, cliquez sur le bouton **Ajouter**.

   La fenêtre avec des règles d'activation du profil de stratégie s'ouvre.

4. Définissez un nom pour la règle.

5. Cochez les cases en regard des conditions qui doivent influencer l'activation du profil de stratégie que vous créez :

   - **Règles générales d'activation du profil de stratégie**

     Cochez la case pour configurer les règles de l'activation du profil de stratégie sur l'appareil en fonction de l'état du mode déconnecté de l'appareil, de la règle de connexion de l'appareil au Serveur d'administration et des tags attribués à l'appareil.

     Définissez cette option à l'étape suivante :

     - **État de l'appareil**

       Définit la condition de la présence de l'appareil sur le réseau :

       - **En ligne** : L'appareil se trouve sur le réseau et le Serveur d'administration est donc accessible.
       - **Déconnecté** : L'appareil se trouve sur un réseau extérieur, c'est-à-dire que le Serveur d'administration n'est pas accessible.
       - **N/A** : Les critères ne sont pas appliqués.

     - **La règle pour la connexion du Serveur d'administration est active sur cet appareil**

       Choisissez la condition d'activation du profil de stratégie (si la règle est exécutée ou non) et sélectionnez le nom de la règle.

       La règle définit l'emplacement réseau de l'appareil pour la connexion au Serveur d'administration dont les conditions doivent être remplies (ou ne doivent pas être remplies) pour l'activation du profil de stratégie.

       La description de l'emplacement réseau de l'appareil pour la connexion au Serveur d'administration peut être créée ou configurée dans la règle de permutation de l'Agent d'administration.

   - **Règles d'un propriétaire particulier de l'appareil**

     Définissez cette option à l'étape suivante :

     - **Propriétaire de l'appareil**

       Activez l'option pour configurer et activer une règle d'activation de profil sur l'appareil en fonction de son propriétaire. La liste déroulante située sous la case permet de sélectionner les critères d'activation du profil :

       - L'appareil appartient au propriétaire indiqué (le symbole "=").
       - L'appareil n'appartient pas au propriétaire indiqué (le symbole "#").

         Si cette option est activée, le profil est activé sur l'appareil en fonction du critère configuré. Vous pouvez indiquer le propriétaire de l'appareil lorsque l'option est activée. Si l'option est désactivée, les critères d'activation du profil ne sont pas appliqués. Cette option est Inactif par défaut.

     - **Le propriétaire de l'appareil appartient à un groupe de sécurité interne**

Activez l'option pour configurer et activer la règle d'activation du profil sur l'appareil en fonction de l'appartenance de son propriétaire au groupe de sécurité interne de Kaspersky Security Center. La liste déroulante située sous la case permet de sélectionner les critères d'activation du profil :

- Le propriétaire de l'appareil appartient au groupe de sécurité indiqué (le symbole "=").
- Le propriétaire de l'appareil n'appartient pas au groupe de sécurité indiqué (le symbole "#").

  Si cette option est activée, le profil est activé sur l'appareil en fonction du critère configuré. Vous pouvez spécifier un groupe de sécurité de Kaspersky Security Center. Si l'option est désactivée, les critères d'activation du profil ne sont pas appliqués. Cette option est Inactif par défaut.

- Règles pour les spécifications matérielles

  Cochez la case pour configurer les règles d'activation du profil de stratégie sur l'appareil en fonction du volume de la mémoire et du nombre de processeurs logiques de l'appareil.

  Définissez cette option à l'étape suivante :

  - Taille de la mémoire RAM (Mo)

    Activez cette option pour configurer et activer une règle d'activation du profil sur l'appareil en fonction du volume de mémoire vive de l'appareil. La liste déroulante située sous la case permet de sélectionner les critères d'activation du profil :

    - Le volume de mémoire vive de l'appareil est inférieur à la valeur indiquée (le symbole " < ").
    - Le volume de mémoire vive de l'appareil est supérieur à la valeur indiquée (le symbole " > ").

    Si cette option est activée, le profil est activé sur l'appareil en fonction du critère configuré. Vous pouvez indiquer le volume de mémoire vive de l'appareil. Si l'option est désactivée, les critères d'activation du profil ne sont pas appliqués. Cette option est Inactif par défaut.

  - Nombre de processeurs logiques

    Activez cette option pour configurer et activer une règle d'activation du profil sur l'appareil en fonction de son nombre de processeurs logiques. La liste déroulante située sous la case permet de sélectionner les critères d'activation du profil :

    - Le nombre de processeurs logiques de l'appareil est inférieur ou égal à la valeur indiquée (le symbole " < ").
    - Le nombre de processeurs logiques de l'appareil est supérieur ou égal à la valeur indiquée (le symbole " > ").

    Si cette option est activée, le profil est activé sur l'appareil en fonction du critère configuré. Vous pouvez indiquer le nombre de processeurs logiques de l'appareil. Si l'option est désactivée, les critères d'activation du profil ne sont pas appliqués. Cette option est Inactif par défaut.

- **Règles pour l'attribution de rôle**

  Définissez cette option à l'étape suivante :

  Activer le profil de stratégie en présence d'un rôle pour le propriétaire de l'appareil

Sélectionnez cette option pour configurer et activer la règle d'activation du profil sur l'appareil en fonction du rôle du propriétaire. Ajoutez le rôle manuellement depuis la liste des rôles existants.

Si cette option est activée, le profil est activé sur l'appareil en fonction du critère configuré.

- **Règles pour l'usage de tag**

  Cochez la case pour configurer les règles d'activation du profil de stratégie sur l'appareil en fonction des tags attribués à l'appareil. Vous pouvez activer le profil de stratégie aux appareils qui ont les tags sélectionnés ou qui ne les ont pas.

  Définissez cette option à l'étape suivante :

  - **Tag**

    Définissez dans la liste des tags la règle d'inclusion des appareils dans le profil de stratégie en cochant la case des tags souhaités.

    Vous pouvez ajouter à la liste de nouveaux tags en les saisissant dans le champ sur la liste et en cliquant sur le bouton **Ajouter**.

    Le profil de stratégie reprendra les appareils dont la description reprend tous les tags sélectionnés. Si les cases sont décochées, les critères ne sont pas appliqués. Les cases sont décochées par défaut.

  - **Appliquer aux appareils sans les tags sélectionnés**

    Activez cette option s'il est nécessaire d'intervertir la sélection de tags.

    Si cette option est activée, les appareils sans tags sélectionnés seront inclus dans le profil de stratégie. Si l'option est désactivée, les critères ne sont pas appliqués.

    Cette option est Inactif par défaut.

- **Règles d'utilisation d'Active Directory**

  Cochez la case pour configurer les règles d'activation du profil de stratégie sur l'appareil en fonction du placement de l'appareil dans une division Active Directory ou de l'appartenance de l'appareil ou du propriétaire de l'appareil au groupe de sécurité Active Directory.

  Définissez cette option à l'étape suivante :

  - **Appartenance du propriétaire de l'appareil au groupe de sécurité Active Directory**

    Si l'option est activée, le profil de stratégie est activé sur l'appareil dont le propriétaire est membre du groupe de sécurité indiqué. Si l'option est désactivée, les critères d'activation du profil ne sont pas appliqués. Cette option est Inactif par défaut.

  - **Appartenance de l'appareil au groupe de sécurité Active Directory**

    Si cette option est activée, le profil de stratégie est activé sur l'appareil. Si l'option est désactivée, les critères d'activation du profil ne sont pas appliqués. Cette option est Inactif par défaut.

- Placement de l'appareil dans une unité organisationnelle Active Directory

  Si cette option est activée, le profil de stratégie est activé sur l'appareil figurant dans la sous-division Active Directory indiquée. Si l'option est désactivée, les critères d'activation du profil ne sont pas appliqués.

  Cette option est Inactif par défaut.

Le nombre de pages supplémentaires de l'assistant dépend des paramètres que vous sélectionnez à la première étape. Vous pouvez modifier les règles d'activation du profil de stratégie plus tard.

6. Consultez la liste des paramètres configurés. Si la liste est correcte, cliquez sur **Créer**.

Le profil est enregistré. Le profil sera activé sur l'appareil lors de l'application des règles d'activation.

Les règles d'activation du profil de stratégie créées pour le profil s'affichent dans les propriétés du profil de stratégie sous l'onglet **Règles d'activation**. Vous pouvez modifier ou supprimer la règle de l'activation du profil de stratégie.

Il est possible d'exécuter simultanément plusieurs règles d'activation.

Suppression d'un profil de stratégie

Pour supprimer un profil de stratégie, procédez comme suit :

1. Passez à la liste des profils d'une stratégie que vous voulez.

   La liste des profils de la stratégie s'ouvre.

2. Sous l'onglet **Profils de stratégie**, cochez la case en regard du profil de stratégie que vous souhaitez supprimer, puis cliquez sur **Supprimer**.

3. Dans la fenêtre qui s'ouvre, cliquez une nouvelle fois sur **Supprimer**.

Le profil de stratégie est supprimé. Si la stratégie est héritée d'un groupe de niveau inférieur, le profil reste dans ce groupe, mais devient le profil de la stratégie de ce groupe. Cela permet d'éliminer les changements importants au niveau des paramètres des applications administrées installées sur les appareils des groupes de niveau inférieur.

Chiffrement et protection des données

Le chiffrement des données diminue les risques de fuite d'informations en cas de vol ou de perte d'un ordinateur portable ou d'un disque dur, ou en cas d'accès aux données par des utilisateurs et des applications non autorisés.

L'utilisation du chiffrement est prise en charge par les applications suivantes de Kaspersky :

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Mac

Vous pouvez afficher ou masquer certains des éléments d'interface liés à la fonction de gestion du chiffrement à l'aide des paramètres de l'interface utilisateur.

Nous ne recommandons pas d'activer le chiffrement dans VDI.

Chiffrement des données dans Kaspersky Endpoint Security for Windows

Vous pouvez administrer les types de chiffrement suivants :

- Chiffrement de disque BitLocker sur les appareils fonctionnant sous le système d'exploitation Windows pour les serveurs
- Kaspersky Disk Encryption sur les appareils fonctionnant sous le système d'exploitation Windows pour les postes de travail

À l'aide de ces modules de Kaspersky Endpoint Security for Windows, vous pouvez, par exemple, activer ou désactiver le chiffrement, consulter la liste des disques chiffrés ou générer et consulter des rapports sur le chiffrement.

Vous configurez le chiffrement en définissant les stratégies de Kaspersky Endpoint Security for Windows dans Kaspersky Security Center. Kaspersky Endpoint Security for Windows effectue le chiffrement et le déchiffrement conformément à la stratégie active. Les instructions détaillées sur la configuration des règles et la description des fonctionnalités de chiffrement sont disponibles dans l'aide de Kaspersky Endpoint Security for Windows.

Chiffrement des données dans Kaspersky Endpoint Security for Mac

Vous pouvez utiliser le chiffrement FileVault sur les appareils exécutant macOS. Lorsque vous travaillez avec Kaspersky Endpoint Security for Mac, vous pouvez activer ou désactiver ce chiffrement.

Vous configurez le chiffrement en définissant les stratégies de Kaspersky Endpoint Security for Mac dans Kaspersky Security Center. Kaspersky Endpoint Security for Mac effectue le chiffrement et le déchiffrement conformément à la stratégie active. Pour obtenir la description détaillée des fonctionnalités de chiffrement, consultez l'aide de Kaspersky Endpoint Security for Mac.

Consultation de la liste des disques chiffrés

Dans Kaspersky Security Center, vous pouvez afficher les détails des lecteurs chiffrés et des appareils chiffrés au niveau du lecteur. Une fois que les informations sur le disque sont déchiffrées, celui-ci sera automatiquement supprimé de la liste.

Pour consulter la liste des disques chiffrés,

Dans le menu principal, accédez à **Opérations** → **Chiffrement et protection des données** → **Disques chiffrés**.

Si la section ne figure pas dans le menu, cela signifie qu'elle est masquée. Dans les paramètres de l'interface utilisateur, activez l'option **Afficher le chiffrement et la protection des données** pour afficher la section.

Vous pouvez exporter la liste des disques chiffrés dans un fichier CSV ou TXT. Pour ce faire, cliquez sur le bouton **Exporter vers un fichier CSV** ou **Exporter vers un fichier TXT**.

Consultation de la liste des événements du chiffrement

Pendant l'exécution des tâches de chiffrement ou de déchiffrement des données sur les appareils, Kaspersky Endpoint Security for Windows envoie dans Kaspersky Security Center les informations sur les événements survenus des types suivants :

- Il est impossible de chiffrer ou déchiffrer le fichier ou de créer l'archive chiffrée en raison d'un espace sur le disque insuffisant.
- Il est impossible de chiffrer ou déchiffrer le fichier ou créer l'archive chiffrée à cause de problèmes avec la licence.
- Il est impossible de chiffrer ou déchiffrer le fichier ou créer une archive chiffrée en raison de l'absence de privilèges d'accès.
- L'accès au fichier chiffré est interdit à l'application.
- Les erreurs inconnues.

Pour consulter la liste des événements survenus lors du chiffrement des données sur les appareils,

Dans le menu principal, accédez à **Opérations → Chiffrement et protection des données → Événements du chiffrement**.

Si la section ne figure pas dans le menu, cela signifie qu'elle est masquée. Dans les paramètres de l'interface utilisateur, activez l'option **Afficher le chiffrement et la protection des données** pour afficher la section.

Vous pouvez exporter la liste des disques chiffrés dans un fichier CSV ou TXT. Pour ce faire, cliquez sur le bouton **Exporter vers un fichier CSV** ou **Exporter vers un fichier TXT**.

Vous pouvez également consulter la liste des événements de chiffrement pour chaque appareil administré.

Pour consulter les événements de chiffrement d'un appareil administré, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils) → Appareils administrés**.
2. Cliquez sur le nom d'un appareil administré.
3. Sous l'onglet **Général**, accédez à la section **Protection**.
4. Cliquez sur le lien **Consulter les erreurs de chiffrement des données**.

Formation et consultation des rapports sur le chiffrement

Vous pouvez créer les rapports suivants :

- Rapport de l'état de chiffrement des appareils administrés. Ce rapport fournit des détails sur le chiffrement des données de divers appareils administrés. Par exemple, le rapport indique le nombre d'appareils auxquels s'applique la stratégie avec les règles de chiffrement configurées. Vous pouvez également savoir, par exemple, combien d'appareils doivent être redémarrés. Le rapport contient également des informations sur la technologie et l'algorithme de chiffrement pour chaque appareil.

- Rapport de l'état de chiffrement des appareils de stockage. Ce rapport contient des informations similaires à celles du rapport sur l'état de chiffrement des appareils administrés, mais il ne fournit des données que pour les appareils de stockage de masse et les disques amovibles.

- Rapport sur les privilèges d'accès aux disques chiffrés. Ce rapport indique quels comptes utilisateurs ont accès aux disques chiffrés.

- Rapport sur les erreurs de chiffrement des fichiers. Ce rapport contient les erreurs survenues lors de l'exécution des tâches de chiffrement ou de déchiffrement des données sur les appareils.

- Rapport sur le blocage de l'accès aux fichiers chiffrés. Ce rapport contient les informations sur le blocage de l'accès de l'application aux fichiers chiffrés. Ce rapport est utile si un utilisateur ou une application non autorisé tente d'accéder à des fichiers ou des disques chiffrés.

Vous pouvez générer n'importe quel rapport dans la section **Surveillance et rapports → Rapports**. Vous pouvez également générer les rapports de chiffrement suivants dans la section **Opérations → Chiffrement et protection des données** :

- Rapport de l'état de chiffrement des appareils de stockage

- Rapport sur les privilèges d'accès aux disques chiffrés

- Rapport sur les erreurs de chiffrement des fichiers

*Pour générer un rapport de chiffrement dans la section **Chiffrement et protection des données** :*

1. Assurez-vous d'avoir activé l'option **Afficher le chiffrement et la protection des données** dans les options d'interface.

2. Dans les propriétés de la stratégie, ouvrez l'onglet **Configuration des événements**.

3. Dans la section **Critique**, cliquez sur **Ajouter un événement** et cochez la case en regard de l'événement *Erreur d'application des règles de chiffrement/déchiffrement des fichiers*.

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

5. Dans le menu principal, accédez à **Opérations → Chiffrement et protection des données**.

6. Ouvrez une des sections suivantes :

   - Les **Disques chiffrés** génèrent le rapport sur l'état du chiffrement des appareils de stockage de masse ou le rapport sur les droits d'accès aux lecteurs chiffrés.
   - Les **Événements du chiffrement** génèrent le rapport sur les erreurs de chiffrement de fichiers.

7. Cliquez sur le nom du rapport que vous souhaitez générer.

La création du rapport démarre.

Accorder l'accès à un disque chiffré en mode déconnecté

Un utilisateur peut demander l'accès à un appareil chiffré, par exemple, lorsque Kaspersky Endpoint Security for Windows n'est pas installé sur l'appareil administré. Après avoir reçu la demande, vous pouvez créer un fichier de clé d'accès et l'envoyer à l'utilisateur. Tous les cas d'utilisation et les instructions détaillées sont fournis dans l'aide de Kaspersky Endpoint Security for Windows.

Pour accorder l'accès à un disque chiffré en mode déconnecté, procédez comme suit :

1. Obtenez une demande d'accès au fichier d'un utilisateur (fichier avec l'extension FDERTC). Suivez les instructions de l'aide de Kaspersky Endpoint Security for Windows pour générer le fichier dans Kaspersky Endpoint Security for Windows.
2. Dans le menu principal, accédez à **Opérations** → **Chiffrement et protection des données** → **Disques chiffrés**.

   Une liste des disques chiffrés s'affiche.
3. Sélectionnez le disque pour lequel l'utilisateur a demandé l'accès.
4. Cliquez sur le bouton **Autoriser l'accès à l'appareil en mode déconnecté**.
5. Dans la fenêtre qui s'ouvre, sélectionnez le plug-in correspondant à l'application Kaspersky utilisée pour chiffrer le disque sélectionné.

   Si un disque est chiffré avec une application Kaspersky non prise en charge par Kaspersky Security Center Web Console, utilisez la Console d'administration Microsoft Management Console pour accorder l'accès hors ligne.
6. Suivez les instructions fournies dans l'aide de Kaspersky Endpoint Security for Windows (voir les blocs d'extension à la fin de la section).

Après cela, l'utilisateur applique le fichier reçu pour accéder au disque chiffré et lire les données stockées sur le disque.

Utilisateurs et rôles d'utilisateurs

Cette section décrit les utilisateurs et les rôles d'utilisateurs et explique comment les créer et les modifier, comment affecter des rôles et des groupes à des utilisateurs et comment associer des profils de stratégie à des rôles.

À propos des rôles d'utilisateurs

Un *rôle d'utilisateur* (ou un *rôle*) est un objet qui contient un ensemble de privilèges. Un rôle peut être associé aux paramètres des applications de Kaspersky installées sur l'appareil de l'utilisateur. Vous pouvez attribuer un rôle à un ensemble d'utilisateurs ou à un ensemble de groupes de sécurité à n'importe quel niveau de la hiérarchie des groupes d'administration, des Serveurs d'administration ou au niveau d'objets spécifiques.

Si vous administrez les appareils via une hiérarchie de Serveurs d'administration comprenant des Serveurs d'administration virtuels, notez que vous ne pouvez créer, modifier ou supprimer des rôles d'utilisateur qu'à partir d'un Serveur d'administration physique. Ensuite, vous pouvez propager les rôles d'utilisateurs sur les Serveurs d'administration secondaires, y compris les serveurs virtuels.

Vous pouvez associer des rôles d'utilisateurs aux profils des stratégies. Si un rôle est attribué à un utilisateur, cet utilisateur obtient les paramètres de sécurité dont il a besoin pour remplir ses fonctions.

Un rôle d'utilisateur peut être associé à des utilisateurs d'appareils dans un groupe d'administration défini.

Portée du rôle d'utilisateur

La *portée du rôle d'utilisateur* est un ensemble d'utilisateurs et de groupes d'administration. Les paramètres associés à un rôle d'utilisateur s'appliquent uniquement aux appareils qui appartiennent aux utilisateurs qui ont ce rôle et uniquement si ces appareils appartiennent aux groupes associés à ce rôle, y compris les groupes enfant.

Avantage de l'utilisation de rôles

Un des avantages liés à l'utilisation de rôles est qu'il n'est pas nécessaire de définir les paramètres de sécurité pour chacun des appareils administrés ou pour chaque utilisateur individuellement. Le nombre d'utilisateurs et d'appareils au sein d'une entreprise peut être relativement élevé, mais le nombre de différentes fonctions qui requièrent différents paramètres de sécurité est quant à lui considérablement plus réduit.

Différences par rapport à l'utilisation de profils des stratégies

Les profils des stratégies désignent des propriétés d'une stratégie qui est créée pour chaque application de Kaspersky séparément. Un rôle est associé à de nombreux profils des stratégies créés pour différentes applications. Par conséquent, un rôle est une manière de réunir en un endroit les paramètres pour un certain type d'utilisateur.

Consultation des comptes utilisateurs et des sessions

Le Kaspersky Security Center permet d'administrer les comptes utilisateurs et groupes de comptes. L'application prend en charge deux types de comptes utilisateur :

- Comptes utilisateur pour les employés de l'entreprise. Le Serveur d'administration reçoit les données relatives aux comptes utilisateur de ces utilisateurs lors du balayage du réseau de l'entreprise.
- Comptes des utilisateurs internes. Appliqués pour l'utilisation des Serveurs d'administration virtuels. Les comptes des utilisateurs internes sont créés et utilisés uniquement à l'intérieur de Kaspersky Security Center.

Vous pouvez consulter la liste des comptes utilisateurs et des sessions d'une des manières suivantes :

- Dans le menu principal, accédez à **Utilisateurs et rôles** → **Utilisateurs et groupes**.
- Dans le menu principal, accédez à **Ressources (Appareils)** → **Appareils administrés** → lien <nom de l'appareil> → onglet **Général** → section **Général** → groupe **Sessions**.

  La section **Sessions** affiche les comptes utilisateurs avec des sessions actives sur les appareils fonctionnant sous Windows.

La liste des comptes utilisateurs et des sessions s'affiche correctement si les conditions suivantes sont remplies :

- Utilisez l'Agent d'administration de la même version que le Serveur d'administration ou d'une version ultérieure.
- Le sondage d'Active Directory est activé pour afficher les comptes des utilisateurs du domaine.
- Sur les appareils administrés fonctionnant sous Windows, le service **Server** (**LanmanServer**) est exécuté.

Configuration des droits d'accès aux fonctionnalités de l'application. Restriction d'accès selon un rôle

Kaspersky Security Center fournit des possibilités d'accès selon un rôle aux fonctionnalités de Kaspersky Security Center et des applications Kaspersky administrées.

Vous pouvez configurer les droits d'accès aux fonctionnalités de l'application pour les utilisateurs de Kaspersky Security Center de l'une des manières suivantes :

- Configurer les privilèges de chaque utilisateur ou groupe d'utilisateurs séparément.
- Créer des rôles types d'utilisateurs avec un ensemble de privilèges configurés au préalable et attribuer ces rôles aux utilisateurs en fonction de leurs responsabilités.

L'application des rôles des utilisateurs vise à simplifier et à raccourcir les procédures courantes de configuration des droits d'accès des utilisateurs aux fonctionnalités de l'application. Les droits d'accès des rôles sont configurés en fonction des tâches types et de la responsabilité des utilisateurs.

Ces rôles peuvent être nommés en fonction de leurs attributs. Il est possible de créer un nombre illimité de rôles dans l'application.

Vous pouvez utiliser les rôles d'utilisateurs prédéfinis avec un ensemble de droits déjà configurés, ou créer des rôles et configurer vous-même les droits requis.

Droits d'accès aux fonctionnalités de l'application

Le tableau ci-dessous présente les fonctionnalités de Kaspersky Security Center avec les droits d'accès pour gérer les tâches associées, les rapports, les paramètres et effectuer les actions utilisateur associées.

Pour exécuter les actions utilisateur répertoriées dans le tableau, un utilisateur doit avoir le droit spécifié en regard de l'action.

Les droits **de lecture**, **Écrire** et **Exécuter** s'appliquent à toute tâche, rapport ou paramètre. En plus de ces droits, un utilisateur doit disposer du droit **Réalisez des opérations sur les sélections d'appareils** pour gérer les tâches, les rapports ou les paramètres sur les sélections d'appareils.

Toutes les tâches, rapports, paramètres et paquets d'installation qui manquent dans le tableau appartiennent à la zone fonctionnelle **Fonctions générales : Fonctionnalité de base**.

Droits d'accès aux fonctionnalités de l'application

Zone fonctionnelle	Droit	Action utilisateur : droit requis pour exécuter l'action	Tâche	Rapport	Autres
Fonctions générales : **Administration des groupes d'administration**	**Écrire**	• Ajouter un appareil à un groupe d'administration : **Écrire** • Supprimer un appareil d'un groupe d'administration : **Écrire** • Ajouter un groupe d'administration à un autre groupe d'administration : **Écrire** • Supprimer un groupe d'administration d'un autre groupe d'administration : **Écrire**	Aucun	Aucun	Aucun
Fonctions générales : **Accéder aux objets quel que soit leur ACL**	**Lire**	Obtenir un accès Lire à tous les objets : **Lire**	Aucun	Aucun	La zone fonctionnelle **Fonctions générales : Accéder aux objets quel que soit leur ACL** est conçue à des fins d'audit. Lorsque les utilisateurs disposent des droits de **Lire** dans cette zone fonctionnelle, ils bénéficient d'un accès complet en **Lire** à tous les objets et peuvent exécuter toutes les tâches créées sur une sélection d'appareils connectés au Serveur d'administration via l'Agent d'administration avec des privilèges d'administrateur local (root pour Linux). Nous vous recommandons d'octroyer ces droits avec précaution et à un nombre limité d'utilisateurs qui en ont besoin pour l'accomplissement de leurs tâches officielles. L'accès est accordé indépendamment des autres droits, même s'ils interdisent l'accès Lire à des objets particuliers.

Zone fonctionnelle	Droit	Action utilisateur : droit requis pour exécuter l'action	Tâche	Rapport	Autres
Fonctions générales : **Fonctionnalité de base**	• **Lire** • **Écrire** • **Exécuter** • **Réalisez des opérations sur les sélections d'appareils**	• Règles de déplacement des appareils (création, modification ou suppression) pour le Serveur virtuel : **Écrire**, **Réalisez des opérations sur les sélections d'appareils** • Définir le certificat personnalisé du protocole mobile (LWNGT) : **Lire** • Définir le certificat personnalisé du protocole mobile (LWNGT) : **Écrire** • Obtenir la liste des réseaux définis par NLA : **Lire** • Ajouter, modifier ou supprimer une liste de réseaux définie par NLA : **Écrire** • Afficher la liste de contrôle d'accès des groupes : **Lire** • Afficher le journal des événements Kaspersky : **Lire** • Afficher la clé de récupération pour restaurer l'accès à un disque dur chiffré par le chiffrement de disque BitLocker : **Exécuter**	• " Télécharger les mises à jour dans le stockage du Serveur d'administration " • "Livrer des rapports" • "Diffusion du paquet d'installation" • "Installation des applications sur les Serveurs d'administration secondaires à distance"	• "Rapport sur l'état de la protection" • "Rapport sur les menaces" • "Rapport sur les appareils les plus infectés" • "Rapport sur l'état des bases antivirus" • "Rapport sur les erreurs" • "Rapport sur les attaques réseau" • " Rapport de synthèse sur les applications de sécurité des systèmes de messagerie installées " • " Rapport de synthèse sur les applications de défense de périmètre installés " • "Rapport de synthèse sur les types d'application installés" • "Rapport sur les utilisateurs des appareils infectés" • " Rapport d'incidents " • "Rapport sur les événements" • " Rapport de fonctionnement des Points de distribution " • " Rapport sur les Serveurs d'administration secondaires " • " Rapport sur les événements du Contrôle des appareils " • "Rapport sur les vulnérabilités" • "Rapport sur les applications interdites" • "Rapport sur le fonctionnement du Contrôle Internet" • " Rapport de l'état de chiffrement des	Aucun

Zone fonctionnelle	Droit	Action utilisateur : droit requis pour exécuter l'action	Tâche	Rapport	Autres
				appareils administrés " • " Rapport de l'état de chiffrement des appareils de stockage de masse " • " Rapport sur les erreurs de chiffrement des fichiers " • " Rapport sur le blocage de l'accès aux fichiers chiffrés " • " Rapport sur les privilèges d'accès aux appareils chiffrés " • " Rapport sur les droits effectifs de l'utilisateur " • "Rapport sur les privilèges"	
Fonctions générales : **Objets supprimés**	• **Lire** • **Écrire**	• Afficher les objets supprimés dans la corbeille : **Lire** • Supprimer des objets de la corbeille : **Écrire**	Aucun	Aucun	Aucun
Fonctions générales : **Traitement des événements**	• **Supprimer les événements** • **Modifier les paramètres de notification des événements** • **Modifier les paramètres d'enregistrement des événements dans le journal** • **Écrire**	• Modifier les paramètres d'enregistrement des événements : **Modifier les paramètres d'enregistrement des événements dans le journal** • Modifier les paramètres de notification d'événements **Modifier les paramètres de notification des événements** • Supprimer des événements : **Supprimer les événements**	Aucun	Aucun	Paramètres : • Paramètres de propagation de virus : nombre de détections de virus nécessaires pour créer un événement d'épidémie virale • Paramètres de propagation de virus : période de temps pour l'évaluation des détections de virus • Le nombre maximal d'événements stockés dans la base de données • Période de stockage des événements des appareils supprimés

Zone fonctionnelle	Droit	Action utilisateur : droit requis pour exécuter l'action	Tâche	Rapport	Autres
Fonctions générales : **Opérations avec le Serveur d'administration**	• **Lire** • **Écrire** • **Exécuter** • **Modifier les ACL d'objet** • **Réalisez des opérations sur les sélections d'appareils**	• Spécifier les ports du Serveur d'administration pour la connexion de l'Agent d'administration : **Écrire** • Spécifier les ports du proxy d'activation lancé sur le Serveur d'administration : **Écrire** • Spécifier les ports du proxy d'activation pour les appareils mobiles lancé sur le Serveur d'administration : **Écrire** • Spécifier les ports du serveur Web pour la distribution des paquets autonomes : **Écrire** • Spécifier les ports du serveur Web pour la distribution des profils MDM : **Écrire** • Spécifier les ports SSL du Serveur d'administration pour la connexion via Kaspersky Security Center Web Console : **Écrire** • Spécifier les ports du Serveur d'administration pour la connexion mobile : **Écrire** • Modifier le nombre maximal d'événements stockés dans la base de données du Serveur d'administration : **Écrire** • Spécifier le nombre maximum d'événements pouvant être envoyés par le Serveur d'administration : **Écrire** • Spécifier la période pendant laquelle les événements peuvent être envoyés par le Serveur d'administration : **Écrire**	• "Sauvegarde des données du Serveur d'administration" • "Maintenance de la base de données"	Aucun	Aucun

Zone fonctionnelle	Droit	Action utilisateur : droit requis pour exécuter l'action	Tâche	Rapport	Autres
Fonctions générales : **Déploiement de l'application Kaspersky**	• **Administration des correctifs de Kaspersky** • **Lire** • **Écrire** • **Exécuter** • **Réalisez des opérations sur les sélections d'appareils**	Approuver ou refuser l'installation du correctif : **Administration des correctifs de Kaspersky**	Aucun	• "Rapport sur les clés de licence utilisées par le Serveur d'administration virtuel" • "Rapport sur les versions des applications Kaspersky" • "Rapport sur les applications incompatibles" • "Rapport sur les versions des mises à jour du module logiciel Kaspersky" • " Rapport sur le déploiement de la protection "	Paquet d'installation : " Kaspersky "
Fonctions générales : **Administration des clés de licence**	• **Exporter le fichier clé** • **Écrire**	• Exporter le fichier clé : **Exporter le fichier clé** • Modifier les paramètres de clé de licence du Serveur d'administration : **Écrire**	Aucun	Aucun	Aucun
Fonctions générales : **Administration des rapports mise en œuvre**	• **Lire** • **Écrire**	• Créer des rapports quel que soit leur ACL : **Écrire** • Exécuter des rapports quel que soit leur ACL : **Lire**	Aucun	Aucun	Aucun
Fonctions générales : **Hiérarchie des Serveurs d'administration**	**Configurer la hiérarchie des Serveurs d'administration**	Enregistrer, mettre à jour ou supprimer des Serveurs d'administration secondaires : **Configurer la hiérarchie des Serveurs d'administration**	Aucun	Aucun	Aucun

Zone fonctionnelle	Droit	Action utilisateur : droit requis pour exécuter l'action	Tâche	Rapport	Autres
Fonctions générales : **Autorisations utilisateur**	**Modifier les ACL d'objet**	• Modifier les propriétés Sécurité de n'importe quel objet : **Modifier les ACL d'objet** • Gérer les rôles utilisateur : **Modifier les ACL d'objet** • Gérer les utilisateurs internes : **Modifier les ACL d'objet** • Gérer les groupes de sécurité : **Modifier les ACL d'objet** • Gérer les alias : **Modifier les ACL d'objet**	Aucun	Aucun	Aucun
Fonctions générales : **Serveurs d'administration virtuels**	• **Administrer les serveurs virtuels** • **Lire** • **Écrire** • **Exécuter** • **Réalisez des opérations sur les sélections d'appareils**	• Obtenir la liste des Serveurs d'administration virtuels : **Lire** • Obtenir des informations sur le Serveur d'administration virtuel : **Lire** • Créer, mettre à jour ou supprimer un Serveur d'administration virtuel : **Administrer les serveurs virtuels** • Déplacer un Serveur d'administration virtuel vers un autre groupe : **Administrer les serveurs virtuels** • Définir les autorisations du Serveur virtuel d'administration : **Administrer les serveurs virtuels**	Aucun	" Rapport sur les résultats de l'installation des mises à jour du logiciel tiers "	Aucun
Fonctions générales : **Gestion des clés de chiffrement**	**Écrire**	Importer les clés de chiffrement : **Écrire**	Aucun	Aucun	Aucun

Zone fonctionnelle	Droit	Action utilisateur : droit requis pour exécuter l'action	Tâche	Rapport	Autres
Administration des appareils mobiles : Général	• **Connexion des nouveaux appareils** • **Envoi uniquement des commandes d'information sur les appareils mobiles** • **Envoi des commandes sur les appareils mobiles** • **Administrer les certificats** • **Lire** • **Écrire**	• Obtenir les données de restauration du service de gestion des clés : **Lire** • Supprimer les certificats utilisateur : **Administrer les certificats** • Obtenir la partie publique du certificat utilisateur : **Lire** • Vérifier si l'infrastructure à clé publique est activée : **Lire** • Vérifier le compte d'infrastructure à clé publique : **Lire** • Obtenir des modèles d'infrastructure à clé publique : **Lire** • Obtenir des modèles d'infrastructure de clé publique par certificat d'utilisation de clé étendue : **Lire** • Vérifier si le certificat d'infrastructure à clé publique est révoqué : **Lire** • Mettre à jour les paramètres d'émission des certificats utilisateur : **Administrer les certificats** • Obtenir les paramètres d'émission de certificat utilisateur : **Lire** • Obtenir des paquets par nom d'application et par version : **Lire** • Définir ou annuler le certificat utilisateur : **Administrer les certificats** • Renouveler le certificat utilisateur : **Administrer les certificats** • Définir la balise de certificat utilisateur : **Administrer les certificats**	Aucun	Aucun	Aucun

Zone fonctionnelle	Droit	Action utilisateur : droit requis pour exécuter l'action	Tâche	Rapport	Autres
		• Exécuter la génération du paquet d'installation MDM ; annuler la génération du paquet d'installation MDM : **Connexion des nouveaux appareils**			
Administration du système : Connectivité	• **Démarrage des sessions RDP** • **Connectez-vous aux sessions RDP existantes** • **Initier le creusement** • **Enregistrer les fichiers des appareils sur le poste de travail de l'administrateur** • **Lire** • **Écrire** • **Exécuter** • **Réalisez des opérations sur les sélections d'appareils**	• Créer une session de partage du bureau : **Démarrage des sessions RDP** • Créer une session RDP : **Connectez-vous aux sessions RDP existantes** • Créer un tunnel : **Initier le creusement** • Enregistrer la liste des réseaux de contenu : **Enregistrer les fichiers des appareils sur le poste de travail de l'administrateur**	Aucun	" Rapport sur les utilisateurs de l'appareil "	Aucun
Administration du système : Inventaire du matériel	• **Lire** • **Écrire** • **Exécuter** • **Réalisez des opérations sur les sélections d'appareils**	• Obtenir ou exporter un objet d'inventaire matériel : **Lire** • Ajouter, définir ou supprimer un objet d'inventaire matériel : **Écrire**	Aucun	• " Rapport sur le registre du matériel " • " Rapport sur les changements de configuration " • " Rapport sur le matériel "	Aucun
Administration du système : Administration d'accès au réseau	• **Lire** • **Écrire**	• Afficher les paramètres CISCO : **Lire** • Modifier les paramètres CISCO : **Écrire**	Aucun	Aucun	Aucun

Zone fonctionnelle	Droit	Action utilisateur : droit requis pour exécuter l'action	Tâche	Rapport	Autres
Administration du système : Déploiement du système d'exploitation	• **Déploiement des serveurs PXE** • **Lire** • **Écrire** • **Exécuter** • **Réalisez des opérations sur les sélections d'appareils**	• Déployer les serveurs PXE : **Déploiement des serveurs PXE** • Afficher une liste de serveurs PXE : **Lire** • Démarrer ou arrêter le processus d'installation sur les clients PXE : **Exécuter** • Gérer les pilotes pour WinPE et les images du système d'exploitation : **Écrire**	" Créer un paquet d'installation sur l'image du système d'exploitation de l'appareil de référence "	Aucun	Paquet d'installation : " OS Image "
Administration du système : Gestion des vulnérabilités et des correctifs	• **Lire** • **Écrire** • **Exécuter** • **Réalisez des opérations sur les sélections d'appareils**	• Afficher les propriétés des correctifs tiers : **Lire** • Modifier les propriétés des correctifs tiers : **Écrire**	• " Synchronisation de Windows Update " • " Installer les mises à jour de Windows Update " • " Corriger les vulnérabilités " • "Installation des mises à jour requises et correction des vulnérabilités"	"Rapport sur les mises à jour des logiciels"	Aucun
Administration du système : Installation à distance	• **Lire** • **Écrire** • **Exécuter** • **Réalisez des opérations sur les sélections d'appareils**	• Afficher les propriétés du paquet d'installation tiers basé sur la gestion des vulnérabilités et des correctifs : **Lire** • Modifier les propriétés du paquet d'installation tiers basé sur la gestion des vulnérabilités et des correctifs : **Écrire**	Aucun	Aucun	Paquets d'installation : • " Application personnalisée " • " Paquet VAPM "

Zone fonctionnelle	Droit	Action utilisateur : droit requis pour exécuter l'action	Tâche	Rapport	Autres
Administration du système : Inventaire des applications	• **Lire** • **Écrire** • **Exécuter** • **Réalisez des opérations sur les sélections d'appareils**	Aucun	Aucun	• " Rapport sur les applications installées " • " Rapport sur l'historique du registre des applications " • " Rapport sur l'état des groupes des applications sous licence " • " Rapport sur les clés de licence des applications tierces "	Aucun
Administration du système : Exécuter des scripts à distance	• **Lire** • **Écrire** • **Exécuter** • **Réalisez des opérations sur les sélections d'appareils**	L'utilisateur peut consulter les propriétés de la tâche : **Lire** L'utilisateur peut créer, supprimer ou modifier un paquet d'installation : **Écrire** L'utilisateur peut exécuter une tâche : **Écrire**. Sur les appareils clients Linux, les scripts sont exécutés avec les privilèges root. L'utilisateur peut exécuter une tâche ou planifier son exécution : **Exécuter** L'utilisateur peut exécuter une tâche sur une sélection d'appareils : **Réalisez des opérations sur les sélections d'appareils**	" Exécuter des scripts à distance "	Aucun	Aucun

À propos des rôles d'utilisateurs prédéfinis

Les rôles d'utilisateurs attribués aux utilisateurs de Kaspersky Security Center leur fournissent des ensembles d'autorisations d'accès aux fonctionnalités des applications.

Les utilisateurs créés sur un Serveur virtuel ne peuvent pas se voir attribuer un rôle sur le Serveur d'administration.

Vous pouvez utiliser les rôles d'utilisateurs prédéfinis avec un ensemble de droits déjà configurés, ou créer des rôles. Dans ce cas, vous devez définir vous-même la portée du rôle et attribuer les droits d'accès aux fonctionnalités de Kaspersky Security Center. Certains des rôles d'utilisateurs prédéfinis disponibles dans Kaspersky Security Center peuvent être associés à des fonctions spécifiques, par exemple, **Auditeur**, **Responsable de la sécurité**, **Superviseur** (ces rôles sont présents dans Kaspersky Security Center à partir de la version 11). Les droits d'accès de ces rôles sont préconfigurés conformément aux tâches standard et à l'étendue des tâches des fonctions associées. Le tableau ci-dessous montre comment les rôles suivants peuvent être associés à des fonctions spécifiques.

Exemples de rôles pour des fonctions particulières

Rôle	Commentaire
Auditeur	Autorise la consultation et l'exécution de toutes les tâches créées sur les appareils sélectionnés connectés au Serveur d'administration via l'Agent d'administration avec des privilèges d'administrateur local (root pour Linux). Nous recommandons d'attribuer ce rôle prudemment et à un nombre limité d'utilisateurs qui en ont besoin pour l'accomplissement de leurs tâches officielles.
Superviseur	Autorise toutes les opérations d'affichage, n'autorise pas les autres opérations. Vous pouvez attribuer ce rôle à un responsable de la sécurité et à d'autres responsables chargé de la sécurité de l'information dans votre organisation.
Responsable de la sécurité	Autorise toutes les informations de consultation, autorise la gestion des rapports, octroie des permissions restreintes dans les domaines **Administration du système** : **Connectivité**. Vous pouvez attribuer ce rôle à la personne chargée de la sécurité de l'information dans votre organisation.

Le tableau ci-dessous montre les droits d'accès attribués à chaque rôle d'utilisateur prédéfini.

Droits d'accès des rôles utilisateur prédéfinis

Rôle	Description

Administrateur du Serveur d'administration	Permet toutes les opérations dans les domaines fonctionnels suivants :
	• **Caractéristiques générales** :
	  • **Fonctionnalité de base**
	  • **Traitement des événements**
	  • **Hiérarchie des Serveurs d'administration**
	  • **Serveurs d'administration virtuels**
	• **Administration du système :**
	  • **Connectivité**
	  • **Inventaire du matériel**
	  • **Inventaire des applications**
	
	Accorde les droits de **lecture** et d'**écriture** dans la zone fonctionnelle **Caractéristiques générales : Gestion des clés de chiffrement**.

Opérateur du Serveur d'administration	Accorde les droits de **lecture** et d' **exécution** dans tous les domaines fonctionnels suivants :
	• **Caractéristiques générales** :
	  • **Fonctionnalité de base**
	  • **Serveurs d'administration virtuels**
	• **Administration du système :**
	  • **Connectivité**
	  • **Inventaire du matériel**
	  • **Inventaire des applications**

Rôle	Description
Auditeur	Permet toutes les opérations dans les zones fonctionnelles, dans **Fonctions générales** : • **Accéder aux objets quel que soit leur ACL** • **Objets supprimés** • **Administration des rapports mise en œuvre** Vous pouvez attribuer ce rôle à une personne qui réalise un audit de votre organisation.

Administrateur d'installation	Permet toutes les opérations dans les domaines fonctionnels suivants :
	• **Caractéristiques générales** :
	  • **Fonctionnalité de base**
	  • **Déploiement de logiciels Kaspersky**
	  • **Gestion des clés de licence**
	• **Administration du système :**
	  • **Déploiement du système d'exploitation**
	  • **Gestion des vulnérabilités et des correctifs**
	  • **Installation à distance**
	  • **Inventaire des applications**
	Accorde les droits de **lecture** et d'**exécution** dans la zone fonctionnelle **Fonctionnalités générales : Serveurs d'administration virtuelle**.

Opérateur d'installation	Accorde les droits de **lecture** et d' **exécution** dans tous les domaines fonctionnels suivants :
	• **Caractéristiques générales** :
	  • **Fonctionnalité de base**
	  • **Déploiement de logiciels Kaspersky** (accorde également les **correctifs Manage Kaspersky** directement dans cette zone)
	  • **Serveurs d'administration virtuels**
	• **Administration du système :**
	  • **Déploiement du système d'exploitation**
	  • **Gestion des vulnérabilités et des correctifs**
	  • **Installation à distance**
	  • **Inventaire des applications**

Administrateur Kaspersky Endpoint Security	Permet toutes les opérations dans les domaines fonctionnels suivants : • **Caractéristiques générales : fonctionnalité de base** • Zone Kaspersky Endpoint Security, y compris toutes les fonctionnalités Accorde les droits de **lecture** et d'**écriture** dans la zone fonctionnelle **Caractéristiques générales : Gestion des clés de chiffrement**.
Opérateur Kaspersky Endpoint Security	Accorde les droits de **lecture** et d' **exécution** dans tous les domaines fonctionnels suivants : • **Caractéristiques générales : fonctionnalité de base** • Zone Kaspersky Endpoint Security, y compris toutes les fonctionnalités
Administrateur principal	Permet toutes les opérations dans les domaines fonctionnels, *à l'exception* des zones suivantes dans **Fonctions générales** : • **Accéder aux objets quel que soit leur ACL** • **Administration des rapports mise en œuvre** Accorde les droits de **lecture** et d'**écriture** dans la zone fonctionnelle **Caractéristiques générales : Gestion des clés de chiffrement**.

Rôle	Description

Opérateur principal	Accorde les droits de **lecture** et d' **exécution** (le cas échéant) dans tous les domaines fonctionnels suivants :
	• **Caractéristiques générales** :
	  • **Fonctionnalité de base**
	  • **Objets supprimés**
	  • **Opérations sur le Serveur d'administration**
	  • **Déploiement de l'application Kaspersky**
	  • **Serveurs d'administration virtuels**
	• **Administration des appareils mobiles : généralités**
	• **Gestion du système**, y compris toutes les fonctionnalités
	• Zone Kaspersky Endpoint Security, y compris toutes les fonctionnalités

Administrateur Administration des appareils mobiles	Permet toutes les opérations dans les domaines fonctionnels suivants : • **Caractéristiques générales : fonctionnalité de base** • **Administration des appareils mobiles : généralités**
Opérateur Administration des appareils mobiles	Accorde les droits de **lecture** et d'**exécution** dans la zone fonctionnelle **Fonctionnalités générales** : **Fonctionnalité de base**. Accorde des commandes de **lecture** et d'**envoi uniquement d'informations aux appareils mobiles** dans la zone fonctionnelle **Administration des appareils mobiles** : **Général**.
Responsable de la sécurité	Autorise toutes les opérations dans les domaines fonctionnels suivants, dans **Fonctions générales** : • **Accéder aux objets quel que soit leur ACL** • **Administration des rapports mise en œuvre** Accorde les droits **Lire**, **Écrire**, **Exécuter**, **Enregistrer les fichiers des appareils sur le poste de travail de l'administrateur** et **Réaliser des opérations sur les sélections d'appareils** dans la zone fonctionnelle **Administration du système : Connectivité**. Vous pouvez attribuer ce rôle à la personne chargée de la sécurité de l'information dans votre organisation.
Utilisateur du Self Service Portal	Autorise toutes les opérations dans la zone fonctionnelle **Administration des appareils mobiles : Self Service Portal**. Cette fonctionnalité n'est pas prise en charge par Kaspersky Security Center 11 ni par les versions ultérieures.
Superviseur	Accorde le droit de **lecture** dans les **fonctionnalités générales** : **objets d'accès quelles que soient leurs ACL** et **fonctionnalités générales** : **Administration des rapports mise en œuvre**. Vous pouvez attribuer ce rôle à un responsable de la sécurité et à d'autres responsables chargé de la sécurité de l'information dans votre organisation.
Administrateur de gestion des vulnérabilités et des correctifs	Permet toutes les opérations dans les zones fonctionnelles **Fonctionnalités générales** : **Fonctionnalité de base** et **Gestion du système** (y compris toutes les fonctionnalités).
Opérateur de gestion des vulnérabilités et des correctifs	Accorde les droits de **lecture** et d'**exécution** (le cas échéant) dans les zones fonctionnelles **Fonctionnalités générales** : **Fonctionnalités de base** et **Gestion du système** (y compris toutes les fonctionnalités).

Attribution de droits d'accès à des objets spécifiques

Outre l'attribution de droits d'accès au niveau du serveur, vous pouvez configurer l'accès à des objets spécifiques, par exemple, à une tâche spécifique. L'application permet de définir les droits d'accès aux types d'objets suivants :

- Groupes d'administration
- Tâches
- Rapports

- Sélections d'appareils
- Sélections d'événements

Pour attribuer des droits d'accès à un objet spécifique, procédez comme suit :

1. Selon le type d'objet, dans le menu principal, accédez à la section correspondante :
   - **Ressources (Appareils) → Hiérarchie des groupes**
   - **Ressources (Appareils) → Tâches**
   - **Surveillance et rapports → Rapports**
   - **Ressources (Appareils) → Sélections d'appareils**
   - **Surveillance et rapports → Sélections d'événements**
2. Ouvrez les propriétés de l'objet pour lequel vous souhaitez configurer les droits d'accès.

   Pour ouvrir la fenêtre des propriétés d'un groupe d'administration ou d'une tâche, cliquez sur le nom de l'objet. Les propriétés d'autres objets peuvent être ouvertes à l'aide du bouton de la barre d'outils.
3. Dans la fenêtre des propriétés, ouvrez la section **Privilèges d'accès**.

   La liste des utilisateurs s'ouvre. Les utilisateurs et les groupes de sécurité répertoriés disposent de droits d'accès à l'objet. Par défaut, si vous utilisez une hiérarchie de groupes d'administration ou de Serveurs, la liste et les droits d'accès sont hérités du groupe d'administration parent ou du Serveur primaire.
4. Pour pouvoir modifier la liste, activez l'option **Utiliser des autorisations personnalisées**.
5. Configurez les droits d'accès :
   - Utilisez les boutons **Ajouter** et **Supprimer** pour modifier la liste.
   - Spécifiez les droits d'accès pour un utilisateur ou un groupe de sécurité. Exécutez une des actions suivantes :
     - Si vous souhaitez définir les droits d'accès manuellement, sélectionnez l'utilisateur ou le groupe de sécurité, cliquez sur le bouton **Privilèges d'accès**, puis indiquez les droits d'accès.
     - Si vous souhaitez attribuer un rôle utilisateur à l'utilisateur ou au groupe de sécurité, sélectionnez l'utilisateur ou le groupe de sécurité, cliquez sur le bouton **Rôles**, puis sélectionnez le rôle à attribuer.
6. Cliquez sur le bouton **Enregistrer**.

Les droits d'accès à l'objet sont configurés.

Attribution de droits d'accès aux utilisateurs et aux groupes de sécurité

Vous pouvez octroyer aux utilisateurs et aux groupes de sécurité des droits d'accès pour utiliser différentes fonctionnalités du Serveur d'administration, par exemple, Kaspersky Endpoint Security for Linux.

Pour attribuer des droits d'accès à un utilisateur ou à un groupe de sécurité :

1. Dans le menu principal, cliquez sur l'icône des paramètres ( ) en regard du nom du Serveur d'administration requis.

   La fenêtre des propriétés du Serveur d'administration s'ouvre.

2. Sous l'onglet **Privilèges d'accès**, cochez la case en regard du nom de l'utilisateur ou du groupe de sécurité auquel attribuer des droits, puis cliquez sur le bouton **Privilèges d'accès**.

   Vous ne pouvez pas sélectionner plusieurs utilisateurs ou groupes de sécurité en même temps. Si vous sélectionnez plusieurs éléments, le bouton **Privilèges d'accès** sera désactivé.

3. Configurez l'ensemble des droits pour l'utilisateur ou le groupe :

   a. Développez le nœud avec les fonctionnalités du Serveur d'administration ou d'une autre application Kaspersky.

   b. Cochez la case **Autoriser** ou **Interdire** en regard de la fonctionnalité ou du droit d'accès souhaité.

      Exemple 1: cochez la case **Autoriser** en regard du nœud **Intégration des applications** pour accorder tous les droits d'accès disponibles à la fonctionnalité d'intégration d'application (**Lecture**, **Écriture** et **Exécution**) pour un utilisateur ou un groupe.

      Exemple 2: développez le nœud **Gestion des clés de chiffrement**, puis cochez la case **Autoriser** en regard de l'autorisation d'**écriture** pour accorder le droit d'accès en **écriture** à la fonctionnalité de gestion des clés de chiffrement pour un utilisateur ou un groupe.

4. Après avoir configuré l'ensemble des droits d'accès, cliquez sur **OK**.

L'ensemble des privilèges pour les utilisateurs ou les groupes d'utilisateurs sont alors configurés.

Les permissions du Serveur d'administration (ou du groupe d'administration) sont réparties dans les catégories suivantes :

- Fonctions générales :
  - Administration des groupes d'administration
  - Accéder aux objets quel que soit leur ACL
  - Fonctionnalité de base
  - Objets supprimés
  - Gestion des clés de chiffrement
  - Traitement des événements
  - Opérations avec le Serveur d'administration (uniquement dans la fenêtre des propriétés du Serveur d'administration)
  - Tags de l'appareil
  - Déploiement de l'application Kaspersky
  - Administration des clés de licence
  - Intégration de l'application
  - Administration des rapports mise en œuvre
  - Hiérarchie des Serveurs d'administration
  - Autorisations utilisateur
  - Serveurs d'administration virtuels
- Administration des appareils mobiles :
  - Général
  - Self Service Portal
- Administration du système :
  - Connectivité
  - Exécuter des scripts à distance
  - Inventaire du matériel
  - Administration d'accès au réseau
  - Déploiement du système d'exploitation
  - Gestion des vulnérabilités et des correctifs

- Installation à distance
- Inventaire des applications

Si aucune des options **Autoriser** ou **Interdire** n'est sélectionnée pour un droit d'accès, ce droit est considérée comme *non défini* : il persiste tant qu'il n'a pas été explicitement autorisé ou interdit pour l'utilisateur.

Les privilèges d'un utilisateur sont la somme des éléments suivants :

- Propres privilèges de l'utilisateur
- Privilèges de tous les rôles attribués à cet utilisateur
- Privilèges de tous les groupe de sécurité auxquels l'utilisateur appartient
- Les privilèges de tous les rôles attribués aux groupes de sécurité auxquels l'utilisateur appartient

Si au moins un de ces ensembles de privilèges a la valeur **Interdire** pour une permission, celle-ci n'est pas accordée à l'utilisateur, même si d'autres ensembles l'autorisent ou ne la définissent pas.

Vous pouvez également ajouter des utilisateurs et des groupes de sécurité à la portée d'un rôle d'utilisateur pour utiliser les différentes fonctionnalités du Serveur d'administration. Les paramètres associés à un rôle d'utilisateur s'appliqueront uniquement aux appareils qui appartiennent aux utilisateurs qui ont ce rôle et uniquement si ces appareils appartiennent aux groupes associés à ce rôle, y compris les groupes enfant.

Ajout d'un compte d'un utilisateur interne

Si vous souhaitez ajouter un compte utilisateur, assurez-vous que votre compte dispose du droit Modifier les ACL des objets dans la zone fonctionnelle Caractéristiques générales : Autorisations utilisateur.

Pour ajouter un nouveau compte d'utilisateur interne à Kaspersky Security Center, procédez comme suit :

1. Dans le menu principal, accédez à **Utilisateurs et rôles** → **Utilisateurs et groupes**, puis sélectionnez l'onglet **Utilisateurs**.
2. Cliquez sur **Ajouter**.

3. Dans la fenêtre **Ajouter un utilisateur** qui s'ouvre, définissez les paramètres du nouveau compte utilisateur :

   - **Nom**
   - **Mot de passe**

     Le mot de passe doit remplir les conditions suivantes :

     - Le mot de passe doit compter entre 8 et 256 caractères.
     - Le mot de passe doit compter des caractères d'au moins trois des groupes ci-dessous :
       - Lettres majuscules (A-Z)
       - Lettre minuscules (a-z)
       - Chiffres (0-9)
       - Caractères spéciaux (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
     - Le mot de passe ne peut pas contenir d'espaces, de caractères Unicode ou de la combinaison " . " et " @ " lorsque " . " est placé devant " @ ".

     Pour consulter le mot de passe saisi, cliquez sur .

     Vous pouvez activer l'option **L'utilisateur doit changer son mot de passe lors de la première connexion** pour forcer la modification du mot de passe lors de la première authentification de l'utilisateur.

4. Enregistrez les modifications pour terminer la création d'un compte utilisateur.

Un nouveau compte utilisateur est ajouté à la liste des utilisateurs.

Création d'un groupe de sécurité

Pour créer un groupe de sécurité, procédez comme suit :

1. Dans le menu principal, accédez à **Utilisateurs et rôles** → **Utilisateurs et groupes**, puis sélectionnez l'onglet **Groupes**.
2. Cliquez sur **Ajouter**.
3. Dans la fenêtre **Créer un groupe de sécurité** qui s'ouvre, spécifiez les paramètres suivants pour le nouveau groupe de sécurité :

   - **Nom du groupe**
   - **Description**

4. Cliquez sur le bouton **Enregistrer** afin d'enregistrer les modifications.

Un nouveau groupe de sécurité est ajouté à la liste des groupes.

Modification d'un compte d'un utilisateur interne

Si vous souhaitez modifier un compte utilisateur, assurez-vous que votre compte dispose du droit Modifier les ACL des objets dans la zone fonctionnelle Caractéristiques générales : Autorisations utilisateur.

Pour modifier le compte d'un utilisateur interne dans Kaspersky Security Center, procédez comme suit :

1. Dans le menu principal, accédez à **Utilisateurs et rôles** → **Utilisateurs et groupes**, puis sélectionnez l'onglet **Utilisateurs**.

2. Cliquez sur le nom du compte utilisateur que vous souhaitez modifier.

3. Dans la fenêtre des paramètres de l'utilisateur qui s'ouvre, sous l'onglet **Général**, modifiez les paramètres du compte utilisateur :

   - **État de l'utilisateur**

     Le cas échéant, placez le commutateur en position **Désactivé** pour empêcher la connexion de l'utilisateur à l'application. Vous pouvez désactiver un compte après qu'un employé a arrêté de travailler pour l'entreprise, par exemple.

   - **Nom**
   - **Nom complet**
   - **Description**
   - **Adresse email**
   - **Numéro de téléphone principal**
   - **Mot de passe**

     En cas de nécessité, vous pouvez définir un nouveau mot de passe pour la connexion de l'utilisateur à Kaspersky Security Center comme suit :

     a. Cliquez sur le bouton **Modifier le mot de passe**, puis définissez un nouveau mot de passe pour le compte utilisateur.

     Le mot de passe doit remplir les conditions suivantes :

     - Le mot de passe doit compter entre 8 et 256 caractères.
     - Le mot de passe doit compter des caractères d'au moins trois des groupes ci-dessous :
       - Lettres majuscules (A-Z)
       - Lettre minuscules (a-z)
       - Chiffres (0-9)
       - Caractères spéciaux (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
     - Le mot de passe ne peut pas contenir d'espaces, de caractères Unicode ou de la combinaison " . " et " @ " lorsque " . " est placé devant " @ ".

     Pour consulter le mot de passe saisi, cliquez sur .

     b. Si nécessaire, vous pouvez activer l'option **L'utilisateur doit changer son mot de passe lors de la première connexion** pour forcer la modification du mot de passe lors de l'authentification de l'utilisateur suivante.

     c. Si le compte utilisateur est protégé contre les modifications non autorisées, vous devez confirmer que vous avez les autorisations pour modifier le compte en question. Dans la fenêtre **Protection du compte**, indiquez les identifiants du compte disposant du droit Modifier les ACL des objets dans la zone fonctionnelle Caractéristiques générales : Autorisations utilisateur.

4. Dans l'onglet **Sécurité d'authentification**, vous pouvez spécifier les paramètres de sécurité de ce compte.
5. Sous l'onglet **Groupes**, vous pouvez ajouter l'utilisateur à des groupes de sécurité.
6. Sous l'onglet **Appareils**, vous pouvez attribuer des appareils à l'utilisateur.
7. Sous l'onglet **Rôles**, vous pouvez attribuer des rôles à l'utilisateur.
8. Enregistrez les modifications pour terminer la modification du compte utilisateur.

Le compte utilisateur mis à jour apparaît dans la liste des utilisateurs.

Modification d'un groupe de sécurité

Pour modifier un groupe de sécurité, procédez comme suit :

1. Dans le menu principal, accédez à **Utilisateurs et rôles** → **Utilisateurs et groupes**, puis sélectionnez l'onglet **Groupes**.
2. Cliquez sur le nom du groupe de sécurité que vous souhaitez modifier.
3. Dans la fenêtre des paramètres de groupe qui s'ouvre, modifiez les paramètres du groupe de sécurité :
   - Sous l'onglet **Général**, vous pouvez modifier les paramètres **Nom** et **Description**. Ces paramètres sont disponibles uniquement pour les groupes de sécurité internes.
   - L'onglet **Utilisateurs** permet d'ajouter des utilisateurs au groupe de sécurité. Ce paramètre est disponible uniquement pour les utilisateurs internes et les groupes de sécurité internes.
   - Sous l'onglet **Rôles**, vous pouvez attribuer le rôle au groupe de sécurité.
4. Cliquez sur le bouton **Enregistrer** afin d'enregistrer les modifications.

Les modifications sont appliquées au groupe de sécurité.

Attribution d'un rôle à un utilisateur ou à un groupe de sécurité

Pour attribuer un rôle à un utilisateur ou à un groupe de sécurité :

1. Dans le menu principal, accédez à **Utilisateurs et rôles** → **Utilisateurs et groupes**, puis sélectionnez l'onglet **Utilisateurs** ou **Groupes**.
2. Sélectionnez le nom de l'utilisateur ou du groupe de sécurité auquel vous voulez attribuer un rôle.

   Il est possible de choisir plusieurs noms.

3. Dans la ligne de menu, cliquez sur le bouton **Attribuer un rôle**.

   L'Assistant d'attribution de rôle se lance.

4. Suivez les instructions de l'assistant : sélectionnez le rôle que vous souhaitez attribuer aux utilisateurs sélectionnés ou aux groupes de sécurité, et puis sélectionnez la zone du rôle.

   La portée du rôle d'utilisateur est un ensemble d'utilisateurs et de groupes d'administration. Les paramètres associés à un rôle d'utilisateur s'appliquent uniquement aux appareils qui appartiennent aux utilisateurs qui ont ce rôle et uniquement si ces appareils appartiennent aux groupes associés à ce rôle, y compris les groupes enfant.

Le rôle comprenant l'ensemble de privilèges concernant l'utilisation du Serveur d'administration sera ainsi attribué à l'utilisateur (ou aux utilisateurs, ou au groupe de sécurité). Dans la liste des utilisateurs ou des groupes de sécurité, une case à cocher s'affiche dans la colonne **Possède des rôles**.

Les utilisateurs créés sur un Serveur virtuel ne peuvent pas se voir attribuer un rôle sur le Serveur d'administration.

Ajout de comptes utilisateurs à un groupe de sécurité interne

Vous ne pouvez ajouter des comptes utilisateurs internes qu'à un groupe de sécurité interne.

Pour ajouter des comptes utilisateurs à un groupe de sécurité interne :

1. Dans le menu principal, accédez à **Utilisateurs et rôles** → **Utilisateurs et groupes**, puis sélectionnez l'onglet **Utilisateurs**.

2. Cochez les cases en regard des comptes utilisateurs que vous souhaitez ajouter à un groupe de securité.

3. Cliquez sur le bouton **Attribuer un groupe**.

4. Dans la fenêtre **Attribuer un groupe** qui s'ouvre, sélectionnez le groupe de securité auquel vous voulez ajouter des comptes utilisateurs.

5. Cliquez sur **Enregistrer**.

Les comptes utilisateurs sont ajoutés au groupe de sécurité. Vous pouvez également ajouter des utilisateurs internes à un groupe de sécurité à l'aide des paramètres du groupe.

Désignation d'un utilisateur en tant que propriétaire de l'appareil

Pour obtenir plus d'informations sur l'attribution d'un utilisateur en tant que propriétaire de l'appareil mobile, consultez l'aide de Kaspersky Security for Mobile.

Pour désigner un utilisateur en tant que propriétaire de l'appareil, procédez comme suit :

1. Si vous souhaitez désigner le propriétaire d'un appareil connecté à un Serveur d'administration virtuel, basculez d'abord sur le Serveur d'administration virtuel :

   a. Dans le menu principal, cliquez sur l'icône en forme de chevron (›) à droite du nom actuel du Serveur d'administration.

   b. Sélectionnez le Serveur d'administration requis.

2. Dans le menu principal, accédez à **Utilisateurs et rôles** → **Utilisateurs et groupes**, puis sélectionnez l'onglet **Utilisateurs**.

   Une liste d'utilisateurs s'ouvre. Si vous êtes actuellement connecté à un Serveur d'administration virtuel, la liste comprend les utilisateurs du Serveur d'administration virtuel actuel et du Serveur d'administration principal.

3. Cliquez sur le nom du compte utilisateur que vous souhaitez désigner comme propriétaire de l'appareil.

4. Dans la fenêtre des paramètres utilisateur qui s'ouvre, sélectionnez l'onglet **Appareils**.

5. Cliquez sur **Ajouter**.

6. Dans la liste des appareils, sélectionnez l'appareil que vous voulez attribuer à l'utilisateur.

7. Cliquez sur le bouton **OK**.

L'appareil sélectionné est ajouté à la liste des appareils attribués à l'utilisateur.

Vous pouvez effectuer la même opération dans **Ressources (Appareils)** → **Appareils administrés**, en cliquant sur le nom de l'appareil que vous voulez attribuer, puis en cliquant sur le lien **Administrer le propriétaire de l'appareil**.

Configuration de la vérification en deux étapes pour tous les utilisateurs

Ce scénario décrit comment activer la vérification en deux étapes pour tous les utilisateurs et comment exclure des comptes utilisateurs de la vérification en deux étapes. Si vous n'avez pas activé la vérification en deux étapes pour votre compte avant de l'activer pour les autres utilisateurs, l'application ouvre d'abord la fenêtre permettant d'activer la vérification en deux étapes pour votre compte. Ce scénario décrit également comment activer la vérification en deux étapes pour votre propre compte.

> Si vous avez activé la vérification en deux étapes pour votre compte, vous pouvez passer à la phase d'activation de la vérification en deux étapes.

Prérequis

Avant de commencer :

- Assurez-vous que votre compte utilisateur dispose du droit Modifier les ACL des objets de la zone fonctionnelle **Fonctionnalités générales : Autorisations utilisateur** pour modifier les paramètres de sécurité des comptes pour d'autres utilisateurs.
- Assurez-vous que les autres utilisateurs du Serveur d'administration installent une application d'authentification sur leurs appareils.

Étapes

L'activation de la vérification en deux étapes pour tous les utilisateurs se déroule par étapes :

1. **Installation d'une application d'authentification sur un appareil**

   Vous pouvez installer n'importe quelle application prenant en charge l'algorithme du mot de passe à usage unique (TOTP), par exemple :

   - Authentificateur Google
   - Authentification Microsoft
   - OTP Bitrix24
   - Clé Yandex
   - Authentificateur Avanpost
   - Aladdin 2FA

   Pour vérifier si Kaspersky Security Center prend en charge l'application d'authentification que vous souhaitez utiliser, activez la vérification en deux étapes pour tous les utilisateurs ou pour un utilisateur en particulier.

   L'une des étapes propose d'indiquer le code de sécurité généré par l'application d'authentification. Si l'opération réussit, Kaspersky Security Center prend en charge l'authentificateur sélectionné.

   > Il est fortement déconseillé d'installer l'application d'authentification sur l'appareil à partir duquel la connexion au Serveur d'administration est établie.

2. **Synchronisation de l'heure de l'application d'authentification définie avec l'heure de l'appareil sur lequel le Serveur d'administration est installé**

   Assurez-vous que l'heure de l'appareil avec l'application d'authentification et l'heure de l'appareil avec le Serveur d'administration sont synchronisées au format UTC, en utilisant des sources externes. Dans le cas contraire, des échecs peuvent se produire lors de l'authentification et de l'activation de la vérification en deux étapes.

3. **Activation de la vérification en deux étapes pour votre compte et réception de la clé secrète de votre compte**

   Instructions pour :

   - Pour la Console d'administration basée sur MMC : activation de la vérification en deux étapes de votre propre compte
   - Pour Kaspersky Security Center Web Console : activation de la vérification en deux étapes pour votre propre compte

   Une fois que vous avez activé la vérification en deux étapes pour votre compte, vous pouvez activer la vérification en deux étapes pour tous les utilisateurs.

4. **Activation de la vérification en deux étapes pour tous les utilisateurs**

   Les utilisateurs dont la vérification en deux étapes est activée doivent l'utiliser pour se connecter au Serveur d'administration.

   Instructions pour :

- Pour la Console d'administration basée sur MMC : activation de la vérification en deux étapes pour tous les utilisateurs
- Pour Kaspersky Security Center Web Console : activation de la vérification en deux étapes pour tous les utilisateurs

5. **Modification du nom d'un émetteur de code de sécurité**

   Si vous disposez de plusieurs Serveurs d'administration avec des noms semblables, vous devrez peut-être modifier les noms des émetteurs de code de sécurité pour mieux reconnaître les différents Serveurs d'administration.

   Instructions pour :

   - Pour la Console d'administration basée sur MMC : modification du nom de l'émetteur du code de sécurité
   - Pour Kaspersky Security Center Web Console : modification du nom d'un émetteur de code de sécurité

6. **Exclusion des comptes utilisateurs pour lesquels vous n'avez pas besoin d'activer la vérification en deux étapes**

   Si nécessaire, vous pouvez exclure des utilisateurs de la vérification en deux étapes. Les utilisateurs avec des comptes exclus n'ont pas à utiliser la vérification en deux étapes pour se connecter au Serveur d'administration.

   Instructions pour :

   - Pour la Console d'administration basée sur MMC : exclusion des comptes de la vérification en deux étapes
   - Pour Kaspersky Security Center Web Console : exclusion de comptes de la vérification en deux étapes

7. **Configuration de la vérification en deux étapes pour votre compte**

   Si les utilisateurs ne sont pas exclus de la vérification en deux étapes et si la vérification en deux étapes n'est pas encore configurée pour leurs comptes, ils doivent la configurer dans la fenêtre qui s'ouvre lorsqu'ils se connectent à Kaspersky Security Center. Dans le cas contraire, il ne pourra pas accéder au Serveur d'administration conformément à ses privilèges.

   Instructions pour :

   - Pour la Console d'administration basée sur MMC : configuration de la vérification en deux étapes de votre propre compte
   - Pour Kaspersky Security Center Web Console : Configuration de la vérification en deux étapes pour votre propre compte

Résultats

À la fin de ce scénario :

- La vérification en deux étapes est activée pour votre compte.
- La vérification en deux étapes est activée pour tous les comptes utilisateurs du Serveur d'administration, à l'exception des comptes utilisateurs qui ont été exclus.

À propos de la vérification en deux étapes

Lorsque la vérification en deux étapes est activée pour un compte, un code de sécurité à usage unique est requis pour se connecter à la Console d'Administration ou à Kaspersky Security Center Web Console en plus du nom d'utilisateur et du mot de passe. L'authentification de domaine étant activée, il suffit à l'utilisateur de saisir le code de sécurité à usage unique.

Pour utiliser la vérification en deux étapes, installez une application d'authentification qui génère des codes de sécurité à usage unique sur l'appareil mobile ou l'ordinateur. Vous pouvez utiliser n'importe quelle application prenant en charge l'algorithme du mot de passe à usage unique (TOTP), par exemple :

- Authentificateur Google
- Authentification Microsoft
- OTP Bitrix24
- Clé Yandex
- Authentificateur Avanpost
- Aladdin 2FA

Pour vérifier si Kaspersky Security Center prend en charge l'application d'authentification que vous souhaitez utiliser, activez la vérification en deux étapes pour tous les utilisateurs ou pour un utilisateur en particulier.

L'une des étapes propose d'indiquer le code de sécurité généré par l'application d'authentification. Si l'opération réussit, Kaspersky Security Center prend en charge l'authentificateur sélectionné.

Nous vous recommandons vivement d'enregistrer la clé secrète (ou le code QR) et de le conserver en lieu sûr. Elle vous aidera à restaurer l'accès à Kaspersky Security Center Web Console au cas où vous perdriez l'accès à l'appareil mobile.

Pour sécuriser l'utilisation de Kaspersky Security Center, vous pouvez activer la vérification en deux étapes pour votre propre compte et activer la vérification en deux étapes pour tous les utilisateurs.

Vous pouvez exclure des comptes de la vérification en deux étapes. Cela peut être nécessaire pour les comptes de service qui ne peuvent pas recevoir de code de sécurité pour l'authentification.

Règles et restrictions

Pour pouvoir activer la vérification en deux étapes pour tous les utilisateurs et désactiver la vérification en deux étapes pour certains utilisateurs, procédez comme suit :

- Assurez-vous que votre compte dispose du droit Modifier les ACL d'objets dans la zone fonctionnelle **Fonctionnalités générales : Autorisations utilisateur**.
- Activez la vérification en deux étapes pour votre compte.

Pour pouvoir désactiver la vérification en deux étapes pour tous les utilisateurs, procédez comme suit :

- Assurez-vous que votre compte dispose du droit Modifier les ACL d'objets dans la zone fonctionnelle **Fonctionnalités générales : Autorisations utilisateur**.
- Connectez-vous à Kaspersky Security Center Web Console à l'aide de la vérification en deux étapes.

Si la vérification en deux étapes est configurée pour un compte utilisateur sur le Serveur d'administration de Kaspersky Security Center version 13 ou suivante, l'utilisateur ne pourra pas se connecter à Kaspersky Security Center Web Console de versions 12, 12.1 ou 12.2.

Réémission de la clé secrète

Tout utilisateur peut réémettre la clé secrète utilisée pour la vérification en deux étapes. Lorsqu'un utilisateur se connecte au Serveur d'administration avec la clé secrète réémise, la nouvelle clé secrète est enregistrée pour le compte de l'utilisateur. Si l'utilisateur saisit une nouvelle clé secrète de manière incorrecte, la nouvelle clé secrète n'est pas enregistrée et la clé secrète actuelle reste valide.

Un code de sécurité comporte un identifiant que l'on appelle *nom de l'émetteur*. Le nom de l'émetteur du code de sécurité est utilisé comme identifiant du Serveur d'administration dans l'application d'authentification. Le nom par défaut de l'émetteur du code de sécurité est identique au nom du Serveur d'administration. Vous pouvez modifier le nom de l'émetteur du code de sécurité. Si vous modifiez le nom de l'émetteur du code de sécurité, vous devez émettre une nouvelle clé secrète et la transmettre à l'application d'authentification.

Activation de la vérification en deux étapes pour votre compte (Web Console)

Vous ne pouvez activer la vérification en deux étapes que pour votre propre compte.

Avant d'activer la vérification en deux étapes pour votre compte, assurez-vous qu'une application d'authentification est installée sur l'appareil mobile. Assurez-vous que l'heure définie dans l'application d'authentification est synchronisée avec celle de l'appareil sur lequel le Serveur d'administration est installé.

Pour activer la vérification en deux étapes pour un compte utilisateur, procédez comme suit :

1. Dans le menu principal, accédez à **Utilisateurs et rôles** → **Utilisateurs**.
2. Cliquez sur le nom de votre compte.
3. Dans la fenêtre des paramètres utilisateur qui s'ouvre, sélectionnez l'onglet **Sécurité d'authentification**.

4. Sous l'onglet **Sécurité d'authentification** :

   a. Sélectionnez l'option **Demander le nom d'utilisateur, le mot de passe et le code de sécurité (vérification en deux étapes)**. Cliquez sur le bouton **Enregistrer**.

   b. Dans la fenêtre de vérification en deux étapes qui s'ouvre, cliquez sur **Découvrir comment configurer une vérification en deux étapes**.

      Saisissez la clé secrète dans l'application d'authentification ou cliquez sur **Afficher le code QR** et scannez le code QR à l'aide de l'application d'authentification sur l'appareil mobile pour recevoir le code de sécurité à usage unique.

   c. Dans la fenêtre de vérification en deux étapes, indiquez le code de sécurité généré par l'application d'authentification, puis cliquez sur le bouton **Vérifier et appliquer**.

5. Cliquez sur le bouton **Enregistrer**.

La vérification en deux étapes est activée pour votre compte.

Activation de la vérification en deux étapes pour votre compte (basée sur MMC)

Avant d'activer la vérification en deux étapes pour votre compte, assurez-vous qu'une application d'authentification est installée sur l'appareil mobile. Assurez-vous que l'heure définie dans l'application d'authentification est synchronisée avec l'heure du Serveur d'administration.

Pour activer la vérification en deux étapes pour votre compte :

1. Dans l'arborescence de la console de Kaspersky Security Center, ouvrez le menu contextuel du dossier **Serveur d'administration** d'un clic-droit, puis choisissez l'option **Propriétés**.

2. Dans la fenêtre des propriétés du Serveur d'administration, accédez au volet **Sections**, sélectionnez **Avancé**, puis **Vérification en deux étapes**.

3. Dans la section **Vérification en deux étapes**, cliquez sur le bouton **Configurer**.

   > Si la vérification en deux étapes est déjà activée pour votre compte, cliquez sur le bouton **Configurer** pour réinitialiser la clé secrète afin que vous puissiez reconfigurer la vérification en deux étapes.

   Dans la fenêtre des propriétés de vérification en deux étapes qui s'ouvre, la clé secrète s'affiche.

4. Entrez la clé secrète dans l'application d'authentification pour recevoir un code de sécurité à usage unique. Vous pouvez indiquer manuellement la clé secrète dans l'application d'authentification ou scanner le code QR par l'application d'authentification sur l'appareil mobile.

5. Indiquez le code de sécurité généré par l'application d'authentification, puis cliquez sur le bouton **OK** pour quitter la fenêtre des propriétés de vérification en deux étapes.

6. Cliquez sur le bouton **Appliquer**.

7. Cliquez sur le bouton **OK**.

La vérification en deux étapes est activée pour votre propre compte.

Activation de la vérification en deux étapes obligatoire pour tous les utilisateurs (Web Console)

Vous pouvez activer la vérification en deux étapes pour tous les utilisateurs du Serveur d'administration si votre compte dispose du droit Modifier les ACL des objets dans la zone fonctionnelle **Fonctionnalités générales : Autorisations utilisateur** et si vous êtes authentifié à l'aide de la vérification en deux étapes.

Pour activer la vérification en deux étapes pour tous les utilisateurs :

1. Dans le menu principal, cliquez sur l'icône des paramètres ( ) en regard du nom du Serveur d'administration requis.

   La fenêtre des propriétés du Serveur d'administration s'ouvre.

2. Sous l'onglet **Sécurité d'authentification** de la fenêtre des propriétés, utilisez le commutateur pour activer l'option de **vérification en deux étapes pour tous les utilisateurs**.

3. Si vous n'avez pas activé la vérification en deux étapes pour votre compte, l'application ouvre la fenêtre permettant d'activer la vérification en deux étapes pour votre propre compte.

   a. Dans la fenêtre de vérification en deux étapes, cliquez sur **Découvrir comment configurer une vérification en deux étapes**.

   b. Saisissez la clé secrète dans l'application d'authentification manuellement ou cliquez sur **Afficher le code QR** et scannez le code QR à l'aide de l'application d'authentification sur l'appareil mobile pour recevoir le code de sécurité à usage unique.

   c. Dans la fenêtre de vérification en deux étapes, indiquez le code de sécurité généré par l'application d'authentification, puis cliquez sur le bouton **Vérifier et appliquer**.

La vérification en deux étapes est activée pour tous les utilisateurs. À partir de maintenant, les utilisateurs du Serveur d'administration, y compris les utilisateurs ajoutés après l'activation de la vérification en deux étapes pour tous les utilisateurs, doivent configurer la vérification en deux étapes pour leurs comptes, à l'exception des utilisateurs sont exclus de la vérification en deux étapes.

Activation de la vérification en deux étapes pour tous les utilisateurs (basée sur MMC)

Vous pouvez activer la vérification en deux étapes pour tous les utilisateurs du Serveur d'administration si votre compte dispose du droit Modifier les ACL des objets dans la zone fonctionnelle **Fonctionnalités générales : Autorisations utilisateur** et si vous êtes authentifié à l'aide de la vérification en deux étapes.

Pour activer la vérification en deux étapes pour tous les utilisateurs :

1. Dans l'arborescence de la console de Kaspersky Security Center, ouvrez le menu contextuel du dossier **Serveur d'administration** d'un clic-droit, puis choisissez l'option **Propriétés**.

2. Dans la fenêtre des propriétés du Serveur d'administration, dans le volet **Sections**, sélectionnez **Avancé**, puis **Vérification en deux étapes**.

3. Cliquez sur le bouton **Définir comme requis** pour activer la vérification en deux étapes pour tous les utilisateurs.

4. Si vous n'avez pas activé la vérification en deux étapes pour votre compte, l'application ouvre la fenêtre permettant d'activer la vérification en deux étapes pour votre propre compte.

   a. Entrez la clé secrète dans l'application d'authentification pour recevoir un code de sécurité à usage unique. Vous pouvez indiquer la clé secrète dans l'application d'authentification manuellement ou numériser le code QR à l'aide de l'application d'authentification sur l'appareil mobile pour recevoir le code de sécurité à usage unique.

   b. Indiquez le code de sécurité généré par l'application d'authentification, puis cliquez sur le bouton **OK** pour quitter la fenêtre des propriétés de vérification en deux étapes.

5. Dans la section **Vérification en deux étapes**, cliquez sur le bouton **Appliquer**, puis cliquez sur le bouton **OK**.

La vérification en deux étapes est activée pour tous les utilisateurs. À partir de maintenant, tous les utilisateurs du Serveur d'administration, y compris les utilisateurs ajoutés après l'activation de cette option, doivent configurer la vérification en deux étapes pour leurs comptes, à l'exception des utilisateurs dont les comptes sont exclus de la vérification en deux étapes.

Désactivation de la vérification en deux étapes d'un compte utilisateur (Web Console)

Vous pouvez désactiver la vérification en deux étapes pour votre propre compte ainsi que pour le compte de tout autre utilisateur.

> Vous pouvez désactiver la vérification en deux étapes du compte d'un autre utilisateur si votre compte dispose du droit Modifier les ACL des objets dans la zone fonctionnelle **Fonctionnalités générales : Autorisations utilisateur** et si vous êtes authentifié à l'aide de la vérification en deux étapes.

Pour désactiver la vérification en deux étapes d'un compte utilisateur, procédez comme suit :

1. Dans le menu principal, accédez à **Utilisateurs et rôles** → **Utilisateurs**.

2. Cliquez sur le nom du compte d'utilisateur interne pour lequel vous souhaitez désactiver la vérification en deux étapes. Il peut s'agir de votre propre compte ou du compte de tout autre utilisateur.

3. Dans la fenêtre des paramètres utilisateur qui s'ouvre, sélectionnez l'onglet **Protection du compte**.

4. Sous l'onglet **Protection du compte**, sélectionnez l'option **Demander uniquement le nom d'utilisateur et le mot de passe** si vous souhaitez désactiver la vérification en deux étapes pour un compte utilisateur.

5. Cliquez sur le bouton **Enregistrer**.

La vérification en deux étapes est désactivée pour le compte utilisateur.

> Si vous souhaitez restaurer l'accès à un utilisateur qui ne peut pas se connecter à Kaspersky Security Center Web Console à l'aide de la vérification en deux étapes, désactivez la vérification en deux étapes pour ce compte utilisateur, puis sélectionnez l'option **Demander uniquement le nom d'utilisateur et le mot de passe**, comme décrit ci-dessus. Après cela, connectez-vous à Kaspersky Security Center Web Console sous le compte utilisateur pour lequel vous avez désactivé la vérification en deux étapes, puis activez à nouveau la vérification.

Désactivation de la vérification en deux étapes d'un compte utilisateur (basée sur MMC)

Pour désactiver la vérification en deux étapes pour votre compte :

1. Dans l'arborescence de la console de Kaspersky Security Center, ouvrez le menu contextuel du dossier **Serveur d'administration** d'un clic-droit, puis choisissez l'option **Propriétés**.
2. Dans la fenêtre des propriétés du Serveur d'administration, dans le volet **Sections**, sélectionnez **Avancé**, puis **Vérification en deux étapes**.
3. Dans la section **Vérification en deux étapes**, cliquez sur le bouton **Désactiver**.
4. Cliquez sur le bouton **Appliquer**.
5. Cliquez sur le bouton **OK**.

La vérification en deux étapes est désactivée pour votre compte.

Vous pouvez désactiver la vérification en deux étapes des comptes d'autres utilisateurs. Cette mesure peut fournir une protection dans le cas où, par exemple, un utilisateur perd ou casse un appareil mobile.

Vous pouvez désactiver la vérification en deux étapes du compte d'un autre utilisateur uniquement si vous disposez du droit Modifier les ACL des objets dans la zone fonctionnelle **Fonctionnalités générales : Autorisations utilisateur** et si vous êtes authentifié à l'aide de la vérification en deux étapes. En outre, en suivant les étapes ci-dessous, vous pouvez également désactiver la vérification en deux étapes pour votre propre compte.

Pour désactiver la vérification en deux étapes d'un compte utilisateur :

1. Ouvrez le dossier **Comptes utilisateurs** dans l'arborescence de la console.

   Le dossier **Comptes utilisateurs** est un sous-dossier par défaut du dossier **Avancé**.
2. Dans l'espace de travail, double-cliquez sur le compte utilisateur pour lequel vous souhaitez désactiver la vérification en deux étapes.

   Pour tous les comptes utilisateurs pour lesquels la vérification en deux étapes est activée, la colonne **2FA requis** est définie sur **Oui**.
3. Dans la fenêtre **Propriétés : <user name>** qui s'ouvre, sélectionnez la section **Vérification en deux étapes**.
4. Dans la section **Vérification en deux étapes**, sélectionnez les options suivantes :

   - Si vous souhaitez désactiver la vérification en deux étapes pour un compte utilisateur, cliquez sur le bouton **Désactiver**.
   - Si vous souhaitez exclure ce compte utilisateur de la vérification en deux étapes, sélectionnez l'option **L'utilisateur peut &passer l'authentification en utilisant uniquement son nom d'utilisateur et son mot de passe**.
5. Cliquez sur le bouton **Appliquer**.
6. Cliquez sur le bouton **OK**.

La vérification en deux étapes pour un compte utilisateur est désactivée.

Si vous souhaitez restaurer l'accès à un utilisateur qui ne peut pas se connecter à la Console d'administration à l'aide de la vérification en deux étapes, désactivez la vérification en deux étapes pour cet utilisateur et sélectionnez l'option **L'utilisateur peut &passer l'authentification en utilisant uniquement son nom d'utilisateur et son mot de passe** dans la section **Vérification en deux étapes** comme décrit ci-dessus. Après cela, connectez-vous à la Console d'administration sous le compte utilisateur pour lequel vous avez désactivé la vérification en deux étapes, puis activez à nouveau la vérification.

Désactivation de la vérification en deux étapes obligatoire pour tous les utilisateurs (Web Console)

Vous pouvez désactiver la vérification en deux étapes obligatoire pour tous les utilisateurs si la vérification en deux étapes est activée pour votre compte et que votre compte dispose du droit Modifier les ACL des objets dans la zone fonctionnelle **Fonctionnalités générales : Autorisations utilisateur**. Si la vérification en deux étapes n'est pas activée pour votre compte, vous devez activer la vérification en deux étapes pour votre compte avant de la désactiver pour tous les utilisateurs.

Pour désactiver la vérification en deux étapes pour tous les utilisateurs :

1. Dans le menu principal, cliquez sur l'icône des paramètres ( ) en regard du nom du Serveur d'administration requis.

   La fenêtre des propriétés du Serveur d'administration s'ouvre.

2. Sous l'onglet **Sécurité d'authentification** de la fenêtre des propriétés, utilisez le commutateur pour désactiver l'option de **vérification en deux étapes pour tous les utilisateurs**.

La vérification en deux étapes est désactivée pour tous les utilisateurs. La désactivation de la vérification en deux étapes pour tous les utilisateurs ne s'applique pas aux comptes spécifiques pour lesquels la vérification en deux étapes a été précédemment activée séparément.

Désactivation de la vérification en deux étapes obligatoire pour tous les utilisateurs (basée sur MMC)

Vous pouvez désactiver la vérification en deux étapes obligatoire pour tous les utilisateurs du Serveur d'administration si vous disposez du droit Modifier les ACL des objets dans la zone fonctionnelle **Fonctionnalités générales : Autorisations utilisateur** et si vous êtes authentifié à l'aide de la vérification en deux étapes.

Pour désactiver la vérification en deux étapes pour tous les utilisateurs :

1. Dans l'arborescence de la console de Kaspersky Security Center, ouvrez le menu contextuel du dossier **Serveur d'administration** d'un clic-droit, puis choisissez l'option **Propriétés**.

2. Dans la fenêtre des propriétés du Serveur d'administration, dans le volet **Sections**, sélectionnez **Avancé**, puis **Vérification en deux étapes**.

3. Cliquez sur le bouton **Définir comme facultatif** pour désactiver la vérification en deux étapes pour tous les utilisateurs.

4. Cliquez sur le bouton **Appliquer** dans la section **Vérification en deux étapes**.

5. Cliquez sur le bouton **OK** dans la section **Vérification en deux étapes**.

La vérification en deux étapes est désactivée pour tous les utilisateurs. La désactivation de la vérification en deux étapes pour tous les utilisateurs ne s'applique pas aux comptes spécifiques pour lesquels la vérification en deux étapes a été précédemment activée séparément.

Exclusion de comptes de la vérification en deux étapes (Web Console)

Vous pouvez exclure des comptes utilisateurs de la vérification en deux étapes si vous disposez du droit Modifier les ACL des objets dans la zone fonctionnelle **Fonctionnalités générales : Autorisations utilisateur**.

Si un compte utilisateur est exclu de la liste de vérification en deux étapes de tous les utilisateurs, cet utilisateur n'a pas à utiliser la vérification en deux étapes.

L'exclusion des comptes de la vérification en deux étapes peut être nécessaire pour les comptes de service qui ne peuvent pas transmettre le code de sécurité lors de l'authentification.

Si vous souhaitez exclure certains comptes utilisateurs de la vérification en deux étapes, procédez comme suit :

1. Vous devez effectuer un sondage du contrôleur de domaine Microsoft Active Directory pour actualiser la liste des utilisateurs du Serveur d'administration si vous souhaitez exclure des comptes Active Directory.

2. Dans le menu principal, cliquez sur l'icône des paramètres ( ) en regard du nom du Serveur d'administration requis.

   La fenêtre des propriétés du Serveur d'administration s'ouvre.

3. Sous l'onglet **Sécurité d'authentification** de la fenêtre des propriétés, dans le tableau des exclusions de la vérification en deux étapes, cliquez sur le bouton **Ajouter**.

4. Dans la fenêtre qui s'ouvre :

   a. Sélectionnez les comptes utilisateurs que vous voulez exclure.

   b. Cliquez sur le bouton **OK**.

Les comptes utilisateurs sélectionnés sont exclus de la vérification en deux étapes.

Exclusion de comptes de la vérification en deux étapes (basée sur MMC)

Vous pouvez exclure un compte de la vérification en deux étapes si votre compte dispose du droit Modifier les ACL des objets dans la zone fonctionnelle **Fonctionnalités générales : Autorisations utilisateur**.

Si un compte utilisateur est exclu de la vérification en deux étapes, l'utilisateur en question peut se connecter à la Console d'administration ou à Kaspersky Security Center Web Console sans utiliser la vérification en deux étapes.

L'exclusion des comptes de la vérification en deux étapes peut être nécessaire pour les comptes de service qui ne peuvent pas transmettre le code de sécurité lors de l'authentification.

Pour exclure un compte utilisateur de la vérification en deux étapes, procédez comme suit :

1. Si vous souhaitez exclure un compte Active Directory, effectuez un sondage Active Directory afin d'actualiser la liste des utilisateurs du Serveur d'administration.
2. Ouvrez le dossier **Comptes utilisateurs** dans l'arborescence de la console.

   Le dossier **Comptes utilisateurs** est un sous-dossier par défaut du dossier **Avancé**.
3. Dans l'espace de travail, double-cliquez sur le compte utilisateur que vous souhaitez exclure de la vérification en deux étapes
4. Dans la fenêtre **Propriétés : <user name>** qui s'ouvre, sélectionnez la section **Vérification en deux étapes**.
5. Dans la section ouverte, sélectionnez l'option **L'utilisateur peut &passer l'authentification en utilisant uniquement son nom d'utilisateur et son mot de passe**.
6. Dans la section **Vérification en deux étapes**, cliquez sur le bouton **Appliquer**, puis cliquez sur le bouton **OK**.

Ce compte utilisateur est exclu de la vérification en deux étapes. Vous pouvez vérifier les comptes exclus dans la liste des comptes utilisateurs.

Modification du nom d'un émetteur de code de sécurité (Web Console)

Vous pouvez avoir plusieurs identifiants (ils sont appelés émetteurs) pour différents Serveurs d'administration. Vous pouvez modifier le nom d'un émetteur de code de sécurité dans le cas, par exemple, si le Serveur d'administration utilise déjà un nom d'émetteur de code de sécurité semblable pour un autre Serveur d'administration. Par défaut, le nom de l'émetteur du code de sécurité est le même que le nom du Serveur d'administration.

Après avoir modifié le nom de l'émetteur du code de sécurité, vous devez émettre une nouvelle clé secrète et la transmettre à l'application d'authentification.

Pour spécifier un nouveau nom d'émetteur du code de sécurité :

1. Dans le menu principal, cliquez sur l'icône des paramètres ( ) en regard du nom du Serveur d'administration requis.

   La fenêtre des propriétés du Serveur d'administration s'ouvre.
2. Dans la fenêtre des paramètres utilisateur qui s'ouvre, sélectionnez l'onglet **Protection du compte**.
3. Sous l'onglet **Protection du compte**, cliquez sur le lien **Modifier**.

   La section **Modifier l'émetteur du code de sécurité** s'ouvre.
4. Indiquez nouveau nom d'émetteur de code de sécurité.
5. Cliquez sur le bouton **OK**.

Un nouveau nom d'émetteur de code de sécurité est indiqué pour le Serveur d'administration.

Modification du nom d'un émetteur de code de sécurité (basé sur MMC)

Vous pouvez avoir plusieurs identifiants (ils sont appelés émetteurs) pour différents Serveurs d'administration. Vous pouvez modifier le nom d'un émetteur de code de sécurité dans le cas, par exemple, si le Serveur d'administration utilise déjà un nom d'émetteur de code de sécurité semblable pour un autre Serveur d'administration. Par défaut, le nom de l'émetteur du code de sécurité est le même que le nom du Serveur d'administration.

Après avoir modifié le nom de l'émetteur du code de sécurité, vous devez émettre une nouvelle clé secrète et la transmettre à l'application d'authentification.

Pour spécifier un nouveau nom d'émetteur du code de sécurité :

1. Dans l'arborescence de la console de Kaspersky Security Center, ouvrez le menu contextuel du dossier **Serveur d'administration** d'un clic-droit, puis choisissez l'option **Propriétés**.
2. Dans la fenêtre des propriétés du Serveur d'administration, dans le volet **Sections**, sélectionnez **Avancé**, puis **Vérification en deux étapes**.
3. Spécifiez un nouveau nom d'émetteur de code de sécurité dans le champ **Émetteur du code de sécurité**.
4. Cliquez sur le bouton **Appliquer** dans la section **Vérification en deux étapes**.
5. Cliquez sur le bouton **OK** dans la section **Vérification en deux étapes**.

Un nouveau nom d'émetteur de code de sécurité est indiqué pour le Serveur d'administration.

Configuration de la vérification en deux étapes pour votre compte (Web Console)

Lors de la première connexion à Kaspersky Security Center après l'activation de la vérification en deux étapes, la fenêtre de configuration de la vérification en deux étapes pour votre propre compte s'ouvre.

Avant de configurer la vérification en deux étapes pour votre compte, assurez-vous qu'une application d'authentification est installée sur l'appareil mobile.

Assurez-vous que l'heure de l'appareil avec l'application d'authentification et l'heure de l'appareil avec le Serveur d'administration sont synchronisées au format UTC, en utilisant des sources externes.

Pour configurer la vérification en deux étapes pour votre compte :

1. Générez un code de sécurité à usage unique à l'aide de l'application d'authentification de l'appareil mobile. Pour ce faire, réalisez une des actions suivantes :

   - Saisissez manuellement la clé secrète dans l'application d'authentification.
   - Cliquez sur **Afficher le code QR** et scannez le code QR à l'aide de l'application d'authentification.

   Un code de sécurité s'affichera sur l'appareil mobile.

2. Dans la fenêtre de configuration de la vérification en deux étapes, indiquez le code de sécurité généré par l'application d'authentification, puis cliquez sur le bouton **Vérifier et appliquer**.

La vérification en deux étapes est configurée pour votre compte. Vous pouvez accéder au Serveur d'administration conformément à vos privilèges.

Configuration de la vérification en deux étapes pour votre compte (basée sur MMC)

Lors de la première connexion à Kaspersky Security Center après l'activation de la vérification en deux étapes, la fenêtre de configuration de la vérification en deux étapes pour votre propre compte s'ouvre.

Avant de configurer la vérification en deux étapes pour votre compte, assurez-vous qu'une application d'authentification est installée sur l'appareil mobile. Assurez-vous que l'heure de l'appareil avec l'application d'authentification et l'heure de l'appareil avec le Serveur d'administration sont synchronisées au format UTC, en utilisant des sources externes.

Pour configurer la vérification en deux étapes pour votre compte :

1. Générez un code de sécurité à usage unique à l'aide de l'application d'authentification de l'appareil mobile. Pour ce faire, réalisez une des actions suivantes :

   - Saisissez manuellement la clé secrète dans l'application d'authentification.
   - Scannez le code QR à l'aide de l'application d'authentification.

   Un code de sécurité s'affichera sur l'appareil mobile.

2. Dans la fenêtre **Configurer la vérification en deux étapes**, indiquez le code de sécurité généré par l'application d'authentification, puis cliquez sur le bouton **OK**.

La vérification en deux étapes est configurée pour votre compte. Vous pouvez accéder au Serveur d'administration conformément à vos privilèges.

Création d'une nouvelle clé secrète

Vous pouvez générer une nouvelle clé secrète pour une vérification en deux étapes pour votre compte uniquement si vous y êtes autorisé, à l'aide de la vérification en deux étapes.

Pour générer une nouvelle clé secrète pour un compte utilisateur, procédez comme suit :

1. Dans le menu principal, accédez à **Utilisateurs et rôles** → **Utilisateurs**.
2. Cliquez sur le nom du compte utilisateur pour lequel vous souhaitez générer une nouvelle clé secrète pour une vérification en deux étapes.
3. Dans la fenêtre des paramètres utilisateur qui s'ouvre, sélectionnez l'onglet **Protection du compte**.
4. Sous l'onglet **Protection du compte**, cliquez sur le lien **Générer une nouvelle clé secrète**.
5. Dans la fenêtre de vérification en deux étapes qui s'ouvre, indiquez une nouvelle clé de sécurité générée par l'application d'authentification.
6. Cliquez sur le bouton **Vérifier et appliquer**.

Une nouvelle clé secrète est générée pour l'utilisateur.

Si vous perdez l'appareil mobile, vous pouvez installer une application d'authentification sur un autre appareil mobile et générer une nouvelle clé secrète pour restaurer l'accès à Kaspersky Security Center Web Console.

Interdire aux nouveaux utilisateurs de configurer eux-mêmes la vérification en deux étapes

Afin d'améliorer encore la sécurité d'accès à Kaspersky Security Center Web Console, vous pouvez interdire aux nouveaux utilisateurs de configurer eux-mêmes la vérification en deux étapes.

Si cette option est activée, un utilisateur dont la vérification en deux étapes est désactivée, par exemple un nouvel administrateur de domaine, ne peut pas configurer lui-même la vérification en deux étapes. Par conséquent, cet utilisateur ne peut pas être authentifié sur le Serveur d'administration et ne peut pas se connecter à Kaspersky Security Center Web Console sans l'approbation d'un autre administrateur de Kaspersky Security Center qui a déjà activé la vérification en deux étapes.

Cette option est disponible si la vérification en deux étapes est activée pour tous les utilisateurs.

Pour interdire aux nouveaux utilisateurs de configurer eux-mêmes la vérification en deux étapes :

1. Dans le menu principal, cliquez sur l'icône paramètres ( ) en face du nom du Serveur d'administration requis.

   La fenêtre des propriétés du Serveur d'administration s'ouvre.
2. Dans l'onglet **Sécurité d'authentification** de la fenêtre des propriétés, placez le bouton bascule **Interdire aux nouveaux utilisateurs de configurer eux-mêmes la vérification en deux étapes** sur la position activée.

Cette option n'affecte pas les comptes d'utilisateurs ajoutés aux exclusions de la vérification en deux étapes.

Afin d'accorder l'accès à Kaspersky Security Center Web Console à un utilisateur dont la vérification en deux étapes est désactivée, désactivez temporairement l'option **Interdire aux nouveaux utilisateurs de configurer eux-mêmes la vérification en deux étapes**, demandez à l'utilisateur d'activer la vérification en deux étapes, puis réactivez l'option.

Désignation d'un utilisateur en tant que propriétaire de l'appareil Linux après l'installation de l'Agent d'administration

Pour autoriser l'enregistrement de l'utilisateur en tant que propriétaire de l'appareil Linux, procédez comme suit :

1. Dans Kaspersky Security Center Web Console, accédez à **Découverte et déploiement** → **Déploiement et attribution** → **Paquets d'installation**.

   La liste des paquets d'installation s'ouvre.

2. Cliquez sur le paquet d'installation de l'Agent d'administration.

   La fenêtre des propriétés du paquet d'installation s'ouvre.

3. Dans la fenêtre des propriétés du paquet d'installation, cliquez sur **Paramètres** → **Avancé**.

4. Dans la section **Enregistrement de l'utilisateur en tant que propriétaire de l'appareil (Linux uniquement)**, activez l'option **Autoriser l'exécution de l'utilitaire d'enregistrement des utilisateurs après l'installation de l'Agent d'administration** et cliquez sur le bouton **Enregistrer**.

L'utilitaire d'enregistrement de l'utilisateur en tant que propriétaire de l'appareil peut être lancé via la ligne de commande sur l'appareil client.

Pour enregistrer un utilisateur en tant que propriétaire de l'appareil client Linux, procédez comme suit :

1. Exécutez la commande suivante dans la ligne de commande sur l'appareil client :
   `$ /opt/kaspersky/klnagent64/bin/nagregister -set_owner`

2. Saisissez l'identifiant et le mot de passe, si vous y êtes invité(e).

   Si l'identifiant et le mot de passe se trouvent dans le fichier de réponses ou dans le paquet d'installation de l'Agent d'administration, exécutez la commande suivante sur l'appareil client dans la ligne de commande :
   `$ /opt/kaspersky/klnagent64/bin/nagregister -set_owner -unattended`

Si l'utilisateur fait partie d'un groupe de sécurité interne, le nom d'utilisateur doit figurer dans l'identifiant.

Si l'utilisateur fait partie d'un groupe de sécurité Active Directory, le nom d'utilisateur et le nom de domaine doivent figurer dans l'identifiant.

Si la vérification en deux étapes est activée pour l'utilisateur, vous devez saisir le mot de passe à usage unique depuis l'application.

L'utilisateur sera enregistré en tant que propriétaire de l'appareil.

Suppression d'un utilisateur ou d'un groupe de sécurité

Vous ne pouvez supprimer que les utilisateurs internes ou les groupes de sécurité internes.

Pour supprimer un utilisateur ou un groupe de sécurité, procédez comme suit :

1. Dans le menu principal, accédez à **Utilisateurs et rôles** → **Utilisateurs et groupes**, puis sélectionnez l'onglet **Utilisateurs** ou **Groupes**.
2. Cochez la case en regard de l'utilisateur ou du groupe de sécurité que vous souhaitez supprimer.
3. Cliquez sur **Supprimer**.
4. Dans la fenêtre qui s'ouvre, cliquez sur **OK**.

L'utilisateur ou le groupe de sécurité est supprimé.

Modification du mot de passe d'un compte utilisateur

Vous devrez peut-être modifier le mot de passe de votre propre compte ou de celui d'un autre utilisateur si le mot de passe actuel est sur le point d'expirer ou si vous souhaitez le remplacer par un mot de passe plus sécurisé.

Le mot de passe doit remplir les conditions suivantes :

- Le mot de passe doit compter entre 8 et 256 caractères.
- Le mot de passe doit compter des caractères d'au moins trois des groupes ci-dessous :
  - Lettres majuscules (A-Z)
  - Lettre minuscules (a-z)
  - Chiffres (0-9)
  - Caractères spéciaux (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
- Le mot de passe ne peut pas contenir d'espaces, de caractères Unicode ou de la combinaison " . " et " @ " lorsque " . " est placé devant " @ ".

Modification du mot de passe de votre propre compte

Pour modifier le mot de passe de votre compte, procédez comme suit :

1. Dans le menu principal, allez dans les paramètres de votre compte et sélectionnez **Modifier le mot de passe**.
2. Saisissez le mot de passe actuel, puis indiquez le nouveau mot de passe pour la connexion à Kaspersky Security Center.

   Pour consulter le mot de passe saisi, cliquez sur .
3. Si votre compte utilisateur est protégé contre les modifications non autorisées, vous devez confirmer que vous avez les autorisations pour modifier le compte en question. Dans la fenêtre **Protection du compte**, indiquez les identifiants de votre propre compte ou du compte disposant du droit Modifier les ACL des objets dans la zone fonctionnelle Caractéristiques générales : Autorisations utilisateur.
4. Si la vérification en deux étapes est activée pour le compte que vous avez utilisé à l'étape précédente, saisissez le code de sécurité généré par l'application d'authentification sur l'appareil mobile.

Modification du mot de passe d'un compte utilisateur interne

Pour modifier le mot de passe d'un compte utilisateur interne, procédez comme suit :

1. Dans le menu principal, accédez à **Utilisateurs et rôles** → **Utilisateurs et groupes**, puis sélectionnez l'onglet **Utilisateurs**.
2. Cliquez sur le nom du compte utilisateur que vous souhaitez modifier.
3. Dans la fenêtre des paramètres utilisateur qui s'ouvre, sous l'onglet **Général**, cliquez sur le bouton **Modifier le mot de passe**.
4. Définissez un nouveau mot de passe pour connecter l'utilisateur à Kaspersky Security Center.

   Pour consulter le mot de passe saisi, cliquez sur .
5. Si nécessaire, vous pouvez activer l'option **L'utilisateur doit changer son mot de passe lors de la première connexion** pour forcer la modification du mot de passe lors de l'authentification de l'utilisateur suivante.
6. Si le compte utilisateur est protégé contre les modifications non autorisées, vous devez confirmer que vous avez les autorisations pour modifier le compte en question. Dans la fenêtre **Protection du compte**, indiquez les identifiants du compte disposant du droit Modifier les ACL des objets dans la zone fonctionnelle Caractéristiques générales : Autorisations utilisateur.

Configuration des options de modification de mot de passe à l'aide d'indicateurs du serveur

Vous pouvez utiliser l'utilitaire klsclag pour configurer la modification du mot de passe à l'aide des commandes suivantes :

- Configuration de la période de rotation des mots de passe (l'indicateur `LP_SplPwdChangePeriodDays`)

  `klscflag.exe -fset -pv .core/.independent -s KLLIM -n LP_SplPwdChangePeriodDays -t d -v <période_de_rotation>`

  Où `<période_de_rotation>` est une période en jours après laquelle le mot de passe de l'utilisateur expire. Valeurs possibles : 0–730. Si la valeur du paramètre est 0, la rotation du mot de passe est désactivée.

- Configuration de l'heure de l'avertissement préliminaire sur la nécessité de modifier le mot de passe (indicateur `LP_SplPwdChangeNotificationHours`)

  `klscflag.exe -fset -pv .core/.independent -s KLLIM -n LP_SplPwdChangeNotificationHours -t d -v <temps_d'avertissement>`

  Où `<temps_d'avertissement>` est une période en heures avant l'expiration du mot de passe de l'utilisateur. Pendant ce temps, la notification indiquant le besoin de modifier le mot de passe s'affiche. Valeurs possibles : 0–17520. Si la valeur du paramètre est 0, la durée d'avertissement est égale à 25 % de la période de rotation du mot de passe.

- Précision de la valeur par défaut de l'option **L'utilisateur doit changer son mot de passe lors de la première connexion** (l'indicateur `LP_SplPwdForceChange`)

  `klscflag.exe -fset -pv .core/.independent -s KLLIM -n LP_SplPwdForceChange -t d -v <valeur>`

  Où les valeurs possibles du paramètre `<valeur>` sont :

  `1` : l'option **L'utilisateur doit changer son mot de passe lors de la première connexion** est activée.

  `0` : l'option **L'utilisateur doit changer son mot de passe lors de la première connexion** est désactivée.

Pour consulter la valeur actuelle de l'indicateur, exécutez la commande suivante :

```
klscflag.exe -fget -pv .core/.independent -s KLLIM -n <indicateur> -t d
```

Où `<indicateur>` est l'indicateur `LP_SplPwdChangePeriodDays`, `LP_SplPwdChangeNotificationHours` ou `LP_SplPwdForceChange`.

Création d'un rôle d'utilisateur

Pour créer un rôle d'utilisateur, procédez comme suit :

1. Dans le menu principal, accédez à **Utilisateurs et rôles** → **Rôles**.
2. Cliquez sur **Ajouter**.
3. Dans la fenêtre **Nom du nouveau rôle** qui s'ouvre, saisissez le nom du nouveau rôle.
4. Cliquez sur le bouton **OK** pour appliquer les modifications.
5. Dans la fenêtre des propriétés du rôle qui s'ouvre, modifiez les paramètres du rôle :
   - Sous l'onglet **Général**, modifiez le nom du rôle.
     Il est impossible de modifier le nom d'un rôle système.
   - Sous l'onglet **Paramètres**, modifiez la portée du rôle et les stratégies et profils associés au rôle.
   - Sous l'onglet **Privilèges d'accès**, modifiez les privilèges d'accès aux applications de Kaspersky.
6. Cliquez sur le bouton **Enregistrer** afin d'enregistrer les modifications.

Le nouveau rôle apparaît dans la liste des rôles des utilisateurs.

Modification d'un rôle d'utilisateur

Pour modifier un rôle d'utilisateur, procédez comme suit :

1. Dans le menu principal, accédez à **Utilisateurs et rôles** → **Rôles**.
2. Cliquez sur le nom du rôle que vous souhaitez modifier.
3. Dans la fenêtre des propriétés du rôle qui s'ouvre, modifiez les paramètres du rôle :
   - Sous l'onglet **Général**, modifiez le nom du rôle.
     Il est impossible de modifier le nom d'un rôle système.
   - Sous l'onglet **Paramètres**, modifiez la portée du rôle et les stratégies et profils associés au rôle.
   - Sous l'onglet **Privilèges d'accès**, modifiez les privilèges d'accès aux applications de Kaspersky.
4. Cliquez sur le bouton **Enregistrer** afin d'enregistrer les modifications.

Le rôle mis à jour apparaît dans la liste des rôles des utilisateurs.

Modification de la zone d'action d'un rôle d'utilisateur

La *portée du rôle d'utilisateur* est un ensemble d'utilisateurs et de groupes d'administration. Les paramètres associés à un rôle d'utilisateur s'appliquent uniquement aux appareils qui appartiennent aux utilisateurs qui ont ce rôle et uniquement si ces appareils appartiennent aux groupes associés à ce rôle, y compris les groupes enfant.

Pour ajouter des utilisateurs, des groupes de sécurité et des groupes d'administration à la portée d'un rôle d'utilisateur, suivez une de ces méthodes :

Méthode 1 :

1. Dans le menu principal, accédez à **Utilisateurs et rôles** → **Utilisateurs et groupes**, puis sélectionnez l'onglet **Utilisateurs** ou **Groupes**.

2. Cochez les cases en regard des utilisateurs ou des groupes de sécurité que vous souhaitez ajouter à la portée du rôle de l'utilisateur.

3. Cliquez sur le bouton **Attribuer un rôle**.

   L'Assistant d'attribution de rôle se lance. Parcourez les étapes de l'assistant à l'aide du bouton **Suivant**.

4. À l'étape **Sélectionner un rôle**, sélectionnez le rôle d'utilisateur que vous souhaitez attribuer.

5. À l'étape **Définir la plage**, sélectionnez le groupe d'administration que vous souhaitez ajouter à la portée du rôle de l'utilisateur.

6. Cliquez sur le bouton **Attribuer un rôle** pour fermer la fenêtre.

Les utilisateurs ou groupes de sécurité sélectionnés et le groupe d'administration sélectionné sont ajoutés à la portée du rôle d'utilisateur.

Méthode 2 :

1. Dans le menu principal, accédez à **Utilisateurs et rôles** → **Rôles**.

2. Cliquez sur le nom du rôle dont vous souhaitez définir la portée.

3. Dans la fenêtre des propriétés des rôles qui s'ouvre, sélectionnez l'onglet **Paramètres**.

4. Dans la section **Portée du rôle**, cliquez sur **Ajouter**.

   L'Assistant d'attribution de rôle se lance. Parcourez les étapes de l'assistant à l'aide du bouton **Suivant**.

5. À l'étape **Définir la plage**, sélectionnez le groupe d'administration que vous souhaitez ajouter à la portée du rôle de l'utilisateur.

6. À l'étape **Sélectionner les utilisateurs**, sélectionnez les utilisateurs et groupes de sécurité que vous souhaitez ajouter à la portée du rôle de l'utilisateur.

7. Cliquez sur le bouton **Attribuer un rôle** pour fermer la fenêtre.

8. Cliquez sur le bouton **Fermer** (✕) pour fermer la fenêtre de propriétés du Serveur d'administration.

Les utilisateurs ou groupes de sécurité sélectionnés et le groupe d'administration sélectionné sont ajoutés à la portée du rôle d'utilisateur.

Méthode 3 :

1. Dans le menu principal, cliquez sur l'icône des paramètres ( ) en regard du nom du Serveur d'administration requis.

   La fenêtre des propriétés du Serveur d'administration s'ouvre.

2. Sous l'onglet **Privilèges d'accès**, cochez la case en regard du nom de l'utilisateur ou du groupe de sécurité que vous souhaitez ajouter à la portée du rôle de l'utilisateur, puis cliquez sur le bouton **Rôles**.

   Vous ne pouvez pas sélectionner plusieurs utilisateurs ou groupes de sécurité en même temps. Si vous sélectionnez plusieurs éléments, le bouton **Rôles** sera désactivé.

3. Dans la fenêtre **Rôles**, sélectionnez le rôle d'utilisateur que vous souhaitez attribuer, puis appliquez et enregistrez les modifications.

   Les utilisateurs ou les groupes de sécurité sélectionnés sont ajoutés à la portée du rôle d'utilisateur.

Suppression d'un rôle d'utilisateur

Pour supprimer un rôle d'utilisateur, procédez comme suit :

1. Dans le menu principal, accédez à **Utilisateurs et rôles** → **Rôles**.

2. Cochez la case en regard du nom du rôle que vous souhaitez supprimer.

3. Cliquez sur **Supprimer**.

4. Dans la fenêtre qui s'ouvre, cliquez sur **OK**.

Le rôle d'utilisateur est supprimé.

Association des profils des stratégies aux rôles

Vous pouvez associer des rôles d'utilisateurs aux profils des stratégies. Dans ce cas, la règle d'activation pour ce profil de stratégie repose sur le rôle : le profil de stratégie devient actif pour un utilisateur qui a le rôle indiqué.

Par exemple, la stratégie interdit les logiciels de navigation GPS pour tous les appareils du groupe d'administration. Les applications de navigation urbaine sont seulement nécessaires au fonctionnement d'un appareil de l'utilisateur jouant le rôle de livreur, dans le groupe d'administration " Utilisateurs ". Dans ce cas, vous pouvez attribuer un rôle de " messager " à son propriétaire, puis créer un profil de stratégie qui autorise l'exécution d'un logiciel de navigation par satellite uniquement sur les appareils dont les propriétaires ont reçu le rôle " Messager ". Tous les autres paramètres de la stratégie sont préservés. Seul l'utilisateur qui a reçu le rôle " Messager " pourra exécuter un logiciel de navigation par satellite. Ensuite, si un autre employé reçoit le rôle " Messager ", il pourra également exécuter le logiciel de navigation sur l'appareil de votre entreprise. L'exécution d'un logiciel de navigation par satellite sera toujours interdite sur les autres appareils au sein du même groupe d'administration.

Pour associer un rôle à un profil de stratégie :

1. Dans le menu principal, accédez à **Utilisateurs et rôles** → **Rôles**.
2. Cliquez sur le nom d du rôle que vous souhaitez associer à un profil de stratégie.

   La fenêtre des propriétés du rôle s'ouvre à l'onglet **Général**.
3. Sélectionnez l'onglet **Paramètres** et passez à la section **Stratégies et profils**.
4. Cliquez sur **Modifier**.
5. Pour associer le rôle à :

   - **Un profil de stratégie existant** : Cliquez sur l'icône de chevron (>) en regard du nom de la stratégie requise, puis cochez la case en regard du profil auquel vous souhaitez associer le rôle.
   - **Un nouveau profil de stratégie** :

     a. Cochez la case en regard de la stratégie pour laquelle vous souhaitez créer un profil.

     b. Cliquez sur **Nouveau profil de stratégie**.

     c. Indiquez un nom pour le nouveau profil et configurez les paramètres du profil.

     d. Cliquez sur le bouton **Enregistrer**.

     e. Cochez la case en regard du nouveau profil.
6. Cliquez sur **Attribuer au rôle**.

Le profil est associé au rôle et apparaît dans les propriétés du rôle. Le profil s'applique alors automatiquement à tout appareil dont le propriétaire possède ce rôle.

Propagation des rôles d'utilisateurs sur les Serveurs d'administration secondaires

Par défaut, les liste des rôles d'utilisateurs des Serveurs d'administration principaux et secondaires sont indépendantes. Vous pouvez configurer l'application afin qu'elle propage automatiquement les rôles d'utilisateurs créés sur le Serveur d'administration principal à l'ensemble des Serveurs d'administration secondaires. Les rôles d'utilisateurs peuvent également être propagés depuis un Serveur d'administration secondaire à ses propres Serveurs d'administration secondaires.

Pour propager les rôles d'utilisateurs depuis le Serveur d'administration principal aux Serveurs d'administration secondaires :

1. Dans le menu principal, cliquez sur l'icône des paramètres ( ) en regard du nom du Serveur d'administration requis.

   La fenêtre des propriétés du Serveur d'administration s'ouvre avec l'onglet **Général** sélectionné.
2. Passez à la section **Hiérarchie des Serveurs d'administration**.
3. Activez l'option **Relayer la liste des rôles aux Serveurs d'administration secondaires**, puis cliquez sur le bouton **Enregistrer**.

L'application copie les rôles d'utilisateurs du Serveur d'administration principal sur les Serveurs d'administration secondaires.

Quand l'option **Relayer la liste des rôles aux Serveurs d'administration secondaires** est activée et que les rôles d'utilisateurs sont propagés, ces rôles ne peuvent être ni modifiés, ni supprimés sur les Serveurs d'administration secondaires. Quand vous créez un rôle ou modifiez un rôle existant sur le Serveur d'administration principal, les modifications sont appliquées automatiquement aux Serveurs d'administration secondaires. Quand vous supprimez un rôle d'utilisateur sur le Serveur d'administration principal, ce rôle demeure sur les Serveurs d'administration secondaires, mais il peut alors modifié ou supprimé.

Les rôles propagés sur le Serveur d'administration secondaire depuis le Serveur d'administration primaire sont accompagnés de coches vertes (✓). Il est impossible de modifier ces rôles sur le Serveur d'administration secondaire.

Si vous créez un rôle sur le Serveur d'administration principal et s'il existe un rôle portant ce nom sur son Serveur d'administration secondaire, le nouveau rôle est copié sur ce Serveur d'administration secondaire avec un index ajouté à son nom, par exemple ~~1, ~~2 (l'index peut être aléatoire).

Quand vous désactivez l'option **Relayer la liste des rôles aux Serveurs d'administration secondaires**, tous les rôles d'utilisateurs demeurent sur les Serveurs d'administration secondaires, mais deviennent indépendants des rôles sur le Serveur d'administration principal. Une fois qu'ils sont devenus indépendants, ces rôles d'utilisateurs sur les Serveurs d'administration secondaires peuvent être modifiés ou supprimés.

Modification du mot de passe d'un compte

Vous pouvez modifier le mot de passe du compte local, par exemple, si l'utilisateur oublie le mot de passe du compte local ou pour effectuer une modification planifiée du mot de passe.

La modification du mot de passe s'appliquera même si l'utilisateur ne s'est pas connecté au compte. Vous pouvez également modifier le mot de passe du compte root local.

Cette tâche peut être exécutée uniquement sur les appareils Linux.

Pour modifier le mot de passe du compte local sur des appareils en particulier, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Tâches**.
2. Cliquez sur **Ajouter**.

   Ceci permet de lancer l'Assistant de création d'une tâche.
3. Dans le champ **Type de tâche**, sélectionnez l'option **Modifier le mot de passe du compte (Linux uniquement)**.

4. Sélectionnez l'une des options ci-dessous :

- **Attribuer la tâche à un groupe d'administration**

  La tâche est affectée aux appareils qui appartiennent à un groupe d'administration. Vous pouvez renseigner un des groupes existants ou en créer un.

  Par exemple, vous pourriez souhaiter utiliser cette option pour exécuter une tâche d'envoi de messages pour les utilisateurs si le message est particulier pour les appareils repris dans un groupe d'administration spécifique.

  Si une tâche est attribuée à un groupe d'administration, l'onglet **Sécurité** ne s'affiche pas dans la fenêtre des propriétés de la tâche, car les tâches de groupe sont soumises aux paramètres de sécurité des groupes auxquels elles s'appliquent.

- **Définir les adresses des appareils manuellement ou les importer à partir d'une liste**

  Vous pouvez définir les noms NetBIOS, les noms DNS, les adresses IP, ainsi que les plages d'adresses IP auxquels il convient d'affecter la tâche.

  Vous pourriez utiliser cette option pour exécuter une tâche pour un sous-réseau défini. Par exemple, vous pourriez souhaiter installer une certaine application sur les appareils des comptables ou analyser des appareils dans un sous-réseau qui est probablement infecté.

- **Attribuer la tâche à une sélection d'appareils**

  La tâche est affectée aux appareils qui appartiennent à une sélection d'appareils. Vous pouvez définir une des sélections existantes.

  Par exemple, vous pourriez souhaiter utiliser cette option pour exécuter une tâche sur des appareils dotés d'une version du système d'exploitation spécifique.

La tâche *Modifier le mot de passe du compte (Linux uniquement)* est créée pour les appareils spécifiés. Si vous avez sélectionné l'option **Attribuer la tâche à un groupe d'administration**, la tâche est de groupe.

5. À l'étape Zone d' **Zone de la tâche**, indiquez un groupe d'administration, des appareils avec des adresses spécifiques ou une sélection d'appareils.

   Les paramètres disponibles dépendent de l'option sélectionnée à l'étape précédente.

6. À l'étape **Saisissez le nom du compte et le nouveau mot de passe**, configurez les paramètres suivants :

   - Dans le champ **Nom du compte utilisateur**, indiquez le nom du compte dont vous souhaitez modifier le mot de passe.
   - Dans le champ **Nouveau mot de passe**, indiquez le mot de passe qui sera défini pour le compte indiqué dans le champ précédent.

     Pour afficher les caractères que vous avez entrés, cliquez sur le bouton **Afficher** et maintenez-le enfoncé.
   - Si nécessaire, cochez la case **Définir comme mot de passe à usage unique (l'utilisateur doit modifier le mot de passe après la première connexion)**.

     - Définir comme mot de passe à usage unique (l'utilisateur doit modifier le mot de passe après la première connexion)

       Si la case est cochée, l'utilisateur sera invité à définir un nouveau mot de passe après la première connexion.

       Si la case est décochée, l'utilisateur ne sera plus invité à définir un nouveau mot de passe après la première connexion.

       Celle-ci est décochée par défaut.

7. À l'étape **Fin de la création de la tâche**, cliquez sur le bouton **Terminer** pour créer la tâche et fermer l'Assistant.

   Si vous avez activé l'option **Ouvrir les détails de la tâche à la fin de la création**, la fenêtre des paramètres de la tâche s'ouvre. Dans cette fenêtre, vous pouvez vérifier les paramètres de la tâche, les modifier ou configurer une planification de lancement de la tâche, si nécessaire.

8. Dans la liste des tâches, sélectionnez la tâche que vous avez créée, puis cliquez sur **Démarrer**.

   Vous pouvez également attendre que la tâche se lance conformément à la planification que vous avez spécifiée dans les paramètres de la tâche.

Une fois que la tâche de modification du mot de passe du compte est terminée, le mot de passe du compte local indiqué est modifié sur les appareils indiqués.

Pour garantir le bon fonctionnement des tâches de modification du mot de passe du compte, SELinux doit être désactivé sur l'appareil de l'utilisateur.

Révocation des droits d'administrateur local

Vous pouvez révoquer les droits d'administrateur local des comptes. Cela vous offre un niveau de contrôle supplémentaire sur les comptes utilisateurs. Par exemple, vous pouvez révoquer les droits d'administrateur local à l'issue d'une attribution à usage unique.

Suite à l'exécution de cette tâche, le compte local indiqué vérifie s'il appartient aux groupes d'administrateurs locaux. Ces groupes sont définis dans les paramètres de la stratégie de l'Agent d'administration. Vous pouvez personnaliser la liste des groupes d'administrateurs locaux dans les paramètres de la stratégie de l'Agent d'administration. Vous pouvez également consulter la liste des comptes utilisateurs à privilèges à l'aide du **Rapport sur les utilisateurs d'appareils à privilèges (Linux uniquement)**.

Cette tâche peut être exécutée uniquement sur les appareils Linux.

Pour révoquer les droits d'administrateur local sur des appareils en particulier, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Tâches**.
2. Cliquez sur **Ajouter**.

   Ceci permet de lancer l'Assistant de création d'une tâche.
3. Dans le champ **Type de tâche**, sélectionnez l'option **Révoquer les autorisations d'administrateur local (Linux uniquement)**.
4. Sélectionnez l'une des options ci-dessous :

   - **Attribuer la tâche à un groupe d'administration**

     La tâche est affectée aux appareils qui appartiennent à un groupe d'administration. Vous pouvez renseigner un des groupes existants ou en créer un.

     Par exemple, vous pourriez souhaiter utiliser cette option pour exécuter une tâche d'envoi de messages pour les utilisateurs si le message est particulier pour les appareils repris dans un groupe d'administration spécifique.

     Si une tâche est attribuée à un groupe d'administration, l'onglet **Sécurité** ne s'affiche pas dans la fenêtre des propriétés de la tâche, car les tâches de groupe sont soumises aux paramètres de sécurité des groupes auxquels elles s'appliquent.

   - **Définir les adresses des appareils manuellement ou les importer à partir d'une liste**

     Vous pouvez définir les noms NetBIOS, les noms DNS, les adresses IP, ainsi que les plages d'adresses IP auxquels il convient d'affecter la tâche.

     Vous pourriez utiliser cette option pour exécuter une tâche pour un sous-réseau défini. Par exemple, vous pourriez souhaiter installer une certaine application sur les appareils des comptables ou analyser des appareils dans un sous-réseau qui est probablement infecté.

   - **Attribuer la tâche à une sélection d'appareils**

     La tâche est affectée aux appareils qui appartiennent à une sélection d'appareils. Vous pouvez définir une des sélections existantes.

     Par exemple, vous pourriez souhaiter utiliser cette option pour exécuter une tâche sur des appareils dotés d'une version du système d'exploitation spécifique.

   La tâche *Révoquer les droits d'administrateur local (Linux uniquement)* est créée pour les appareils indiqués. Si vous avez sélectionné l'option **Attribuer la tâche à un groupe d'administration**, la tâche est de groupe.
5. À l'étape Zone d' **Zone de la tâche**, indiquez un groupe d'administration, des appareils avec des adresses spécifiques ou une sélection d'appareils.

   Les paramètres disponibles dépendent de l'option sélectionnée à l'étape précédente.

6. À cette étape de l'Assistant, définissez les paramètres suivants :

   - Dans le groupe de paramètres **Mode de fonctionnement**, sélectionnez le mode de fonctionnement :

     - **Révoquer les privilèges d'administrateur local des comptes répertoriés**

       Si cette option a été sélectionnée, les droits d'administrateur local des comptes locaux indiqués seront révoqués.

       Cette option est sélectionnée par défaut.

     - **Exclure les comptes mentionnés de la révocation des privilèges d'administrateur local**

       Si cette option a été sélectionnée, les droits d'administrateur local seront révoqués pour tous les comptes locaux, sauf les comptes indiqués.

       Par défaut, cette option n'est pas sélectionnée.

   - Indiquez les comptes locaux :

     - Cliquez sur le bouton **Ajouter**.

     - Dans la fenêtre qui s'ouvre, procédez comme suit :

       - Dans le champ **Nom du compte utilisateur**, indiquez le nom du compte local.

       - Dans le groupe de paramètres **Action du compte** (disponible uniquement si l'option **Révoquer les privilèges d'administrateur local des comptes répertoriés** est sélectionnée), sélectionnez l'action.

       - **Garder le compte**

         Si cette option a été sélectionnée, le compte local n'est pas supprimé après la révocation des droits d'administrateur local.

         Cette option est sélectionnée par défaut.

       - **Supprimer le compte**

         Si cette option a été sélectionnée, le compte local sera supprimé, qu'il dispose ou non des droits d'administrateur local.

         Par défaut, cette option n'est pas sélectionnée.

7. À l'étape **Fin de la création de la tâche**, cliquez sur le bouton **Terminer** pour créer la tâche et fermer l'Assistant.

   Si vous avez activé l'option **Ouvrir les détails de la tâche à la fin de la création**, la fenêtre des paramètres de la tâche s'ouvre. Dans cette fenêtre, vous pouvez vérifier les paramètres de la tâche, les modifier ou configurer une planification de lancement de la tâche, si nécessaire.

8. Dans la liste des tâches, sélectionnez la tâche que vous avez créée, puis cliquez sur **Démarrer**.

   Vous pouvez également attendre que la tâche se lance conformément à la planification que vous avez spécifiée dans les paramètres de la tâche.

Lorsque la tâche de révocation des droits d'administrateur local est terminée, les droits d'administrateur local sont révoqués pour les comptes locaux définis sur les appareils en question.

Utilisation des révisions des objets

Cette section contient les informations sur l'utilisation des révisions des objets. Kaspersky Security Center permet de suivre les modifications des objets. Chaque enregistrement de modification dans une objet entraîne la création d'une *révision*. Chaque révision possède un numéro.

Voici les objets de l'application compatibles avec les révisions :

- Propriétés du Serveur d'administration
- Stratégies
- Tâches
- Groupes d'administration
- Comptes utilisateurs
- Paquets d'installation

Vous pouvez réaliser les opérations suivantes avec les révisions d'objets :

- Afficher la révision sélectionnée (disponible uniquement pour les stratégies)
- Annuler les modifications d'un objet jusqu'à la révision sélectionnée
- Enregistrer les révisions dans un fichier JSON (disponible uniquement pour les stratégies)

La section **Historique des révisions** de la fenêtre des propriétés des objets compatibles avec la gestion des révisions reprend une liste des révisions avec les informations suivantes :

- **Révision** – le numéro de la révision de l'objet.
- **Heure** – la date et l'heure de modification de l'objet.
- **Utilisateur** – le nom de l'utilisateur ayant modifié l'objet.
- **Adresse IP de l'appareil de l'utilisateur** – l'adresse IP de l'appareil à partir duquel lequel l'objet a été modifié.
- **Adresse IP de la Web Console** – l'adresse IP de Kaspersky Security Center Web Console avec laquelle l'objet a été modifié.
- **Action** – l'action exécutée avec l'objet.
- **Description** – la description de la révision de modification des paramètres de l'objet.

  Par défaut, la description de la révision de l'objet n'est pas remplie. Pour ajouter une description de la révision, choisissez la révision requise, puis cliquez sur le bouton **Modifier la description**. Dans la fenêtre qui s'ouvre, saisissez un texte correspondant à la description de la révision.

Restauration d'un objet à une révision précédente

En cas de besoin, vous pouvez restaurer les modifications de l'objet. Par exemple, il peut être nécessaire de rétablir les paramètres de la stratégie à leur état à la date définie.

Pour restaurer les modifications d'un objet, procédez comme suit :

1. Dans la fenêtre des propriétés de l'objet, ouvrez l'onglet **Historique des révisions**.
2. Dans la liste des révisions de l'objet, sélectionnez la révision dont vous souhaitez annuler les modifications.
3. Cliquez sur le bouton **Restaurer**.
4. Cliquez sur le bouton **OK** pour confirmer l'opération.

   La version sélectionnée est restaurée. La liste des révisions de l'objet reprend une entrée sur l'action exécutée. La description de la révision affiche les informations sur le numéro de révision rétablie pour l'objet.

L'opération de restauration n'est disponible que pour les objets de stratégie et de tâche.

Ajout d'une description de la révision

Kaspersky Security Center permet de suivre les modifications des objets. Chaque enregistrement de modification dans une objet entraîne la création d'une révision. Chaque révision possède un numéro.

Vous pouvez ajouter une description de la révision afin de pouvoir la retrouver facilement dans la liste à l'avenir.

Pour ajouter une description de la révision, procédez comme suit :

1. Dans la fenêtre des propriétés de l'objet, ouvrez l'onglet **Historique des révisions**.
2. Dans la liste des révisions de l'objet, sélectionnez la révision pour laquelle vous souhaitez ajouter une description.
3. Cliquez sur le bouton **Modifier la description**.

   La fenêtre **Description** s'ouvrira.
4. Dans la fenêtre **Description**, saisissez un texte correspondant à la description de la révision.

   Par défaut, la description de la révision de l'objet n'est pas remplie.
5. Enregistrez la description de la révision.

La description est ajoutée pour la révision de l'objet.

Affichage et enregistrement d'une révision de la stratégie

Kaspersky Security Center permet de consulter les modifications apportées à une stratégie au cours d'une période donnée et d'enregistrer les informations sur ces modifications dans un fichier.

L'affichage et l'enregistrement d'une révision de la stratégie sont disponibles si le plug-in Internet d'administration correspondant prend en charge cette fonctionnalité.

Pour consulter la révision d'une stratégie, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Stratégies et profils**.
2. Cliquez sur la stratégie de la révision que vous souhaitez consulter, puis passez à la section **Historique des révisions**.
3. Dans la liste des révisions de la stratégie, cliquez sur le numéro de la révision que vous souhaitez consulter.

   Si la taille de la révision est supérieure à 10 Mo, vous ne pourrez pas la consulter à l'aide de Kaspersky Security Center Web Console. Vous serez invité à enregistrer la révision sélectionnée dans un fichier JSON.

   Si la taille de la révision ne dépasse pas 10 Mo, un rapport au format HTML avec les paramètres de la révision de la stratégie sélectionnée s'affiche. Comme le rapport s'affiche dans une fenêtre contextuelle, assurez-vous que les fenêtres contextuelles sont autorisées dans votre navigateur.

Pour enregistrer une révision de la stratégie dans un fichier JSON, procédez comme suit :

Dans la liste des révisions de la stratégie, sélectionnez la révision que vous souhaitez enregistrer, puis cliquez sur **Enregistrer dans le fichier**.

La révision est enregistrée dans un fichier JSON.

Suppression d'objets

Cette section fournit des informations sur la suppression d'objets.

Vous pouvez supprimer les objets suivants :

- Stratégies
- Tâches
- Paquets d'installation
- Serveurs d'administration virtuels
- Utilisateurs
- Groupes de sécurité
- Groupes d'administration

Pour supprimer un objet, procédez comme suit :

1. Ouvrez la section requise de Kaspersky Security Center Web Console, puis sélectionnez l'objet.
2. Dans la barre d'outils, cliquez sur le bouton **Supprimer**.
3. Dans la fenêtre qui s'ouvre, cliquez **OK** pour confirmer votre choix.

L'objet sélectionné est supprimé.

Quand vous supprimez un objet, les informations à son sujet demeurent dans la base de données. La Durée de stockage des informations relatives aux objets supprimés est identique à la période de stockage des révisions de l'objet (la période recommandée est de 90 jours). Vous pouvez modifier la durée de conservation uniquement si vous possédez la permission **Modifier** dans la zone de privilèges **Objets supprimés**.

À propos de la suppression des appareils clients

Lorsque vous supprimez un appareil administré d'un groupe d'administration, l'application place l'appareil dans le groupe Appareils non définis. Après la suppression de l'appareil, les applications Kaspersky installées (Agent d'administration et toute application de sécurité, par exemple, Kaspersky Endpoint Security) restent sur l'appareil.

Kaspersky Security Center gère les appareils du groupe Appareils non définis selon les règles suivantes :

- Si vous avez configuré des règles de déplacement d'appareils et qu'un appareil répond aux critères d'une règle de déplacement, l'appareil est automatiquement déplacé vers un groupe d'administration conformément à la règle.

- L' appareil est stocké dans le groupe Appareils non définis et automatiquement supprimé du groupe conformément aux règles de conservation des appareils.

  Les règles de conservation des appareils n'affectent pas les appareils dont un ou plusieurs disques sont chiffrés à l'aide du chiffrement du disque. Ces appareils ne sont pas supprimés automatiquement. Vous ne pouvez les supprimer que manuellement. Si vous devez supprimer un appareil doté d'un disque chiffré, commencez par déchiffrer le disque, puis supprimez l'appareil.

  > Lorsque vous supprimez un appareil doté d'un disque chiffré, les données nécessaires au déchiffrement du disque sont également supprimées. Si vous cochez la case **Je comprends le risque et je souhaite supprimer les appareils sélectionnés** dans la fenêtre de confirmation qui s'ouvre lorsque vous supprimez de tels appareils (soit du groupe **Appareils non définis**, soit du groupe **Appareils administrés**), cela signifie que vous êtes au courant de la suppression des données ultérieure.

  Pour déchiffrer le disque, les conditions suivantes doivent être remplies :

  - L'appareil est reconnecté au Serveur d'administration pour restaurer les données nécessaires au déchiffrement du disque.
  - L'utilisateur de l'appareil se souvient du mot de passe de déchiffrement.
  - L'application de sécurité utilisée pour chiffrer le disque, par exemple, Kaspersky Endpoint Security for Windows, est toujours installée sur l'appareil.

  Si le disque a été chiffré à l'aide de la technologie Kaspersky Disk Encryption, vous pouvez également essayer de récupérer les données à l'aide de l'utilitaire de restauration FDERT.

> Dans VDI, si vous disposez d'un appareil avec des disques chiffrés, les informations contenues sur le disque chiffré sont supprimées après la suppression de l'appareil.

Lorsque vous supprimez manuellement un appareil du groupe Appareils non définis, l'application supprime l'appareil de la liste. Après la suppression de l'appareil, les applications Kaspersky installées (le cas échéant) restent sur l'appareil. Ensuite, si l'appareil est toujours visible pour le Serveur d'administration et que vous avez configuré le sondage du réseau régulier, Kaspersky Security Center découvre l'appareil lors du sondage du réseau et l'ajoute au groupe Appareils non définis. Par conséquent, il est raisonnable de supprimer un appareil manuellement uniquement si l'appareil est invisible pour le Serveur d'administration.

Kaspersky Security Network (KSN)

Cette section explique l'utilisation de l'infrastructure de services en ligne Kaspersky Security Network (KSN). Elle comporte des informations relatives à KSN, ainsi que des instructions pour l'activation de KSN, la configuration de l'accès à KSN et la consultation des statistiques d'utilisation du serveur proxy KSN.

> La fonctionnalité de mises à jour (y compris la fourniture de mises à jour des signatures antivirus et des bases de code), ainsi que la fonctionnalité KSN peuvent ne pas être disponibles dans le logiciel aux États-Unis.

À propos de KSN

Kaspersky Security Network (KSN) est une infrastructure de services en ligne qui donne accès à la base opérationnelle des connaissances de Kaspersky concernant la réputation des fichiers, des ressources Internet et des logiciels. L'utilisation des données de Kaspersky Security Network assure une vitesse de réaction plus élevée des applications de Kaspersky sur les menaces, augmente l'efficacité de fonctionnement de certains modules de protection, ainsi que diminue la possibilité des faux positifs. KSN vous permet de recevoir des informations sur les applications installées sur les appareils administrés. Ces informations se trouvent dans les bases de réputation de Kaspersky.

Kaspersky Security Center est compatible avec les solutions d'infrastructure suivantes :

- *KSN* est une solution qui permet d'échanger des informations avec Kaspersky Security Network. Si vous participez à KSN, vous acceptez de transmettre automatiquement à Kaspersky les informations relatives au fonctionnement des applications de Kaspersky installées sur les appareils clients administrés par le Kaspersky Security Center. Le transfert des informations s'exécute conformément aux paramètres d'accès à KSN configurés. Les analystes de Kaspersky analysent également les informations reçues et les incluent dans les bases de données statistiques et de réputation de Kaspersky Security Network. Kaspersky Security Center utilise cette solution par défaut.

- *Kaspersky Private Security Network (KPSN)* est une solution qui permet aux utilisateurs d'appareils dotés d'applications Kaspersky d'accéder aux bases de données de réputation de Kaspersky Security Network et à d'autres données statistiques sans envoyer de données de leurs propres appareils à KSN global. KPSN est conçu pour les entreprises qui ne peuvent pas participer à Kaspersky Security Network pour l'une des raisons suivantes :

  - Les appareils de l'utilisateur ne sont pas connectés à Internet.

  - La transmission de données à l'extérieur du pays ou à l'extérieur du réseau local de l'entreprise est interdite par la loi ou restreinte par les stratégies de sécurité de l'entreprise.

  Vous pouvez configurer les paramètres d'accès de Kaspersky Private Security NetworK dans la section **Paramètres du proxy KSN** de la fenêtre des propriétés du Serveur d'administration.

L'application vous invite à vous connecter à KSN lors de l'exécution de l'Assistant de configuration initiale de l'application. Vous pouvez commencer à utiliser KSN ou refuser le service KSN à tout moment du fonctionnement de l'application.

Vous utilisez KSN conformément à la Déclaration KSN que vous lisez et acceptez en activant KSN. Si la Déclaration KSN est mise à jour, elle s'affiche lorsque vous mettez à niveau une version du Serveur d'administration. Vous pouvez accepter la Déclaration KSN mise à jour ou la refuser. Si vous le refusez, vous continuez à utiliser KSN conformément à la version précédente de la Déclaration KSN que vous avez acceptée auparavant.

Lorsque KSN est activé, Kaspersky Security Center vérifie si les serveurs KSN sont accessibles. Si l'accès aux serveurs via le DNS système n'est pas possible, l'application utilise les serveurs DNS publics. Cela est nécessaire pour garantir le maintien du niveau de sécurité des appareils administrés.

Les appareils clients administrés par le Serveur d'administration interagissent avec KSN à l'aide du serveur proxy KSN. Le serveur proxy KSN fournit les possibilités suivantes :

- Les appareils clients peuvent exécuter les demandes à KSN, obtenir des informations de KSN et transmettre dans KSN les informations même s'ils n'ont pas d'accès Internet direct.
- Le serveur proxy KSN met en cache les données traitées en diminuant la charge sur le canal du réseau externe et en accélérant l'obtention des informations demandées par l'appareil client.

Vous pouvez configurer le serveur proxy KSN dans la section **Paramètres du proxy KSN** de la fenêtre des propriétés du Serveur d'administration.

Configuration de l'accès à KSN

Vous pouvez configurer l'accès à Kaspersky Security Network (KSN) sur le Serveur d'administration et sur un point de distribution.

Pour configurer l'accès du Serveur d'administration à KSN :

1. Dans le menu principal, cliquez sur l'icône paramètres ( ) en face du nom du Serveur d'administration requis.

   La fenêtre des propriétés du Serveur d'administration s'ouvre.

2. Sous l'onglet **Général**, sélectionnez la section **Paramètres du proxy KSN**.

3. Basculez le commutateur sur la position **Activer le proxy KSN sur le Serveur d'administration Activé**.

   Si cette option est activée, le serveur proxy KSN envoie des données à KSN pour augmenter l'efficacité des modules de Kaspersky Security Center et améliorer les performances des applications de Kaspersky. La transmission des informations depuis les appareils clients vers KSN est régie par la stratégie Kaspersky Endpoint Security active sur ces appareils. Si ce commutateur est désactivé, la transmission des données depuis le Serveur d'administration ou les appareils clients vers KSN via le Kaspersky Security Center ne s'exécute pas. Toutefois, selon leur configuration, les appareils clients peuvent transmettre directement les données à KSN (et non via le Kaspersky Security Center). La stratégie de Kaspersky Endpoint Security appliquée sur les appareils clients définit quelles données de ces appareils sont envoyées directement à KSN (et non via le Kaspersky Security Center).

4. Basculez le commutateur sur la position **Utiliser Kaspersky Security Network Activé**.

   Si cette option est activée, les appareils clients transmettent les résultats de l'installation des correctifs à Kaspersky. Une fois que vous avez activé cette option, vous devez lire et accepter la Déclaration KSN.

   Si vous utilisez KPSN, basculez le commutateur sur la position **Utiliser Kaspersky Private Security Network Activé** et cliquez sur le bouton **Sélectionner le fichier de paramètres de proxy KSN** pour télécharger les paramètres du KPSN (fichiers avec les extensions .pkcs7 et .pem). Suite au téléchargement des paramètres, l'interface affiche le nom du fournisseur, ses coordonnées et la date de création du fichier avec les paramètres de KPSN.

   > Lorsque vous activez KPSN, faites attention aux points de distribution configurés pour envoyer les requêtes KSN directement au Cloud KSN. Les points de distribution sur lesquels l'Agent d'administration version 11 (ou antérieure) est installé continueront d'envoyer des requêtes KSN au Cloud KSN. Pour reconfigurer les points de distribution pour envoyer des requêtes KSN à KPSN, activez l'option **Transférer les requêtes KSN au Serveur d'administration** pour chaque point de distribution. Vous pouvez activer cette option dans les propriétés du point de distribution ou dans la stratégie d'Agent d'administration.

   Lorsque vous basculez le commutateur sur la position **Utiliser Kaspersky Private Security Network Activé**, un message s'affiche avec des détails sur le KPSN.

   Les applications Kaspersky suivantes prennent en charge KPSN :

   - Kaspersky Security Center
   - Kaspersky Endpoint Security for Windows
   - Kaspersky Endpoint Security for Linux
   - Kaspersky Security for Virtualization 3.0 Agentless Service Pack 2
   - Kaspersky Security for Virtualization 3.0 Service Pack 1 Light Agent

   Si vous activez le KPSN dans Kaspersky Security Center, ces applications reçoivent des informations sur la prise en charge de KPSN. Dans la fenêtre de paramètres de l'application, dans la sous-section **Kaspersky Security Network** de la section **Protection avancée**, les informations sur le fournisseur KSN sélectionné s'affichent : KSN ou KPSN.

   > Si vous utilisez KPSN via des versions de l'application antérieures à Kaspersky Security for Virtualization 3.0 Agentless Service Pack 2 ou à Kaspersky Security for Virtualization 3.0 Service Pack 1 Light Agent, il est recommandé d'utiliser les Serveurs d'administration secondaires pour lesquels l'utilisation de KPSN n'a pas été configurée.

   > Kaspersky Security Center n'envoie pas de données statistiques à Kaspersky Security Network si KPSN est configuré dans la section **Paramètres du proxy KSN** de la fenêtre des propriétés du Serveur d'administration.

5. Si vous avez configuré les paramètres du serveur proxy dans les propriétés du Serveur d'administration mais votre architecture réseau nécessite d'utiliser directement le KSN privé, activez l'option **Ignorer les paramètres du serveur proxy lors de la connexion à KPSN**. Dans le cas contraire, les requêtes des applications administrées ne peuvent pas atteindre le KPSN.

6. Configurez les paramètres de connexion du Serveur d'administration au service KSN proxy :

   - Sous **Paramètres de connexion**, pour **Port TCP**, indiquez le numéro du port TCP via lequel la connexion au serveur proxy KSN sera établie. Par défaut, la connexion au serveur proxy KSN est exécutée via le port 13111.

   - Pour que le Serveur d'administration se connecte au serveur proxy KSN via un port UDP, activez l'option **Utiliser un port UDP** et indiquez le numéro du port dans le champ **Port UDP**. Cette option est désactivée et le port TCP est utilisé par défaut. Si cette option est activée, la connexion au serveur proxy KSN est exécutée par défaut via le port UDP 15111.

   - Si vous souhaitez que le Serveur d'administration se connecte au serveur proxy KSN via un port HTTPS, activez l'option **Utiliser HTTPS**, et spécifiez un numéro de port pour **HTTPS par le port**. Cette option est désactivée et le port TCP est utilisé par défaut. Si cette option est activée, la connexion au serveur proxy KSN est exécutée par défaut via le port HTTPS 17111.

7. Basculez le commutateur sur la position **Connecter les Serveurs d'administration secondaires à KSN via le Serveur d'administration principal Activé**.

   Si cette option est activée, les Serveurs d'administration secondaires utilisent le Serveur d'administration principal comme serveur proxy KSN. Si cette option est désactivée, les Serveurs d'administration secondaires se connectent au KSN indépendamment. Dans ce cas, les appareils administrés utilisent les Serveurs d'administration secondaires comme serveurs proxy KSN.

   Les Serveurs d'administration secondaires utilisent le Serveur d'administration principal comme serveur proxy si dans le volet droit de la section **Paramètres du proxy KSN**, dans les propriétés des Serveurs d'administration secondaires, le commutateur est sur la position **Activer le proxy KSN sur le Serveur d'administration Activé**.

8. Cliquez sur le bouton **Enregistrer**.

Cela enregistre les paramètres d'accès à KSN.

Vous pouvez également configurer un accès de point de distribution à KSN, par exemple si vous souhaitez réduire la charge sur le Serveur d'administration. Le point de distribution dont le rôle du serveur proxy KSN envoie directement les requêtes KSN des appareils administrés à Kaspersky, sans utiliser le serveur d'administration.

Pour configurer l'accès du point de distribution à Kaspersky Security Network (KSN) :

1. Vérifiez que le point de distribution est assigné manuellement.

2. Dans le menu principal, cliquez sur l'icône des paramètres ( ) en regard du nom du Serveur d'administration requis.

   La fenêtre des propriétés du Serveur d'administration s'ouvre.

3. Sous l'onglet **Général**, sélectionnez la section **Points de distribution**.

4. Cliquez sur le nom du point de distribution pour ouvrir la fenêtre de propriétés de la tâche.

5. Dans la fenêtre des propriétés du point de distribution, dans la section **Proxy KSN**, activez l'option **Activer le proxy KSN du côté du point de distribution**, puis activez l'option **Accéder à KSN Cloud/KPSN directement via Internet**.

6. Cliquez sur le bouton **OK**.

Le point de distribution agit comme un serveur proxy KSN.

Activation et désactivation de l'utilisation de KSN

Pour activer l'utilisation de KSN, procédez comme suit :

1. Dans le menu principal, cliquez sur l'icône des paramètres ( ) en regard du nom du Serveur d'administration requis.

   La fenêtre des propriétés du Serveur d'administration s'ouvre.

2. Sous l'onglet **Général**, sélectionnez la section **Paramètres du proxy KSN**.

3. Basculez le commutateur sur la position **Activer le proxy KSN sur le Serveur d'administration Activé**.

Le serveur proxy KSN est activé et envoie des données à KSN pour augmenter l'efficacité des modules de Kaspersky Security Center et améliorer les performances des applications de Kaspersky.

1. En fonction de la solution d'infrastructure KSN que vous utilisez, activez les commutateurs correspondants.

   - Si vous utilisez KSN global, basculez le commutateur sur la position **Utiliser Kaspersky Security Network Activé**.

     L'envoi de données à KSN est désormais disponible. Une fois que vous avez activé cette option, vous devez lire et accepter la Déclaration KSN.

   - Si vous utilisez KPSN, basculez le commutateur sur la position **Utiliser Kaspersky Private Security Network Activé**, puis cliquez sur le bouton **Sélectionner le fichier de paramètres de proxy KSN** pour télécharger les paramètres du KPSN (fichiers avec les extensions .pkcs7 et .pem). Suite au téléchargement des paramètres, l'interface affiche le nom du fournisseur, ses coordonnées et la date de création du fichier avec les paramètres de KPSN.

     Lorsque vous basculez le commutateur sur la position **Utiliser Kaspersky Private Security Network Activé**, un message s'affiche avec des détails sur le KPSN.

2. Cliquez sur **Enregistrer**.

Pour désactiver l'utilisation de KSN, procédez comme suit :

1. Dans le menu principal, cliquez sur l'icône des paramètres ( ) en regard du nom du Serveur d'administration requis.

   La fenêtre des propriétés du Serveur d'administration s'ouvre.

2. Sous l'onglet **Général**, sélectionnez la section **Paramètres du proxy KSN**.

3. Basculez le commutateur sur la position **Activer le proxy KSN sur le Serveur d'administration Désactivé** pour désactiver le service KSN Proxy.

4. Cliquez sur le bouton **Enregistrer**.

Affichage de la Déclaration KSN acceptée

Lorsque vous activez Kaspersky Security Network (KSN), vous devez lire et accepter la Déclaration KSN. Vous pouvez consulter à tout moment la déclaration KSN.

Pour afficher la Déclaration KSN acceptée, procédez comme suit :

1. Dans le menu principal, cliquez sur l'icône paramètres ( ) en face du nom du Serveur d'administration requis.

   La fenêtre des propriétés du Serveur d'administration s'ouvre.

2. Sous l'onglet **Général**, sélectionnez la section **Paramètres du proxy KSN**.

3. Cliquez sur le lien **Afficher la Déclaration de Kaspersky Security Network**.

Dans la fenêtre qui s'ouvre, vous pouvez voir le texte de la Déclaration KSN acceptée.

Accepter une Déclaration KSN mise à jour

Vous utilisez KSN conformément à la Déclaration KSN que vous lisez et acceptez en activant KSN. Si la Déclaration KSN est mise à jour, elle s'affiche lorsque vous mettez à niveau une version du Serveur d'administration. Vous pouvez accepter la Déclaration KSN mise à jour ou la refuser. Si vous la refusez, vous continuerez à utiliser KSN conformément à la version précédente de la Déclaration KSN que vous avez acceptée auparavant.

Après la mise à niveau d'une version du Serveur d'administration, la Déclaration KSN mise à jour s'affiche automatiquement. Si vous refusez la Déclaration KSN mise à jour, vous pouvez toujours la consulter et l'accepter ultérieurement.

Pour afficher, puis accepter ou refuser une Déclaration KSN mise à jour, procédez comme suit :

1. Cliquez sur le lien **Afficher les notifications** dans le coin supérieur droit de la fenêtre principale de l'application.

   La fenêtre **Notifications** s'ouvre.

2. Cliquez sur le lien **Afficher la déclaration KSN mise à jour**.

   La fenêtre **Mise à jour de la Déclaration de Kaspersky Security Network** s'ouvre.

3. Lisez la Déclaration KSN, puis faites votre choix en cliquant sur l'un des boutons suivants :

   - **J'accepte la déclaration KSN mise à jour**
   - **Utiliser KSN sous l'ancienne Déclaration**

En fonction de votre choix, KSN continue de fonctionner conformément aux conditions de la Déclaration KSN actuelle ou de celle qui est mise à jour. Vous pouvez consulter le texte de la Déclaration KSN acceptée dans les propriétés du Serveur d'administration à tout moment.

Vérifier si le point de distribution fonctionne en tant que serveur proxy KSN

Sur un appareil administré qui fonctionne comme un point de distribution, vous pouvez activer le serveur proxy KSN. Un appareil administré fonctionne comme un serveur proxy KSN lorsque le service ksnproxy est exécuté sur l'appareil. Vous pouvez vérifier, activer ou désactiver ce service sur l'appareil localement.

Vous pouvez désigner un appareil Windows ou Linux comme point de distribution. La méthode de vérification du point de distribution dépend du système d'exploitation de ce point de distribution.

Pour vérifier si le point de distribution basé sur Windows fonctionne comme serveur proxy KSN, procédez comme suit :

1. Sur l'appareil du point de distribution, sous Windows, ouvrez **Services** (**Tous les programmes** → **Outils d'administration** → **Services**).

2. Dans la liste des services, vérifiez si le service ksnproxy est en cours d'exécution.

   Si le service ksnproxy est en cours d'exécution, l'Agent d'administration de l'appareil participe à Kaspersky Security Network et fonctionne comme serveur proxy KSN pour les appareils administrés inclus dans la zone d'action du point de distribution.

Si vous le souhaitez, vous pouvez désactiver le service ksnproxy. Dans ce cas, l'Agent d'administration sur le point de distribution cesse de participer à Kaspersky Security Network. Cela requiert des autorisations d'administrateur local.

Pour vérifier si le point de distribution basé sur Linux fonctionne comme serveur proxy KSN, procédez comme suit :

1. Sur l'appareil du point de distribution, affichez la liste des processus en cours d'exécution.

2. Dans la liste des processus en cours d'exécution, vérifiez si le processus `/opt/kaspersky/ksc64/sbin/ksnproxy` est en cours d'exécution.

Si le processus `/opt/kaspersky/ksc64/sbin/ksnproxy` est en cours d'exécution, l'Agent d'administration de l'appareil participe à Kaspersky Security Network et fonctionne comme serveur proxy KSN pour les appareils administrés inclus dans la zone d'action du point de distribution.

Scénario de mise à niveau de Kaspersky Security Center et des applications de sécurité administrées

Cette section présente le scénario principal de mise à niveau du Kaspersky Security Center et des applications de sécurité administrées.

La mise à niveau de Kaspersky Security Center et des applications de sécurité administrées s'effectue par étapes :

1. **Vérification de la configuration matérielle et logicielle requise**

   Assurez-vous que votre matériel répond à la configuration requise et installez les mises à jour requises.

2. **Planification des ressources**

   Évaluez l'espace disque occupé par votre base de données. Vérifiez que l'espace libre sur le disque est suffisant pour sauvegarder une copie des paramètres du Serveur d'administration et de la base de données.

3. **Obtenir le fichier d'installation pour Kaspersky Security Center**

   Récupérez le fichier exécutable de la version actuelle de Kaspersky Security Center et enregistrez-le sur l'appareil qui fonctionne comme Serveur d'administration. Lisez les notes de sortie de version de Kaspersky Security Center que vous voulez utiliser.

4. **Création d'une copie de sauvegarde de la version précédente**

   Utilisez l'utilitaire de sauvegarde et de récupération de données pour créer une copie de sauvegarde des données du Serveur d'administration. Vous pouvez également créer une tâche de sauvegarde.

   Il est recommandé d'exporter la liste des plug-ins installés.

5. **Exécuter le programme d'installation**

   Exécutez le fichier exécutable pour la dernière version de Kaspersky Security Center. Pendant l'exécution du fichier, indiquiez que vous disposez d'une copie de sauvegarde et précisez son emplacement. Vos données seront restaurées à partir de la sauvegarde.

6. **Mise à niveau des applications administrées**

   Vous pouvez mettre à niveau l'application si une version plus récente est disponible. Lisez la liste des applications de Kaspersky prises en charge et assurez-vous que votre version de Kaspersky Security Center est compatible avec cette application. Ensuite, mettez à niveau de l'application comme décrit dans les notes de sortie de version.

Résultats

Une fois le scénario de mise à niveau terminé, assurez-vous que la nouvelle version du Serveur d'administration est correctement installée dans Microsoft Management Console. Cliquez sur **Aide → À propos de Kaspersky Security Center**. La version est affichée.

Pour vous assurer que vous utilisez la version la plus récente du Serveur d'administration dans Kaspersky Security Center Web Console, cliquez en haut de l'écran sur l'icône paramètres ( ) à côté du nom du Serveur d'administration. Dans la fenêtre des propriétés du Serveur d'administration qui s'ouvre, dans l'onglet **Général**, sélectionnez la section **Général**. La version est affichée.

Si vous devez restaurer les données du Serveur d'administration, suivez les étapes décrites dans la rubrique suivante : Sauvegarde et restauration des données en mode interactif.

Si vous avez mis à niveau une application de sécurité administrée, vérifiez qu'elle est correctement installée sur le ou le(les) appareil(s) administré(s). Pour plus d'informations, reportez-vous à la documentation de cette application.

Mise à jour des bases de données et des applications Kaspersky

Cette section décrit les étapes à suivre pour effectuer une mise à jour régulière des éléments suivants :

- Bases de données et modules logiciels de Kaspersky
- Applications de Kaspersky installées, y compris les modules et les applications de sécurité de Kaspersky Security Center

La fonctionnalité de mises à jour (y compris la fourniture de mises à jour des signatures antivirus et des bases de code), ainsi que la fonctionnalité KSN peuvent ne pas être disponibles dans le logiciel aux États-Unis.

Scénario : Mise à jour régulière des bases de données et des applications Kaspersky

Cette section fournit un scénario de mise à jour régulière des bases de données, des modules logiciels et des applications Kaspersky. Après avoir terminé le scénario de configuration de la protection du réseau, vous devez conserver la fiabilité du système de protection pour vous assurer que les Serveurs d'administration et les appareils administrés sont protégés contre plusieurs menaces, y compris des virus, des attaques réseau et des attaques par phishing.

La protection du réseau reste à jour pour assurer les mises à jour régulières des éléments suivants :

- Bases de données et modules logiciels de Kaspersky
- Applications de Kaspersky installées, y compris les modules et les applications de sécurité de Kaspersky Security Center

Lorsque vous terminez ce scénario, vous pouvez être sûr que :

- Votre réseau est protégé par le dernier logiciel de Kaspersky, y compris les modules et les applications de sécurité de Kaspersky Security Center.
- Les bases antivirus et les autres bases de données de Kaspersky critiques pour la sécurité du réseau sont toujours à jour.

Prérequis

Les appareils administrés doivent disposer d'une connexion au Serveur d'administration. Si ce n'est pas un cas, pensez à mettre à jour manuellement les bases de données, les modules logiciels et les applications de Kaspersky ou directement à partir des serveurs de mise à jour de Kaspersky.

Le Serveur d'administration doit avoir une connexion à Internet.

Avant de démarrer, assurez-vous que vous avez :

1. Déployé les applications de sécurité de Kaspersky sur les appareils administrés selon le scénario de déploiement des applications de Kaspersky par Kaspersky Security Center Web Console.
2. Créé et configuré l'ensemble des stratégies, profils de stratégie et tâches obligatoire selon le scénario de configuration de la protection du réseau.
3. Désigné une quantité appropriée de points de distribution en fonction du nombre d'appareils administrés et de la topologie du réseau.

Étapes de la mise à jour des bases de données et des applications Kaspersky :

1. **Choix d'un schéma de mise à jour**

   Vous pouvez utiliser plusieurs schémas pour installer les mises à jour des modules et des applications de sécurité de Kaspersky Security Center. Choisissez le schéma ou plusieurs schémas qui répondent le mieux aux exigences de votre réseau.

2. **Création de la tâche de téléchargement des mises à jour dans le stockage du Serveur d'administration**

Cette tâche est créée automatiquement par l'Assistant de configuration initiale de l'application Kaspersky Security Center. Si vous n'aviez pas exécuté l'Assistant, créez la tâche maintenant.

Cette tâche est requise pour télécharger les mises à jour des serveurs de mise à jour de Kaspersky dans le stockage du Serveur d'administration, ainsi que pour mettre à jour les bases de données et les modules logiciels de Kaspersky pour Kaspersky Security Center. Une fois téléchargées, les mises à jour peuvent être propagées vers les appareils administrés.

Si votre réseau comporte des points de distribution désignés, les mises à jour sont automatiquement téléchargées du stockage du Serveur d'administration aux stockages des points de distribution. Dans ce cas, les appareils administrés inclus dans la zone d'action d'un point de distribution téléchargent les mises à jour du stockage du point de distribution au lieu du stockage du Serveur d'administration.

Instructions pour :

- Console d'administration : Création de la tâche de téléchargement des mises à jour dans le stockage du Serveur d'administration
- Kaspersky Security Center Web Console : Création de la tâche de téléchargement des mises à jour dans le stockage du Serveur d'administration

3. **Création de la tâche de téléchargement des mises à jour dans les stockages des points de distribution (facultatif)**

   Par défaut, les mises à jour sont téléchargées sur les points de distribution à partir du Serveur d'administration. Vous pouvez configurer Kaspersky Security Center pour télécharger les mises à jour sur les points de distribution directement à partir des serveurs de mise à jour de Kaspersky. Le téléchargement vers les stockages des points de distribution est préférable si le trafic entre le Serveur d'administration et les points de distribution est plus cher que le trafic entre les points de distribution et les serveurs de mise à jour de Kaspersky ou si votre Serveur d'administration n'a pas d'accès Internet.

   Lorsque votre réseau comporte des points de distribution désignés et que la tâche *Téléchargement des mises à jour sur les stockages des points de distribution* est créée, les points de distribution téléchargent les mises à jour à partir des serveurs de mises à jour de Kaspersky, et non à partir du stockage du Serveur d'administration.

   Instructions pour :

   - Console d'administration : Création de la tâche de téléchargement des mises à jour sur les stockages des points de distribution
   - Kaspersky Security Center Web Console : Création de la tâche de téléchargement des mises à jour sur les stockages des points de distribution

4. **Configuration des points de distribution**

   Lorsque votre réseau comporte des points de distribution désignés, assurez-vous que l'option **Déployer les mises à jour** est activée dans les propriétés de tous les points de distribution nécessaires. Lorsque cette option est désactivée pour un point de distribution, les appareils inclus dans la zone d'action du point de distribution téléchargent les mises à jour à partir du stockage du Serveur d'administration.

   Si vous souhaitez que les appareils administrés reçoivent des mises à jour uniquement à partir des points de distribution, activez l'option **Distribuer les fichiers uniquement via les points de distribution** dans la stratégie de l'Agent d'administration.

5. **Optimisation du processus de mise à jour à l'aide du modèle déconnecté de téléchargement de mise à jour ou des fichiers diff (facultatif)**

   Vous pouvez optimiser le processus de mise à jour à l'aide du modèle déconnecté de téléchargement de mise à jour (activé par défaut) ou à l'aide de fichiers diff. Pour chaque segment du réseau, vous devez choisir laquelle de ces deux fonctions activer car elles ne peuvent pas s'exécuter simultanément.

Lorsque le modèle déconnecté de téléchargement de mise à jour est activé, l'Agent d'administration télécharge les mises à jour nécessaires dans l'appareil administré une fois qu'elles sont téléchargées dans le stockage du Serveur d'administration, avant que l'application de sécurité les demande. Cela améliore la fiabilité du processus de mise à jour. Pour utiliser cette fonctionnalité, activez l'option **Télécharger au préalable les mises à jour et les bases antivirus depuis le Serveur d'administration (recommandé)** dans la stratégie de l'Agent d'administration.

Si vous n'utilisez pas le modèle déconnecté de téléchargement de mise à jour, vous pouvez optimiser le trafic entre le Serveur d'administration et les appareils administrés avec des fichiers diff. Lorsque cette fonction est activée, le Serveur d'administration ou un point de distribution télécharge des fichiers diff au lieu de fichiers entiers de bases de données ou de modules logiciels de Kaspersky. Un fichier diff décrit les différences entre deux version d'un fichier d'une base de données ou d'un module logiciel. Par conséquent, un fichier diff occupe moins d'espace qu'un fichier entier. Cela entraîne une baisse du trafic entre le Serveur d'administration ou les points de distribution et les appareils administrés. Pour utiliser cette fonctionnalité, activez l'option **Télécharger les fichiers diff** dans les propriétés de la tâche *Téléchargement des mises à jour sur le stockage du Serveur d'administration* et/ou de la tâche *Téléchargement des mises à jour sur les stockages des points de distribution*.

Instructions pour :

- Utilisation de fichiers diff pour la mise à jour des bases de données et des modules logiciels Kaspersky
- Console d'administration : Activation et désactivation du modèle déconnecté de téléchargement de mise à jour
- Kaspersky Security Center Web Console : Activation et désactivation du modèle déconnecté de téléchargement de mise à jour

6. **Vérification des mises à jour téléchargées (facultatif)**

Avant d'installer les mises à jour téléchargées, vous pouvez les vérifier via la tâche d'*analyse des mises à jour*. Cette tâche exécute de manière séquentielle les tâches de mise à jour des appareils et les tâches d'analyse des logiciels malveillants pour la collecte spécifiée d'appareils de test. Dès l'obtention des résultats de la tâche, le Serveur d'administration démarre ou bloque la propagation des mises à jour sur les appareils restants.

Dans le cadre de l'exécution de la tâche *Télécharger les mises à jour dans le stockage du Serveur d'administration*, la tâche d'*analyse des mises à jour* peut être exécutée. Dans les propriétés de la tâche de *Télécharger les mises à jour dans le stockage du Serveur d'administration*, activez l'option **Vérifier les mises à jour avant de les déployer** dans la Console d'administration ou l'option **Exécuter la vérification de mise à jour** dans Kaspersky Security Center Web Console.

Instructions pour :

- Console d'administration : Vérification des mises à jour téléchargées
- Kaspersky Security Center Web Console : Vérification des mises à jour téléchargées

7. **Approbation et refus des mises à jour logicielles**

Par défaut, les mises à jour logicielles téléchargées sont à l'état *Non défini*. Vous pouvez modifier l'état en *Approuvée* ou *Rejetée*. Les mises à jour confirmées sont toujours installées. Si une mise à jour nécessite une révision et l'acceptation des termes du Contrat de licence utilisateur final, vous devez d'abord les accepter. Ensuite, la mise à jour peut être propagée sur les appareils administrés. Les mises à jour non définies peuvent uniquement être installées sur l'Agent d'administration et sur les autres modules de Kaspersky Security Center conformément aux paramètres de stratégie de l'Agent d'administration. Les mises à jour auxquelles vous avez attribué l'état *Rejetée* ne seront pas installées sur les appareils. Si une mise à jour rejetée pour une application de sécurité a été installée précédemment, Kaspersky Security Center essaiera de la désinstaller de tous les appareils.

L'approbation et le refus de mises à jour est disponible uniquement pour l'Agent d'administration et les applications Kaspersky administrées installées sur les appareils clients Windows et Linux. La mise à jour transparente du Serveur d'administration, de Kaspersky Security Center Web Console et des plug-ins Web d'administration n'est pas prise en charge.

Instructions pour :

- Console d'administration : Approbation et refus des mises à jour logicielles
- Kaspersky Security Center Web Console : Approbation et refus des mises à jour logicielles

8. **Configuration de l'installation automatique des mises à jour et des correctifs des composants de Kaspersky Security Center**

   Les mises à jour et les correctifs téléchargés pour l'Agent d'administration et les autres composants de Kaspersky Security Center sont installés automatiquement. Si vous n'avez pas laissé l'option **Installer automatiquement les mises à jour et les correctifs nécessaires pour les modules dont l'état est Non défini** activée dans les propriétés de l'Agent d'administration, toutes les mises à jour seront installées automatiquement après leur téléchargement dans le stockage (ou plusieurs stockages). Si l'option est désactivée, les correctifs de Kaspersky chargés avec l'état *Non défini* sont installés après que l'administrateur a modifié leur état pour qu'il soit *Approuvé*.

   Instructions pour :

   - Console d'administration : Activation et désactivation de la mise à jour automatique et de l'installation automatique des correctifs pour les modules de Kaspersky Security Center
   - Kaspersky Security Center Web Console : Activation et désactivation de l'installation automatique des mises à jour et des correctifs pour les modules de Kaspersky Security Center

9. **Installation des mises à jour du Serveur d'administration.**

   Les mises à jour logicielles du Serveur d'administration ne dépendent pas des états de la mise à jour. Elles ne sont pas installées automatiquement et doivent être préalablement approuvées par l'administrateur dans l'onglet **Surveillance** de la Console d'administration (**Serveur d'administration** `<nom du serveur>` → **Surveillance**) ou dans la section **Notifications** de Kaspersky Security Center Web Console (**Surveillance et rapports** → **Notifications**). Ensuite, l'administrateur doit exécuter explicitement l'installation des mises à jour.

10. **Configuration de l'installation automatique des mises à jour des applications de sécurité**

    Créez les tâches de *mise à jour* pour les applications administrées afin de fournir des mises à jour rapides des applications, des modules logiciels et des bases de données Kaspersky, et notamment des bases antivirus. Pour assurer des mises à jour en temps opportun, nous vous recommandons de sélectionner l'option **Lors du téléchargement des mises à jour dans le stockage** lors de la configuration de la planification des tâches.

    Si votre réseau comprend des appareils IPv6 uniquement et que vous souhaitez mettre à jour régulièrement les applications de sécurité installées sur ces appareils, assurez-vous que le Serveur d'administration (version non inférieure à 13.2) et l'Agent d'administration (version non inférieure à 13.2) sont installés sur les appareils administrés.

    Par défaut, les mises à jour de Kaspersky Endpoint Security for Windows et de Kaspersky Endpoint Security for Linux sont installées uniquement après que vous avez redéfini l'état de la mise à jour sur *Approuvée*. Vous pouvez modifier les paramètres des mises à jour dans la tâche de *mise à jour*.

    Si une mise à jour nécessite une révision et l'acceptation des termes du Contrat de licence utilisateur final, vous devez d'abord les accepter. Ensuite, la mise à jour peut être propagée sur les appareils administrés.

    Instructions pour :

    - Console d'administration : Installation automatique des mises à jour pour Kaspersky Endpoint Security sur les appareils
    - Kaspersky Security Center Web Console : Installation automatique des mises à jour pour Kaspersky Endpoint Security sur les appareils

Résultats

Lorsque le scénario est terminé, Kaspersky Security Center est configuré pour mettre à jour les bases de données de Kaspersky et les applications de Kaspersky installées après que les mises à jour sont téléchargées dans le stockage du Serveur d'administration ou dans les stockages des points de distribution. Vous pouvez ensuite passer à la surveillance de l'état du réseau.

À propos de la mise à jour des bases de données, des modules logiciels et des applications de Kaspersky

Pour vous assurer que la protection de vos Serveurs d'administration et des appareils administrés est à jour, vous devez fournir des mises à jour opportunes des éléments suivants :

- Bases de données et modules logiciels de Kaspersky

  Avant de télécharger les bases de données et les modules logiciels de Kaspersky, Kaspersky Security Center vérifie si les serveurs de Kaspersky sont accessibles. Si l'accès aux serveurs via le DNS système n'est pas possible, l'application utilise les serveurs DNS publics. Cela est nécessaire pour s'assurer que les bases de données antivirus sont mises à jour et que le niveau de sécurité est maintenu pour les appareils administrés.

- Applications de Kaspersky installées, y compris les modules et les applications de sécurité de Kaspersky Security Center

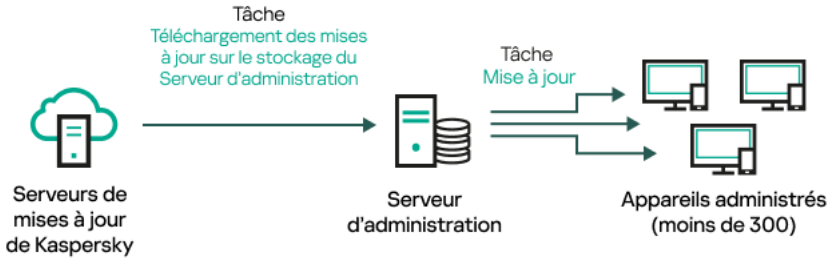
  Kaspersky Security Center permet de mettre à jour automatiquement l'Agent d'administration et les applications Kaspersky installées sur les appareils clients Windows et Linux. La mise à jour transparente du Serveur d'administration, de Kaspersky Security Center Web Console et des plug-ins Web d'administration n'est pas prise en charge. Pour mettre à jour ces modules, vous devez télécharger les dernières versions à partir du site Internet de Kaspersky, puis les installer manuellement.

En fonction de la configuration de votre réseau, vous pouvez utiliser les schémas suivants de téléchargement et de distribution des mises à jour requises sur les appareils administrés :

- En utilisant une seule tâche : *Téléchargement des mises à jour sur le stockage du Serveur d'administration*
- En utilisant deux tâches :
  - *Téléchargement des mises à jour sur le stockage du Serveur d'administration*
  - Tâche de *Téléchargement des mises à jour sur les stockages des points de distribution*
- Manuellement via un dossier local, un dossier partagé ou un serveur FTP
- Directement à partir des serveurs de mise à jour de Kaspersky vers Kaspersky Endpoint Security sur les appareils administrés
- Via un dossier local ou réseau si le Serveur d'administration n'a pas de connexion Internet

Cliquez sur la tâche de Téléchargement des mises à jour sur le stockage du Serveur d'administration

Dans ce schéma, Kaspersky Security Center télécharge les mises à jour via la tâche *Téléchargement des mises à jour sur le stockage du Serveur d'administration*. Dans les petits réseaux qui contiennent moins de 300 appareils administrés dans un segment de réseau unique ou moins de 10 appareils administrés dans chaque segment de réseau, les mises à jour sont distribuées aux appareils administrés directement à partir du stockage du Serveur d'administration (voir figure ci-dessous).

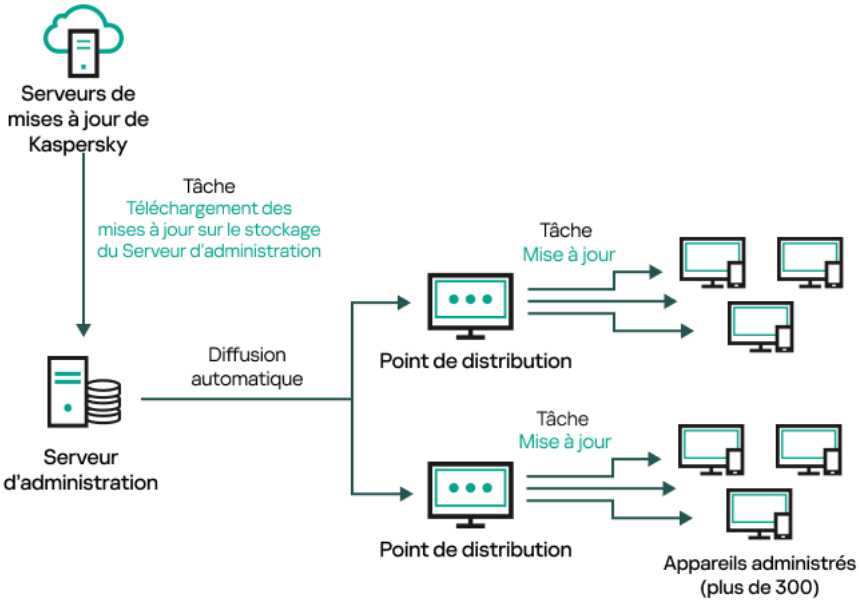


Mise à jour à l'aide de la tâche Téléchargement des mises à jour sur le stockage du Serveur d'administration sans points de distribution

Par défaut, le Serveur d'administration communique avec les serveurs de mise à jour de Kaspersky et télécharge les mises à jour au moyen du protocole HTTPS. Vous pouvez configurer le Serveur d'administration pour qu'il utilise le protocole HTTP au lieu du protocole HTTPS.

Si votre réseau contient plus de 300 appareils administrés ou si votre réseau comprend plusieurs segments de réseau avec plus de 9 appareils administrés dans chacun d'entre eux, nous vous recommandons d'utiliser des points de distribution pour propager les mises à jour vers les appareils administrés (voir figure ci-dessous). Les points de distribution réduisent la charge sur le Serveur d'administration et optimisent le trafic entre le Serveur d'administration et les appareils administrés. Vous pouvez calculer le nombre et la configuration de points de distribution nécessaires pour votre réseau.

Dans ce schéma, les mises à jour sont automatiquement téléchargées du stockage du Serveur d'administration vers les stockages des points de distribution. Les appareils administrés inclus dans la zone d'action d'un point de distribution téléchargent les mises à jour du stockage du point de distribution au lieu du stockage du Serveur d'administration.



Mise à jour à l'aide de la tâche Téléchargement des mises à jour sur le stockage du Serveur d'administration avec points de distribution

Lorsque la tâche *Téléchargement des mises à jour sur le stockage du Serveur d'administration* est terminée, les mises à jour suivantes sont téléchargées dans le stockage du Serveur d'administration :

- Bases de données et modules logiciels de Kaspersky pour Kaspersky Security Center

  Ces mises à jour sont installées automatiquement.

- Bases de données et modules logiciels de Kaspersky pour les applications de sécurité sur les appareils administrés

  Ces mises à jour sont installées via la tâche de mise à jour pour Kaspersky Endpoint Security for Windows.

- Mises à jour du Serveur d'administration

  Ces mises à jour ne sont pas installées automatiquement. L'administrateur doit approuver et exécuter explicitement l'installation des mises à jour.

  > L'installation de correctifs sur le Serveur d'administration requiert des privilèges d'administrateur.

- Mises à jour des modules de Kaspersky Security Center

  Par défaut, ces mises à jour sont installées automatiquement. Vous pouvez modifier les paramètres dans la stratégie de l'Agent d'administration.

- Mises à jour des programmes de protection

  Par défaut, Kaspersky Endpoint Security for Windows installe uniquement les mises à jour que vous approuvez. (Vous pouvez approuver les mises à jour via la Console d'administration ou via Kaspersky Security Center Web Console). Les mises à jour sont installées via la tâche de *mise à jour* et peuvent être configurées dans les propriétés de cette tâche.

> La tâche *Télécharger les mises à jour dans le stockage de la tâche du Serveur d'administration* n'est pas disponible sur les Serveurs d'administration virtuels. Les mises à jour téléchargées sur le Serveur d'administration principal s'affichent dans le stockage du Serveur d'administration virtuel.

Vous pouvez configurer l'analyse des mises à jour reçues sur la productivité et sur la présence des erreurs sur un ensemble d'appareils de test. Si la vérification réussit, les mises à jour sont distribuées à d'autres appareils administrés.

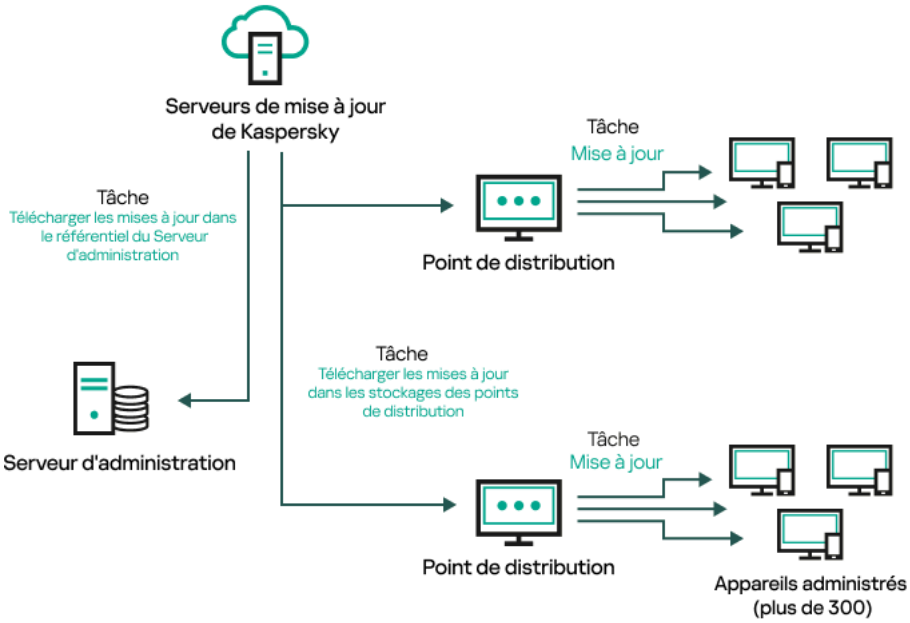
Chaque application de Kaspersky sollicite les mises à jour requises au serveur d'administration. Le Serveur d'administration accumule ces requêtes et télécharge uniquement les mises à jour requises par n'importe quelle application. Cela évite de télécharger les mêmes mises à jour plusieurs fois, voire de télécharger les mises à jour inutiles. Lors de l'exécution de la tâche *Téléchargement des mises à jour sur le stockage du Serveur d'administration*, le Serveur d'administration envoie automatiquement les informations suivantes aux serveurs de mise à jour de Kaspersky afin de garantir le téléchargement des versions appropriées des bases de données et des modules logiciels de Kaspersky :

- ID et version de l'application
- Identifiant d'installation de l'application
- ID de la clé active
- ID d'exécution de la tâche *Télécharger les mises à jour dans le stockage du Serveur d'administration*

Aucune des informations transmises ne contient des données personnelles ou confidentielles. AO Kaspersky Lab protège les informations obtenues conformément aux exigences définies par la loi.

En utilisant deux tâches : la tâche Téléchargement des mises à jour sur le stockage du Serveur d'administration et la tâche Téléchargement des mises à jour sur les stockages des points de distribution

Vous pouvez télécharger des mises à jour vers les stockages des points de distribution directement à partir des serveurs de mise à jour de Kaspersky au lieu du stockage du Serveur d'administration, puis distribuer les mises à jours sur les appareils administrés (voir figure ci-après). Le téléchargement vers les stockages des points de distribution est préférable si le trafic entre le Serveur d'administration et les points de distribution est plus cher que le trafic entre les points de distribution et les serveurs de mise à jour de Kaspersky ou si votre Serveur d'administration n'a pas d'accès Internet.



Mise à jour à l'aide de la tâche Téléchargement des mises à jour sur le stockage du Serveur d'administration et de la tâche Téléchargement des mises à jour sur les stockages des points de distribution

Par défaut, le Serveur d'administration et les points de distribution communiquent avec les serveurs de mise à jour de Kaspersky et télécharge les mises à jour au moyen du protocole HTTPS. Vous pouvez configurer le Serveur d'administration et/ou les points de distribution pour utiliser le protocole HTTP au lieu de HTTPS.

Pour implémenter ce schéma, créez la tâche *Téléchargement des mises à jour sur les stockages des points de distribution* en plus de la tâche *Téléchargement des mises à jour sur le stockage du Serveur d'administration*. Ensuite, les points de distribution téléchargent les mises à jour à partir des serveurs de mise à jour de Kaspersky, et non à partir du stockage du Serveur d'administration.

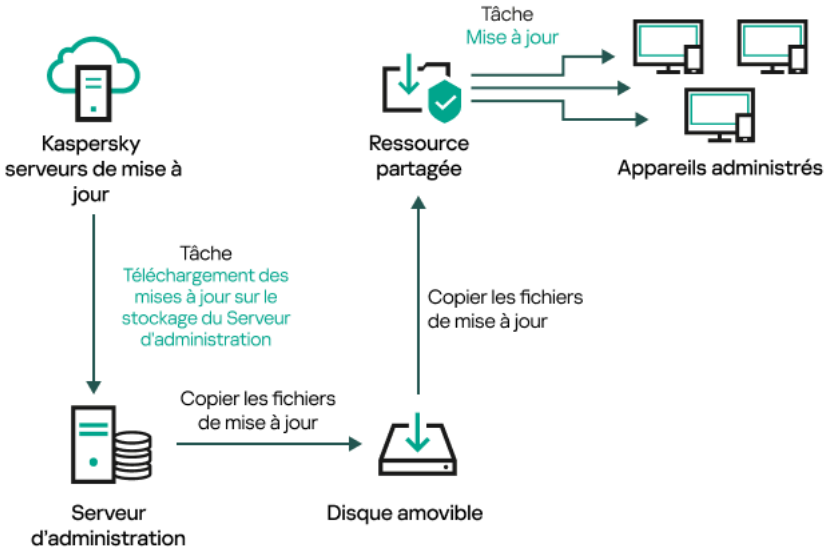
Les appareils de points de distribution exécutant macOS ne peuvent pas télécharger les mises à jour à partir des serveurs de mises à jour de Kaspersky.

Si un ou plusieurs appareils exécutant macOS sont inclus dans la zone d'action de la tâche *Télécharger les mises à jour sur les stockages des points de distribution*, la tâche reçoit l'état *Échec*, même si elle s'est terminée avec succès sur tous les appareils Windows.

La tâche *Téléchargement des mises à jour sur le stockage du Serveur d'administration* est également nécessaire pour ce schéma, car cette tâche sert à télécharger les bases de données et les modules logiciels de Kaspersky pour Kaspersky Security Center.

Manuellement via un dossier local, un dossier partagé ou un serveur FTP

Si les appareils client ne disposent pas d'une connexion au Serveur d'administration, vous pouvez utiliser un dossier local ou une ressource partagée comme source de mise à jour des bases de données, des modules logiciels et des applications de Kaspersky. Dans ce schéma, vous devez copier les mises à jour nécessaires du stockage du Serveur d'administration sur un disque amovible, puis copier les mises à jour dans le dossier local ou dans la ressource spécifiée comme source des mise à jour dans les paramètres de Kaspersky Endpoint Security (voir figure ci-dessous).



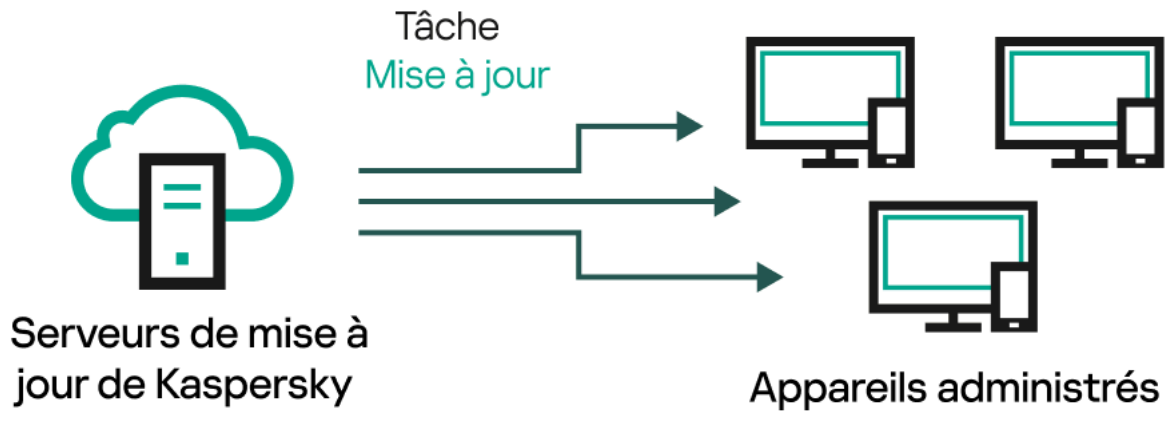
Mise à jour via un dossier local, un dossier partagé ou un serveur FTP

Pour en savoir plus sur les sources des mises à jour dans Kaspersky Endpoint Security, consultez les aides suivantes :

- Aide de Kaspersky Endpoint Security for Windows
- Aide de Kaspersky Endpoint Security for Linux

Directement à partir des serveurs de mise à jour de Kaspersky vers Kaspersky Endpoint Security sur les appareils administrés

Sur les appareils administrés, vous pouvez configurer Kaspersky Endpoint Security pour recevoir directement les mises à jour à partir des serveurs de mise à jour de Kaspersky (voir figure ci-dessous).



Mise à jour des applications de sécurité directement à partir des serveurs de mise à jour de Kaspersky

Dans ce schéma, l'application de sécurité n'utilise pas les stockages fournis par Kaspersky Security Center. Pour recevoir directement les mises à jour à partir des serveurs de mise à jour de Kaspersky, spécifiez ces derniers comme source de mises à jour dans l'interface de l'application de sécurité. Pour plus d'informations sur ces paramètres, consultez les aides suivantes :

- Aide de Kaspersky Endpoint Security for Windows
- Aide de Kaspersky Endpoint Security for Linux

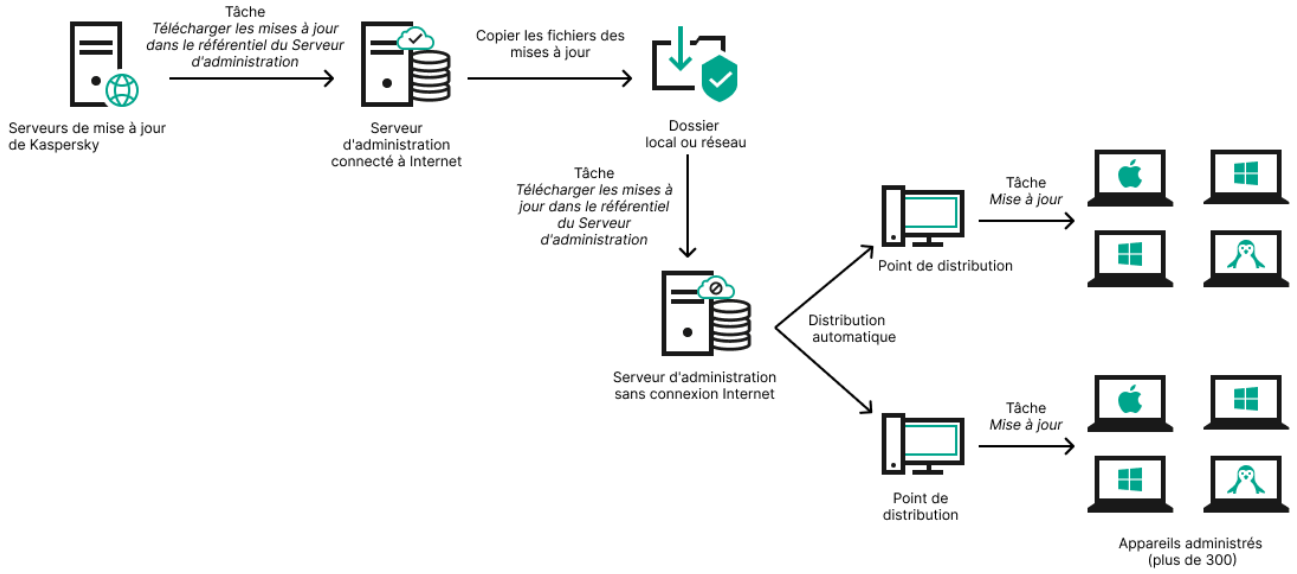
Via un dossier local ou réseau si le Serveur d'administration n'a pas de connexion Internet

Si le Serveur d'administration n'a pas de connexion Internet, vous pouvez configurer la tâche *Téléchargement des mises à jour sur le stockage du Serveur d'administration* pour télécharger les mises à jour à partir d'un dossier local ou réseau. Dans ce cas, vous devez copier les fichiers de mise à jour requis dans le dossier indiqué de temps en temps. Par exemple, vous pouvez copier les fichiers de mise à jour requis à partir de l'une des sources suivantes :

- Serveur d'administration doté d'une connexion Internet (voir la figure ci-dessous)

  Étant donné qu'un Serveur d'administration télécharge uniquement les mises à jour demandées par les applications de sécurité, les ensembles d'applications de sécurité administrés par les Serveurs d'administration (celui qui dispose d'une connexion Internet et celui qui n'en a pas) doivent correspondre.

  Si le Serveur d'administration que vous utilisez pour télécharger les mises à jour a la version 13.2 ou une version antérieure, ouvrez les propriétés de la tâche *Téléchargement des mises à jour sur le stockage du Serveur d'administration*, puis activez l'option **Télécharger les mises à jour en utilisant l'&ancien système**.



Mise à jour via un dossier local ou réseau si le Serveur d'administration n'a pas de connexion Internet

- Kaspersky Update Utility

  Étant donné que cet utilitaire utilise l'ancien schéma pour télécharger les mises à jour, ouvrez les propriétés de la tâche *Téléchargement des mises à jour sur le stockage du Serveur d'administration*, puis activez l'option **Télécharger les mises à jour en utilisant l'&ancien système**.

Créez la tâche Téléchargement des mises à jour sur le stockage du Serveur d'administration

La tâche *Téléchargement des mises à jour sur le stockage du Serveur d'administration* du Serveur d'administration est créée automatiquement par l'Assistant de configuration initiale de l'application Kaspersky Security Center. Vous ne pouvez créer qu'une seule tâche *Téléchargement des mises à jour sur le stockage du Serveur d'administration*. Par conséquent, vous pouvez créer une tâche *Téléchargement des mises à jour sur le stockage du Serveur d'administration* uniquement si elle a été supprimée de la liste des tâches du Serveur d'administration.

Cette tâche est nécessaire pour télécharger les mises à jour des serveurs de mise à jour de Kaspersky sur le stockage du Serveur d'administration. La liste de mises à jour inclut les éléments suivants :

- Mises à jour des bases de données et des modules logiciels pour le Serveur d'administration
- Mises à jour des bases de données et des modules logiciels pour les applications de sécurité Kaspersky
- Mises à jour des modules de Kaspersky Security Center
- Mises à jour des applications de sécurité Kaspersky

Une fois téléchargées, les mises à jour peuvent être propagées vers les appareils administrés.

Avant de distribuer les mises à jour sur les appareils administrés, vous pouvez exécuter la tâche de *vérification des mises à jour*. Cela vous permet de vous assurer que le Serveur d'administration installera correctement les mises à jour téléchargées et qu'un niveau de sécurité ne diminuera pas à cause des mises à jour. Pour les vérifier avant distribution, configurez l'option **Exécuter la vérification de mise à jour** dans les paramètres de la tâche *Téléchargement des mises à jour sur le stockage du Serveur d'administration*.

*Pour créer une tâche **Téléchargement des mises à jour sur le stockage du Serveur d'administration**, procédez comme suit :*

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Tâches**.
2. Cliquez sur **Ajouter**.

   Ceci permet de lancer l'assistant de création d'une tâche. Suivez les étapes de l'assistant.
3. Pour l'application Kaspersky Security Center, sélectionnez le type de tâche **Téléchargement des mises à jour sur le stockage du Serveur d'administration**.
4. Spécifiez le nom de la tâche créée. Le nom de la tâche ne peut pas contenir plus de 100 symboles et contenir de symboles spéciaux ("*<>?\:|).
5. Si vous souhaitez modifier les paramètres de la tâche par défaut, activez l'option **Ouvrir les détails de la tâche à la fin de la création** sur la page **Fin de la création de la tâche**. Si vous n'activez pas cette tâche, la tâche est créée selon les paramètres par défaut. Vous pourrez modifier ces paramètres par défaut plus tard, à tout moment.
6. Cliquez sur le bouton **Créer**.

   La tâche est créée et s'affiche dans la liste des tâches.

7. Cliquez sur le nom de la tâche créée pour ouvrir la fenêtre de propriétés de la tâche.

8. Dans la fenêtre des propriétés de la tâche, onglet **Paramètres de l'application**, spécifiez les paramètres suivants :

- Sources des mises à jour

  Les ressources suivantes peuvent faire office de source des mises à jour pour le Serveur d'administration :

  - Serveurs de mises à jour de Kaspersky

    Serveurs HTTP(S) Kaspersky sur lesquels les applications de Kaspersky récupèrent les mises à jour des bases de données et des modules de l'application. Par défaut, le Serveur d'administration communique avec les serveurs de mise à jour de Kaspersky et télécharge les mises à jour au moyen du protocole HTTPS. Vous pouvez configurer le Serveur d'administration pour qu'il utilise le protocole HTTP au lieu du protocole HTTPS.

    Sélectionné par défaut.

  - Serveur d'administration principal

    Cette ressource s'applique aux tâches créées pour un Serveur d'administration virtuel ou secondaire.

  - Dossier local ou réseau

    Un dossier local ou de réseau qui contient les mises à jour les plus récentes. Un dossier de réseau peut être un serveur FTP ou HTTP ou un dossier partagé SMB. Si un dossier réseau nécessite une authentification, seul le protocole SMB est pris en charge. Lors de la sélection du dossier local, il faut indiquer le dossier sur l'appareil avec le Serveur d'administration installé.

    > Un serveur FTP ou http ou un dossier de réseau utilisé par une source des mises à jour doit contenir une structure de dossiers (avec les mises à jour) qui correspond à la structure créée lors de l'utilisation des serveurs de mise à jour de Kaspersky.

  Si le dossier partagé contenant les mises à jour est protégé par un mot de passe, activez l'option **Indiquer le compte utilisateur pour accéder au dossier partagé de la source des mises à jour (le cas échéant)** et saisissez les informations d'identification du compte requises pour l'accès.

- Dossier de stockage des mises à jour

  Le chemin d'accès au dossier spécifié pour stocker les mises à jour enregistrées. Vous pouvez copier le chemin du dossier spécifié dans un presse-papiers. Vous ne pouvez pas modifier le chemin d'accès à un dossier spécifié pour une tâche de groupe.

- Autres paramètres :

  - Forcer la mise à jour des Serveurs d'administration secondaires

    Si cette option est activée, le Serveur d'administration lance les tâches de mise à jour sur les Serveurs d'administration secondaires dès que de nouvelles mises à jour sont téléchargées. Les tâches de mise à jour sont lancées en utilisant la source de mise à jour configurée dans les propriétés de la tâche sur les Serveurs d'administration secondaires.

    Si cette option est désactivée, les tâches de mise à jour sur les Serveurs d'administration secondaires sont lancées conformément à leur programmation.

    Cette option est Inactif par défaut.

- **Copier les mises à jour récupérées dans des dossiers complémentaires**

  Après que le Serveur d'administration reçoit les mises à jour, il les copie dans les dossiers indiqués. Utilisez cette option si vous voulez administrer manuellement la distribution des mises à jour sur votre réseau.

  Par exemple, vous pourriez vouloir utiliser cette option dans la situation suivante : le réseau de votre organisation comprend plusieurs sous-réseaux indépendants et les appareils sur chacun de ces sous-réseaux n'ont pas accès aux autres sous-réseaux. Toutefois, les appareils dans tous les sous-réseaux ont accès à un dossier partagé central. Dans ce cas, vous installez le Serveur d'administration dans un des sous-réseaux pour télécharger les mises à jour depuis les serveurs de mise à jour de Kaspersky, vous activez cette option, puis vous définissez ce dossier partagé réseau. Dans les tâches de téléchargement des mises à jour dans le stockage pour les autres Serveurs d'administration, définissez le nom du dossier réseau partagé en tant que source des mises à jour.

  Cette option est Inactif par défaut.

- **Ne pas forcer la mise à jour des appareils et des Serveurs d'administration secondaires avant la fin de la copie**

  Les tâches de téléchargement des mises à jour sur les appareils clients et les Serveurs d'administration secondaires démarrent uniquement après la copie de ces mises à jour depuis le dossier de mise à jour principal vers les dossiers de mise à jour complémentaires.

  Cette option doit être activée si les appareils clients et les Serveurs d'administration secondaires téléchargent les mises à jour depuis des dossiers réseau complémentaires.

  Cette option est Inactif par défaut.

- **Contenu des mises à jour** :

  - **Télécharger les fichiers diff**

    Cette option active la fonction de téléchargement des fichiers diff.

    Cette option est Inactif par défaut.

- **Télécharger les mises à jour en utilisant l'ancien système**

Depuis la version 14, Kaspersky Security Center télécharge les mises à jour des bases de données et des modules logiciels en utilisant le nouveau schéma. Pour que l'application télécharge les mises à jour à l'aide du nouveau schéma, la source de mise à jour doit contenir les fichiers de mise à jour avec les métadonnées compatibles avec le nouveau schéma. Si la source de mise à jour contient les fichiers de mise à jour avec les métadonnées compatibles avec l'ancien schéma uniquement, activez l'option **Télécharger les mises à jour en utilisant l'ancien système**. Sinon, la tâche de téléchargement de la mise à jour échouera.

Par exemple, vous devez activer cette option lorsqu'un dossier local ou réseau est spécifié comme source de mise à jour et que les fichiers de mise à jour de ce dossier ont été téléchargés par l'une des applications suivantes :

- Kaspersky Update Utility

  Cet utilitaire télécharge les mises à jour en utilisant l'ancien schéma.

- Kaspersky Security Center 13.2 ou version antérieure

  Par exemple, votre Serveur d'administration 1 n'a pas de connexion Internet. Dans ce cas, vous pouvez télécharger les mises à jour à l'aide d'un Serveur d'administration 2 doté d'une connexion Internet, puis placer les mises à jour dans un dossier local ou réseau pour l'utiliser comme source de mise à jour pour le Serveur d'administration 1. Si le Serveur d'administration 2 dispose de la version 13.2 ou antérieure, activez l'option **Télécharger les mises à jour en utilisant l'ancien système** dans la tâche du Serveur d'administration 1.

Cette option est Inactif par défaut.

- **Exécuter la vérification de mise à jour**

Le Serveur d'administration télécharge les mises à jour depuis la source, les enregistre dans un stockage provisoire et exécute la tâche définie dans le champ **Tâche d'analyse des mises à jour**. Si la tâche aboutit, les mises à jour sont copiées depuis le stockage local vers un dossier partagé sur le Serveur d'administration, puis elles sont distribuées sur tous les appareils pour lesquels le Serveur d'administration fait office de source des mises à jour (les tâches dont le type de planification est **Lors du téléchargement des mises à jour dans le stockage** sont lancées). La tâche de téléchargement des mises à jour sur les référentiels se termine uniquement après la fin de la tâche d'*analyse des mises à jour*.

Cette option est Inactif par défaut.

9. Dans la fenêtre des propriétés de la tâche, onglet **Programmation**, créez une planification pour le démarrage de la tâche. Le cas échéant, configurez les paramètres suivants :

- Démarrer la tâche :

  Sélectionnez la programmation de l'exécution de la tâche, puis configurez la programmation sélectionnée.

  - Manuel

    La tâche ne s'exécute pas automatiquement. Vous pouvez uniquement la lancer manuellement.

    Cette option est sélectionnée par défaut.

  - Toutes les N minutes

    La tâche s'exécute régulièrement, à l'intervalle défini en minutes, à partir de l'heure indiquée le jour de la création de la tâche.

    La tâche s'exécute par défaut toutes les 30 minutes, à partir de l'heure actuelle du système.

  - Toutes les N heures

    La tâche s'exécute régulièrement, selon l'intervalle défini en heures, à partir de la date et heure définis.

    La tâche s'exécute par défaut toutes les six heures à partir de la date et de l'heure actuelles du système.

  - Tous les N jours

    La tâche s'exécute régulièrement, selon l'intervalle défini en jours. En outre, vous pouvez spécifier la date et l'heure de la première exécution de la tâche. Ces options supplémentaires deviennent disponibles si elles sont prises en charge par l'application pour laquelle vous créez la tâche.

    La tâche s'exécute par défaut chaque jour, à partir de la date et de l'heure actuelle du système.

  - Selon les jours de la semaine

    La tâche s'exécute régulièrement les jours définis de la semaine, à l'heure indiquée.

    Par défaut, la tâche s'exécute chaque vendredi à 18h00.

  - Chaque mois

    La tâche s'exécute régulièrement le jour du mois défini, à l'heure indiquée.

    Si le jour en question ne figure pas dans le mois, la tâche s'exécute le dernier jour.

    La tâche s'exécute par défaut le premier jour de chaque mois, à l'heure système actuelle.

  - Mensuellement, les jours indiqués des semaines sélectionnées

La tâche s'exécute régulièrement les jours du mois définis, à l'heure indiquée.

Par défaut, aucun jour du mois n'est sélectionné. L'heure de début par défaut est 18:00.

- **Lors de la détection d'une propagation de virus**

  La tâche s'exécute après un événement *Attaque de virus* de virus. Sélectionnez les types d'application qui vont surveiller les propagations de virus. Les types suivants de Application sont présent :

  - Antivirus pour postes de travail et serveurs de fichiers
  - Antivirus de protection du périmètre
  - Antivirus pour systèmes de messagerie

  Tous les types d'application sont cochés par défaut.

  Il se peut que vous souhaitiez exécuter différentes tâches en fonction du type d'application de sécurité qui signale une propagation de virus. Dans ce cas, supprimez la sélection des types d'application dont vous n'avez pas besoin.

- **À la fin d'une autre tâche**

  La tâche actuelle démarre à la fin d'une autre tâche. Cette option ne fonctionne que si les deux tâches sont affectées aux mêmes appareils. Par exemple, vous pouvez exécuter la tâche *Administration des appareils* avec l'option **&Activer l'appareil** et, une fois celle-ci terminée, exécuter la tâche de *recherche de virus* comme tâche de déclenchement.

  Il faut sélectionner la tâche de déclenchement dans le tableau et l'état avec lequel cette tâche doit se terminer (**Terminée avec succès** ou **Échec**).

  Si nécessaire, vous pouvez rechercher, trier et filtrer les tâches dans le tableau comme suit :

  - Saisissez le nom de la tâche dans le champ de recherche pour rechercher une tâche par son nom.
  - Cliquez sur l'icône de tri pour trier les tâches par nom.

    Par défaut, les tâches sont triées par ordre alphabétique croissant.
  - Cliquez sur l'icône du filtre, et dans la fenêtre qui s'ouvre, filtrez les tâches par groupe, puis cliquez sur le bouton **Appliquer**.

- **Lancer les tâches non exécutées**

Cette option détermine le comportement d'une tâche si un appareil client n'est pas visible sur le réseau quand la tâche est sur le point de démarrer.

Si la case est Activé, lors du lancement suivant de l'application de Kaspersky sur cet appareil client, une tentative de lancement de la tâche sera faite. Si la programmation de la tâche est **Manuel**, **Une fois** ou **Immédiatement**, la tâche est immédiatement lancée dès que l'appareil apparaît sur le réseau ou immédiatement après l'inclusion de l'appareil dans la zone d'action de la tâche.

Si cette option est désactivée, seules les tâches planifiées s'exécutent sur les appareils clients. Pour les planifications **Manuel**, **Une fois** et **Immédiatement**, les tâches s'exécutent uniquement sur les appareils clients qui sont visibles sur le réseau. Par exemple, vous pouvez désactiver cette option pour une tâche qui consomme des ressources que vous voulez exécuter uniquement en dehors des heures de bureau.

Cette option est Inactif par défaut.

- Adopter un décalage aléatoire automatique pour les lancements de tâche

  Si cette option est activée, la tâche est lancée sur les appareils clients de manière aléatoire au cours d'un intervalle défini. C'est ce qu'on appelle un *lancement échelonné d'une tâche*. Un lancement échelonné de tâche permet d'éviter la communication simultanée d'un nombre important d'appareils clients avec le Serveur d'administration lors du lancement de la tâche programmée.

  Le temps du lancement aléatoire est automatiquement calculée lors de la création d'une tâche selon le nombre d'appareils clients sur lesquels la tâche est diffusée. Par la suite, la tâche démarre toujours à l'heure de lancement calculée. Toutefois, quand les paramètres de la tâche sont modifiés ou si la tâche est lancée manuellement, la valeur calculée de l'heure de lancement de la tâche est modifiée.

  Si la case n'est pas cochée, le lancement de la tâche sur les appareils clients s'opère selon la planification.

- Décaler aléatoirement et automatiquement le lancement de la tâche dans un intervalle de

  Si cette option est activée, la tâche est lancée sur les appareils clients de manière aléatoire au cours de l'intervalle défini. Un lancement échelonné de tâche permet d'éviter la communication simultanée d'un nombre important d'appareils clients avec le Serveur d'administration lors du lancement de la tâche programmée.

  Si la case n'est pas cochée, le lancement de la tâche sur les appareils clients s'opère selon la planification.

  Cette option est Inactif par défaut. Par défaut, la valeur de cet intervalle est de une minute.

- Arrêter la tâche si elle prend plus de

  A l'issue du délai défini, la tâche s'arrête automatiquement, qu'elle soit finie ou non.

  Activez cette option si vous souhaitez interrompre (ou arrêter) les tâches dont l'exécution dure trop longtemps.

  Cette option est Inactif par défaut. La durée d'exécution de la tâche par défaut est de 120 minutes.

10. Cliquez sur le bouton **Enregistrer**.

La tâche est créée et configurée.

Quand le Serveur d'administration exécute la tâche *Téléchargement des mises à jour sur le stockage du Serveur d'administration*, les mises à jour des bases de données et des modules logiciels sont téléchargées depuis la source de mise à jour et stockées dans le dossier partagé du Serveur d'administration. Si une tâche est créée pour un groupe d'administration, elle est diffusée uniquement aux Agents d'administration inclus dans le groupe d'administration indiqué.

Les mises à jour du dossier partagé sur le Serveur d'administration sont diffusées sur les appareils clients et les Serveurs d'administration secondaires.

Analyse des mises à jour récupérées

Avant l'installation des mises à jour sur les appareils administrés, vous pouvez d'abord vérifier l'efficacité des mises à jour et rechercher les erreurs via la tâche d'*analyse des mises à jour*. Au cours de la tâche *Téléchargement des mises à jour sur le stockage du Serveur d'administration*, la tâche d'*analyse des mises à jour* est exécutée automatiquement. Le Serveur d'administration télécharge les mises à jour depuis la source, les enregistre dans le stockage temporaire et exécute la tâche d'*analyse des mises à jour*. Si la tâche réussit, les mises à jour sont copiées depuis le stockage temporaire vers le dossier partagé du Serveur d'administration. Elles sont diffusées à l'ensemble des appareils clients pour lesquels le Serveur d'administration est la source des mises à jour.

Si, à la fin de la tâche d'*analyse des mises à jour* placées dans le stockage temporaire, les mises à jour sont considérées comme incorrectes ou si la tâche d'*analyse des mises à jour* se solde sur une erreur, la copie de ces mises à jour dans le dossier partagé n'a pas lieu. La version précédente des mises à jour est conservée sur le Serveur d'administration. De plus, les tâches disposant du type de programmation **Lors du téléchargement des mises à jour dans le stockage** n'ont pas encore été lancées. Ces opérations sont réalisées à la prochaine exécution de la tâche *Téléchargement des mises à jour sur le stockage du Serveur d'administration*, si l'analyse des nouvelles mises à jour réussit.

L'ensemble de mises à jour est considéré comme incorrect si une des conditions suivantes est remplie sur au moins un appareil d'essai :

- Une erreur s'est produite pendant l'exécution de la tâche de mise à jour.
- Après l'application des mises à jour, l'état de la protection en temps réel de l'application de sécurité est modifié.
- Un objet infecté a été identifié durant la tâche d'analyse à la demande.
- Une erreur de l'application de Kaspersky s'est produite.

Si aucune des conditions citées n'est remplie sur aucun des appareils d'essai, alors les mises à jour sont considérées comme correctes et la tâche d'*analyse des mises à jour* a réussi.

Avant de commencer à créer la tâche de *vérification des mises à jour*, réalisez les prérequis :

1. Créez un groupe d'administration avec plusieurs appareils de test. Vous aurez besoin de ce groupe pour vérifier les mises à jour.

   Nous recommandons d'utiliser des appareils bien protégés avec la configuration logicielle la plus répandue dans le réseau de l'entreprise. Cette approche augmente la qualité et la probabilité de détection des virus lors des analyses et minimise le risque de faux positifs. En cas de détection de virus sur les appareils d'essai, la tâche d'*analyse des mises à jour* échoue.

2. Créez les tâches Mise à jour et Analyse des logiciels malveillants pour une application prise en charge par Kaspersky Security Center, par exemple, Kaspersky Endpoint Security for Windows ou Kaspersky Security for Windows Server. Lors de la création des tâches Mise à jour et Analyse des logiciels malveillants, indiquez le groupe d'administration avec les appareils de test.

   La tâche *Vérification des mises à jour* exécute séquentiellement les tâches Mise à jour et Analyse des logiciels malveillants sur les appareils de test pour vérifier que toutes les mises à jour sont valides. De plus, lors de la création de la tâche *Vérification des mises à jour*, vous devez spécifier les tâches Mise à jour et Analyse des logiciels malveillants.

3. Créez la tâche *Téléchargement des mises à jour sur le stockage du Serveur d'administration*.

Pour que Kaspersky Security Center analyse les mises à jour reçues avant de les diffuser sur les appareils clients, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Tâches**.

2. Cliquez sur la tâche **Téléchargement des mises à jour sur le stockage du Serveur d'administration**.

3. Dans la fenêtre des propriétés de la tâche qui s'ouvre, accédez à l'onglet **Paramètres de l'application**, puis activez l'option **Exécuter la vérification de mise à jour**.

4. Si la tâche de *vérification des mises à jour* existe, cliquez sur le bouton **Sélectionnez une tâche**. Dans la fenêtre qui s'ouvre, sélectionnez la tâche de *vérification des mises à jour* dans le groupe d'administration avec les appareils de test.

5. Si vous n'avez pas créé la tâche de *vérification des mises à jour* auparavant, procédez comme suit :

   a. Cliquez sur le bouton **Nouvelle tâche**.

   b. Dans l'Assistant de création d'une tâche qui s'ouvre, indiquez le nom de la tâche si vous souhaitez modifier le nom prédéfini.

   c. Sélectionnez le groupe d'administration avec les appareils de test que vous avez créé précédemment.

   d. Sélectionnez d'abord la tâche Mise à jour d'une application requise prise en charge par Kaspersky Security Center, puis la tâche Analyse des logiciels malveillants.

   Après cela, les options suivantes s'affichent. Nous vous recommandons de les laisser activés :

   - **Redémarrer l'appareil après la mise à jour des bases de données**

     Une fois que les bases de données antivirus sont mises à jour sur un appareil, nous vous recommandons de redémarrer l'appareil.

     L'option est activée par défaut.

   - **Vérifier l'état de la protection en temps réel après la mise à jour des bases de données et le redémarrage de l'appareil**

     Si cette option est activée, la tâche de *vérification des mises à jour* vérifie si les mises à jour téléchargées dans le stockage du Serveur d'administration sont valides et si le niveau de protection a diminué après la mise à jour de la base antivirus et le redémarrage de l'appareil.

     Cette option est activée par défaut.

   e. Indiquez un compte à partir duquel la tâche de *vérification des mises à jour* sera exécutée. Vous pouvez utiliser votre compte et laisser l'option **Compte par défaut** activée. Vous pouvez également indiquer que la tâche doit être exécutée sous un autre compte disposant des droits d'accès nécessaires. Pour ce faire, sélectionnez l'option **Indiquer un compte**, puis saisissez les informations d'identification de ce compte.

6. Fermez la fenêtre des propriétés de la tâche *Téléchargement des mises à jour sur le stockage du Serveur d'administration* en cliquant sur le bouton **Enregistrer**.

La vérification de la mise à jour automatique est activée. Vous pouvez maintenant exécuter la tâche *Téléchargement des mises à jour sur le stockage du Serveur d'administration* et elle démarrera à partir de la vérification des mises à jour.

Création de la tâche de téléchargement des mises à jour sur les stockages des points de distribution

La tâche de *téléchargement de mises à jour dans les stockages de points de distribution* ne fonctionne que sur les appareils de point de distribution exécutant Windows. Les appareils de points de distribution fonctionnant sous Linux ou macOS ne peuvent pas télécharger les mises à jour à partir des serveurs de mises à jour de Kaspersky. Si au moins un appareil fonctionnant Linux ou macOS se trouve dans la zone d'action de la tâche, la tâche présentera l'état *Échec*. Même si la tâche est terminée avec succès sur tous les appareils Windows, elle renverra une erreur sur les appareils restants.

Vous pouvez créer la tâche *Télécharger les mises à jour sur les stockages des points de distribution* pour un groupe d'administration. Cette tâche est exécutée pour les points de distribution inclus dans le groupe d'administration indiqué.

Vous pouvez utiliser cette tâche par exemple si le trafic entre le Serveur d'administration et le ou les point(s) de distribution est plus cher que le trafic entre le ou les point(s) de distribution et les serveurs de mise à jour de Kaspersky ou si votre Serveur d'administration n'a pas d'accès Internet.

Cette tâche est nécessaire pour télécharger les mises à jour des serveurs de mise à jour de Kaspersky dans les stockages des points de distribution. La liste de mises à jour inclut les éléments suivants :

- Mises à jour des bases de données et des modules logiciels pour les applications de sécurité Kaspersky
- Mises à jour des modules de Kaspersky Security Center
- Mises à jour des applications de sécurité Kaspersky

Une fois téléchargées, les mises à jour peuvent être propagées vers les appareils administrés.

Si les points de distribution se connectent à Internet en utilisant un serveur proxy, vous devez définir les paramètres correspondants dans la stratégie de l'Agent d'administration.

*Pour créer la tâche **Téléchargement des mises à jour sur les stockages des points de distribution** pour un groupe d'administration sélectionné, procédez comme suit :*

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Tâches**.
2. Cliquez sur le bouton **Ajouter**.

   Ceci permet de lancer l'assistant de création d'une tâche. Suivez les étapes de l'Assistant.
3. Pour l'application Kaspersky Security Center, dans le champ **Type de tâche**, sélectionnez **Téléchargement des mises à jour sur les stockages des points de distribution**.
4. Spécifiez le nom de la tâche créée. Le nom de la tâche ne peut pas contenir plus de 100 symboles et contenir de symboles spéciaux ("*<>?\:|).
5. Sélectionnez un bouton d'option pour spécifier le groupe d'administration, la sélection d'appareils ou les appareils auxquels la tâche s'applique.
6. À l'étape **Fin de la création de la tâche**, si vous souhaitez modifier les paramètres de tâche par défaut, activez l'option **Ouvrir les détails de la tâche à la fin de la création**. Si vous n'activez pas cette tâche, la tâche est créée selon les paramètres par défaut. Vous pourrez modifier ces paramètres par défaut plus tard, à tout moment.
7. Cliquez sur le bouton **Créer**.

   La tâche est créée et s'affiche dans la liste des tâches.
8. Cliquez sur le nom de la tâche créée pour ouvrir la fenêtre de propriétés de la tâche.

9. Dans l'onglet **Paramètres de l'application** de la fenêtre des propriétés de la tâche, spécifiez les paramètres suivants :

- **Sources des mises à jour**

  Les ressources suivantes peuvent faire office de source des mises à jour pour le point de distribution :

  - Serveurs de mise à jour de Kaspersky

    Serveurs HTTP(S) Kaspersky sur lesquels les applications de Kaspersky récupèrent les mises à jour des bases de données et des modules de l'application.

    Par défaut, cette option est sélectionnée.

  - Dossier local ou réseau

    Un dossier local ou de réseau qui contient les mises à jour les plus récentes. Un dossier de réseau peut être un serveur FTP ou HTTP ou un dossier partagé SMB. Si un dossier réseau nécessite une authentification, seul le protocole SMB est pris en charge. Lors de la sélection du dossier local, il faut indiquer le dossier sur l'appareil avec le Serveur d'administration installé.

    Un serveur FTP ou http ou un dossier de réseau utilisé par une source des mises à jour doit contenir une structure de dossiers (avec les mises à jour) qui correspond à la structure créée lors de l'utilisation des serveurs de mise à jour de Kaspersky.

- **Dossier de stockage des mises à jour**

  Le chemin d'accès au dossier spécifié pour stocker les mises à jour enregistrées. Vous pouvez copier le chemin du dossier spécifié dans un presse-papiers. Vous ne pouvez pas modifier le chemin d'accès à un dossier spécifié pour une tâche de groupe.

- **Télécharger les fichiers diff**

  Cette option active la fonction de téléchargement des fichiers diff.

  Cette option est Inactif par défaut.

- **Télécharger les mises à jour en utilisant l'ancien système**

Depuis la version 14, Kaspersky Security Center télécharge les mises à jour des bases de données et des modules logiciels en utilisant le nouveau schéma. Pour que l'application télécharge les mises à jour à l'aide du nouveau schéma, la source de mise à jour doit contenir les fichiers de mise à jour avec les métadonnées compatibles avec le nouveau schéma. Si la source de mise à jour contient les fichiers de mise à jour avec les métadonnées compatibles avec l'ancien schéma uniquement, activez l'option **Télécharger les mises à jour en utilisant l'ancien système**. Sinon, la tâche de téléchargement de la mise à jour échouera.

Par exemple, vous devez activer cette option lorsqu'un dossier local ou réseau est spécifié comme source de mise à jour et que les fichiers de mise à jour de ce dossier ont été téléchargés par l'une des applications suivantes :

- Kaspersky Update Utility

  Cet utilitaire télécharge les mises à jour en utilisant l'ancien schéma.

- Kaspersky Security Center 13.2 ou version antérieure

  Par exemple, un point de distribution est configuré pour prendre les mises à jour d'un dossier local ou réseau. Dans ce cas, vous pouvez télécharger les mises à jour à l'aide d'un Serveur d'administration doté d'une connexion Internet, puis placer les mises à jour dans le dossier local du point de distribution. Si le Serveur d'administration dispose de la version 13.2 ou antérieure, activez l'option **Télécharger les mises à jour en utilisant l'ancien système** dans la tâche *Télécharger les mises à jour dans les stockages des points de distribution*.

Cette option est Inactif par défaut.

10. Créez une programmation pour le démarrage de la tâche. Le cas échéant, configurez les paramètres suivants :

- **Démarrer la tâche**

  Sélectionnez la programmation de l'exécution de la tâche, puis configurez la programmation sélectionnée.

  - **Manuel**

    La tâche ne s'exécute pas automatiquement. Vous pouvez uniquement la lancer manuellement.

    Cette option est sélectionnée par défaut.

  - **Toutes les N minutes**

    La tâche s'exécute régulièrement, à l'intervalle défini en minutes, à partir de l'heure indiquée le jour de la création de la tâche.

    La tâche s'exécute par défaut toutes les 30 minutes, à partir de l'heure actuelle du système.

  - **Toutes les N heures**

    La tâche s'exécute régulièrement, selon l'intervalle défini en heures, à partir de la date et heure définis.

    La tâche s'exécute par défaut toutes les six heures à partir de la date et de l'heure actuelles du système.

  - **Tous les N jours**

    La tâche s'exécute régulièrement, selon l'intervalle défini en jours. En outre, vous pouvez spécifier la date et l'heure de la première exécution de la tâche. Ces options supplémentaires deviennent disponibles si elles sont prises en charge par l'application pour laquelle vous créez la tâche.

    La tâche s'exécute par défaut chaque jour, à partir de la date et de l'heure actuelle du système.

  - **Par jours de la semaine**

    La tâche s'exécute régulièrement les jours définis de la semaine, à l'heure indiquée.

    Par défaut, la tâche s'exécute chaque vendredi à 18h00.

  - **Chaque mois**

    La tâche s'exécute régulièrement le jour du mois défini, à l'heure indiquée.

    Si le jour en question ne figure pas dans le mois, la tâche s'exécute le dernier jour.

    La tâche s'exécute par défaut le premier jour de chaque mois, à l'heure système actuelle.

  - **Chaque mois, les jours indiqués des semaines sélectionnées**

La tâche s'exécute régulièrement les jours du mois définis, à l'heure indiquée.

Par défaut, aucun jour du mois n'est sélectionné. L'heure de début par défaut est 18:00.

- **Lors de la détection d'une attaque de virus**

  La tâche s'exécute après un événement *Attaque de virus* de virus. Sélectionnez les types d'application qui vont surveiller les propagations de virus. Les types suivants de Application sont présent :

  - Antivirus pour postes de travail et serveurs de fichiers
  - Antivirus de protection du périmètre
  - Antivirus pour systèmes de messagerie

  Tous les types d'application sont cochés par défaut.

  Il se peut que vous souhaitiez exécuter différentes tâches en fonction du type d'application de sécurité qui signale une propagation de virus. Dans ce cas, supprimez la sélection des types d'application dont vous n'avez pas besoin.

- **Après l'exécution d'une autre tâche**

  La tâche actuelle démarre à la fin d'une autre tâche. Cette option ne fonctionne que si les deux tâches sont affectées aux mêmes appareils. Par exemple, vous pouvez exécuter la tâche *Administration des appareils* avec l'option **&Activer l'appareil** et, une fois celle-ci terminée, exécuter la tâche de *recherche de virus* comme tâche de déclenchement.

  Il faut sélectionner la tâche de déclenchement dans le tableau et l'état avec lequel cette tâche doit se terminer (**Terminée avec succès** ou **Échec**).

  Si nécessaire, vous pouvez rechercher, trier et filtrer les tâches dans le tableau comme suit :

  - Saisissez le nom de la tâche dans le champ de recherche pour rechercher une tâche par son nom.
  - Cliquez sur l'icône de tri pour trier les tâches par nom.

    Par défaut, les tâches sont triées par ordre alphabétique croissant.
  - Cliquez sur l'icône du filtre, et dans la fenêtre qui s'ouvre, filtrez les tâches par groupe, puis cliquez sur le bouton **Appliquer**.

- **Lancer les tâches non exécutées**

Cette option détermine le comportement d'une tâche si un appareil client n'est pas visible sur le réseau quand la tâche est sur le point de démarrer.

Si la case est Activé, lors du lancement suivant de l'application de Kaspersky sur cet appareil client, une tentative de lancement de la tâche sera faite. Si la programmation de la tâche est **Manuel**, **Une fois** ou **Immédiatement**, la tâche est immédiatement lancée dès que l'appareil apparaît sur le réseau ou immédiatement après l'inclusion de l'appareil dans la zone d'action de la tâche.

Si cette option est désactivée, seules les tâches planifiées s'exécutent sur les appareils clients. Pour les planifications **Manuel**, **Une fois** et **Immédiatement**, les tâches s'exécutent uniquement sur les appareils clients qui sont visibles sur le réseau. Par exemple, vous pouvez désactiver cette option pour une tâche qui consomme des ressources que vous voulez exécuter uniquement en dehors des heures de bureau.

Cette option est Inactif par défaut.

- Adopter un décalage aléatoire automatique pour les lancements de tâche

  Si cette option est activée, la tâche est lancée sur les appareils clients de manière aléatoire au cours d'un intervalle défini. C'est ce qu'on appelle un *lancement échelonné d'une tâche*. Un lancement échelonné de tâche permet d'éviter la communication simultanée d'un nombre important d'appareils clients avec le Serveur d'administration lors du lancement de la tâche programmée.

  Le temps du lancement aléatoire est automatiquement calculée lors de la création d'une tâche selon le nombre d'appareils clients sur lesquels la tâche est diffusée. Par la suite, la tâche démarre toujours à l'heure de lancement calculée. Toutefois, quand les paramètres de la tâche sont modifiés ou si la tâche est lancée manuellement, la valeur calculée de l'heure de lancement de la tâche est modifiée.

  Si la case n'est pas cochée, le lancement de la tâche sur les appareils clients s'opère selon la planification.

- Décaler aléatoirement et automatiquement le lancement de la tâche dans un intervalle de

  Si cette option est activée, la tâche est lancée sur les appareils clients de manière aléatoire au cours de l'intervalle défini. Un lancement échelonné de tâche permet d'éviter la communication simultanée d'un nombre important d'appareils clients avec le Serveur d'administration lors du lancement de la tâche programmée.

  Si la case n'est pas cochée, le lancement de la tâche sur les appareils clients s'opère selon la planification.

  Cette option est Inactif par défaut. Par défaut, la valeur de cet intervalle est de une minute.

11. Cliquez sur le bouton **Enregistrer**.

    La tâche est créée et configurée.

    En plus des paramètres que vous définissez lors de la création de la tâche, vous pouvez modifier d'autres propriétés de la tâche créée.

Suite à l'exécution de la tâche *Téléchargement des mises à jour sur les stockages des points de distribution*, les mises à jour des bases de données et des modules des applications sont téléchargées depuis la source de mises à jour et stockées dans le dossier partagé. Les mises à jour chargées sont utilisées uniquement par les points de distribution qui appartiennent au groupe d'administration indiqué et pour lesquels il n'existe aucune tâche de téléchargement des mises à jour clairement définie.

Activation et désactivation de l'installation automatique des mises à jour et des correctifs pour les modules de Kaspersky Security Center

Les mises à jour et les correctifs du Serveur d'administration ne peuvent être installés que manuellement après obtention de l'approbation explicite de l'administrateur.

L'installation automatique des mises à jour pour les modules de Kaspersky Security Center est activée par défaut lors de l'installation de l'Agent d'administration sur l'appareil. Vous pouvez la désactiver lors de l'installation de l'Agent d'administration ou plus tard, à l'aide d'une stratégie.

Pour désactiver l'installation automatique des mises à jour pour les modules de Kaspersky Security Center lors de l'installation locale de l'Agent d'administration sur l'appareil, procédez comme suit :

1. Lancez l'installation locale de l'Agent d'administration sur l'appareil.
2. À l'étape **Paramètres complémentaires**, décochez la case **Installer automatiquement les mises à jour et les correctifs applicables aux composants dont la case à cocher de statut est Non défini**.
3. Suivez les instructions de l'assistant.

   L'Agent d'administration s'installe sur l'appareil sans l'option d'installé des mises à jour et des correctifs pour les modules de Kaspersky Security Center. Vous pouvez activer l'installation automatique plus tard à l'aide d'une stratégie.

Pour désactiver l'installation automatique des mises à jour pour les modules de Kaspersky Security Center lors de l'installation de l'Agent d'administration sur l'appareil à l'aide d'un paquet d'installation, procédez comme suit :

1. Dans le menu principal, accédez à **Opérations → Stockages → Paquets d'installation**.
2. Cliquez sur le paquet **Agent d'administration de Kaspersky Security Center <numéro de version>**.
3. Dans la fenêtre des propriétés, ouvrez l'onglet **Paramètres**.
4. Désactivez le commutateur **Installer automatiquement les mises à jour et les correctifs nécessaires pour les modules dont l'état est Non défini**.

   L'Agent d'administration est installé depuis ce paquet avec l'option d'installation automatique des mises à jour et des correctifs pour les modules de Kaspersky Security Center désactivée. Vous pouvez activer l'installation automatique plus tard à l'aide d'une stratégie.

Si lors de l'installation de l'Agent d'administration sur un appareil la case a été cochée (décochée), vous pouvez ultérieurement désactiver (activer) l'installation automatique à l'aide d'une stratégie de l'Agent d'administration.

Pour activer ou désactiver l'installation automatique des mises à jour et les correctifs pour les modules de Kaspersky Security Center à l'aide d'une stratégie de l'Agent d'administration, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Stratégies et profils**.
2. Cliquez sur la stratégie de l'Agent d'administration.
3. Dans la fenêtre des propriétés de la stratégie, ouvrez l'onglet **Paramètres de l'application**.
4. Dans la section **Administration des correctifs et des mises à jour**, désactivez le commutateur **Installer automatiquement les mises à jour et les correctifs nécessaires pour les modules dont l'état est Non défini** pour activer ou désactiver respectivement l'installation automatique des mises à jour et des correctifs.
5. Fermez le cadenas (🔒) de ce bouton à bascule.

La stratégie est appliquée aux appareils sélectionnés et l'installation automatique des mises à jour et des correctifs pour les modules de Kaspersky Security Center est activée (désactivée) sur ces appareils.

Installation automatique des mises à jour pour Kaspersky Endpoint Security for Windows

Vous pouvez configurer les mises à jour automatiques des bases de données et des modules logiciels Kaspersky Endpoint Security for Windows sur les appareils clients.

Pour configurer le téléchargement et l'installation automatique des mises à jour de Kaspersky Endpoint Security for Windows sur les appareils, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Tâches**.
2. Cliquez sur le bouton **Ajouter**.

   Ceci permet de lancer l'assistant de création d'une tâche. Suivez les étapes de l'assistant.
3. Pour l'application Kaspersky Endpoint Security for Windows, sélectionnez **Mise à jour** comme sous-type de tâche.
4. Spécifiez le nom de la tâche créée. Le nom de la tâche ne peut pas contenir plus de 100 symboles et contenir de symboles spéciaux ("*<>?\:|).
5. Choisissez la zone d'action de la tâche.
6. Spécifiez le groupe d'administration, la sélection d'appareils ou les appareils auxquels la tâche s'applique.
7. À l'étape **Fin de la création de la tâche**, si vous souhaitez modifier les paramètres de tâche par défaut, activez l'option **Ouvrir les détails de la tâche à la fin de la création**. Si vous n'activez pas cette tâche, la tâche est créée selon les paramètres par défaut. Vous pourrez modifier ces paramètres par défaut plus tard, à tout moment.
8. Cliquez sur le bouton **Créer**.

   La tâche est créée et s'affiche dans la liste des tâches.
9. Cliquez sur le nom de la tâche créée pour ouvrir la fenêtre de propriétés de la tâche.

10. Dans l'onglet **Paramètres de l'application** des propriétés de la tâche, définissez les paramètres de la tâche de mise à jour en mode local ou mobile :

    - **Mode local** : la connexion est établie entre l'appareil et le Serveur d'administration.
    - **Mode mobile** : la connexion n'est pas établie entre l'appareil et Kaspersky Security Center (par exemple, quand l'appareil n'est pas connecté à Internet).

11. Activez les sources de mise à jour que vous souhaitez utiliser pour mettre à jour des bases de données et des modules d'application pour Kaspersky Endpoint Security for Windows. Si nécessaire, modifiez les positions des sources dans la liste avec les boutons **Haut** et **Bas**. Si plusieurs sources de mise à jour sont activées, Kaspersky Endpoint Security for Windows essaie de s'y connecter les unes après les autres, en commençant par le haut de la liste, et effectue la tâche de mise à jour en récupérant le paquet de mise à jour à partir de la première source disponible.

12. Activez l'option **Installer les mises à jour des modules de l'application approuvés** pour télécharger et installer simultanément les mises à jour des modules logiciels avec les bases de l'application.

    Si l'option est activée, Kaspersky Endpoint Security for Windows informe l'utilisateur des mises à jour de module logiciel disponibles et les inclut dans le paquet de mise à jour lors de l'exécution de la tâche de mise à jour. Kaspersky Endpoint Security for Windows installe uniquement les mises à jour pour lesquelles vous avez défini le statut *Approuvé* . ils seront installés localement via l'interface de l'application ou via Kaspersky Security Center.

    Vous pouvez aussi activer l'option **Installer automatiquement les mises à jour critiques des modules d'application**. Si des mises à jour sont disponibles pour les modules logiciels, Kaspersky Endpoint Security for Windows installe automatiquement ceux qui ont le statut *Critique*. les mises à jour restantes seront installées après leur approbation.

    Si la mise à jour des modules implique la lecture et l'acception des conditions du Contrat de licence et de la Politique de confidentialité, l'application installe les mises à jour après que l'utilisateur a accepté ces conditions.

13. Cochez la case **Copier les mises à jour dans un dossier** pour que l'application enregistre les mises à jour téléchargées dans un dossier indiqué, puis spécifiez le chemin du dossier.

14. Planifiez la tâche. Pour garantir des mises à jour opportunes, nous vous recommandons de sélectionner l'option **Lors du téléchargement des mises à jour dans le stockage**.

15. Cliquez sur **Enregistrer**.

Lors de l'exécution de la tâche **Mise à jour**, l'application envoie des requêtes aux serveurs de mise à jour de Kaspersky.

Certaines mises à jour requièrent l'installation des versions les plus récentes des plug-ins d'administration.

Approbation et refus des mises à jour du logiciel

Les paramètres d'une tâche d'installation de mise à jour peuvent nécessiter l'approbation des mises à jour à installer. Vous pouvez approuver les mises à jour à installer et refuser les mises à jour qui ne doivent pas installer.

Par exemple, vous souhaitez d'abord vérifier l'installation des mises à jour dans un environnement d'essai et vous assurer qu'elles ne perturbent pas le fonctionnement des appareils avant d'autoriser l'installation de ces mises à jour sur les appareils clients.

L'approbation et le refus de mises à jour est disponible uniquement pour l'Agent d'administration et les applications administrées installées sur les appareils clients Windows. La mise à jour transparente du Serveur d'administration, de Kaspersky Security Center Web Console et des plug-ins Web d'administration n'est pas prise en charge. Pour mettre à jour ces modules, vous devez télécharger les dernières versions à partir du site Internet de Kaspersky, puis les installer manuellement.

Pour approuver ou refuser une ou plusieurs mises à jour :

1. Dans le menu principal, accédez à **Opérations → Applications Kaspersky → Mises à jour transparentes**.

   Une liste des mises à jour disponibles s'affiche.

   Les mises à jour des applications administrées peuvent nécessiter l'installation d'une version minimale spécifique de Kaspersky Security Center. Si cette version est postérieure à votre version actuelle, ces mises à jour sont affichées mais ne peuvent pas être approuvées. De plus, aucun paquet d'installation ne peut être créé à partir de ces mises à jour tant que vous n'avez pas mis à niveau Kaspersky Security Center. Vous êtes invité à mettre à niveau votre instance de Kaspersky Security Center vers la version minimale requise.

2. Sélectionnez les mises à jour que vous souhaitez approuver ou refuser.

3. Cliquez sur **Approuver** pour approuver les mises à jour sélectionnées ou sur **Refuser** pour les refuser.

   Par défaut, la valeur *Non défini* est cochée.

Les mises à jour auxquelles vous attribuez l'état *Approuvée* sont placées dans une file d'attente d'installation.

Les mises à jour auxquelles vous attribuez l'état *Rejetée* sont supprimées (si possible) de tous les appareils sur lesquels elles avaient été installées. Et elles ne seront installées sur aucun autre appareil à l'avenir.

Il est impossible de désinstaller certaines mises à jour pour les applications de Kaspersky. Si vous leur attribuez l'état *Rejetée*, Kaspersky Security Center ne les supprime pas des appareils sur lesquels elles avaient été installées. Toutefois, ces mises à jour ne seront jamais installées sur d'autres appareils à l'avenir.

Si vous attribuez l'état *Rejetée* aux mises à jour du logiciel tiers, ces mises à jour ne sont pas installées sur les appareils où elles ont été planifiées mais pas encore installées. Les mises à jour seront conservées sur les appareils où elles ont déjà été installées. Si vous devez supprimer les mises à jour, vous pouvez le faire manuellement en local.

Mise à jour du Serveur d'administration

Vous pouvez installer les mises à jour du Serveur d'administration à l'aide de l'Assistant de mise à jour du Serveur d'administration.

Pour installer une mise à jour du Serveur d'administration :

1. Dans le menu principal, accédez à **Opérations → Applications Kaspersky → Mises à jour transparentes**.
2. Lancez l'Assistant de mise à jour du Serveur d'administration d'une des façons suivantes :
   - Cliquez sur le nom d'une mise à jour du Serveur d'administration dans la liste des mises à jour, et dans la fenêtre qui s'ouvre, cliquez sur le lien **Exécuter l'Assistant de mise à jour du Serveur d'administration**.
   - Cliquez sur le lien **Exécuter l'Assistant de mise à jour du Serveur d'administration** dans le champ de notification en haut de la fenêtre.
3. Dans la fenêtre Assistant de mise à jour du Serveur d'administration, sélectionnez l'une des options suivantes pour indiquer quand installer une mise à jour :
   - **Installer maintenant**. Choisissez cette option, si vous voulez installer maintenant la mise à jour.
   - **&Reporter l'installation**. Choisissez cette option, si vous voulez installer la mise à jour plus tard. Dans ce cas, une notification concernant cette mise à jour s'affichera.
   - **Ignorer cette mise à jour**. Sélectionnez cette option si vous ne souhaitez pas installer de mise à jour et ne souhaitez pas recevoir de notifications concernant cette mise à jour.
4. Sélectionnez le **Faire une copie de sauvegarde du Serveur d'administration avant l'installation de la mise à jour** si vous souhaitez créer une sauvegarde du Serveur d'administration avant d'installer la mise à jour.
5. Cliquez sur le bouton **OK** pour fermer l'Assistant.

Dans le processus de sauvegarde est interrompu, le processus d'installation de mise à jour est également interrompu.

Activation et désactivation d'un modèle hors ligne de téléchargement des mises à jour

Il est déconseillé de désactiver le modèle hors ligne de téléchargement des mises à jour. La désactivation peut entraîner un échec dans la remise des mises à jour aux appareils. Dans certains cas, un expert du Support Technique de Kaspersky peut vous recommander de désactiver l'option **Téléchargement des mises à jour et des bases antivirus depuis le Serveur d'administration**. Ensuite, vous devrez confirmer que la tâche de récupération des mises à jour pour les applications de Kaspersky a été configurée.

Pour activer ou désactiver le modèle hors ligne de téléchargement des mises à jour pour le groupe d'administration, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils) → Stratégies et profils**.
2. Cliquez sur **Groupes**.
3. Dans la structure de groupes d'administration, sélectionnez le groupe d'administration pour lequel il faut activer le modèle déconnecté de téléchargement des mises à jour.

4. Cliquez sur la stratégie de l'Agent d'administration.

   La fenêtre des propriétés de la stratégie de l'Agent d'administration s'ouvre.

   Par défaut, les paramètres des stratégies enfant sont héritées des stratégies parent et ne peuvent pas être modifiées. Si la stratégie que vous voulez modifier est héritée, vous devez d'abord créer une nouvelle stratégie pour l'Agent d'administration dans le groupe d'administration requis. Dans la nouvelle stratégie créée, vous pouvez modifier les paramètres qui ne sont pas verrouillés dans la stratégie parent.

5. Sous l'onglet **Paramètres de l'application**, sélectionnez la section **Administration des correctifs et des mises à jour**.

6. Activez ou désactivez l'option **Télécharger au préalable les mises à jour et les bases antivirus depuis le Serveur d'administration (recommandé)** pour activer ou désactiver, respectivement, le modèle hors ligne de téléchargement de mise à jour.

   Par défaut, le modèle hors ligne de téléchargement des mises à jour est activé.

Suite à cette action, le modèle hors ligne de téléchargement des mises à jour est activé ou désactivé.

Mise à jour des bases de données et des modules logiciels de Kaspersky sur des appareils déconnectés

La mise à jour des bases de données et des modules logiciels de Kaspersky sur des appareils administrés est une tâche importante pour maintenir la protection des appareils contre les virus et les autres menaces. Les administrateurs configurent habituellement des mises à jour régulières via le stockage du Serveur d'administration ou les stockages des points de distribution.

Lorsque vous devez mettre à jour les bases de données et les modules logiciels sur un appareil (ou un groupe d'appareils) non connecté au Serveur d'administration (principal ou secondaire), à un point de distribution ou à Internet, vous devez utiliser d'autres sources de mise à jour comme un serveur FTP ou un dossier local. Dans ce cas, vous devez livrer les fichiers des mises à jour nécessaires à l'aide d'un appareil de stockage de masse comme un disque flash ou un disque dur externe.

Vous pouvez copier les mises à jour nécessaires à partir des éléments suivants :

- Serveur d'administration.

  Pour garantir que le stockage du Serveur d'administration contient les mises à jour nécessaires à l'application de sécurité installée sur un appareil déconnecté, au moins un des appareils connectés administrés doit avoir la même application de sécurité installée. Cette application doit être configurée pour recevoir les mises à jour du stockage du Serveur d'administration via la tâche Téléchargement des mises à jour sur le stockage du Serveur d'administration.

- Tout appareil qui a la même application de sécurité installée et configuré pour recevoir les mises à jour à partir du stockage du Serveur d'administration, d'un stockage de point de distribution ou directement à partir des serveurs de mises à jour de Kaspersky.

Voici un exemple de configuration des bases de données et des modules logiciels par copie à partir du stockage du Serveur d'administration.

Pour mettre à jour des bases de données et des modules logiciels de Kaspersky sur des appareils déconnectés :

1. Connectez le disque amovible à l'appareil où le Serveur d'administration est installé.
2. Copiez les fichiers de mises à jour sur le disque amovible.

   Par défaut, les mises à jour se trouvent à l'emplacement suivant : \\<nom du serveur>\KLSHARE\Updates.

   Sinon, vous pouvez configurer Kaspersky Security Center pour copier régulièrement les mises à jour dans le dossier sélectionné. Pour ce faire, utilisez l'option **Copier les mises à jour récupérées dans des dossiers complémentaires** dans les propriétés de la tâche Téléchargement des mises à jour sur le stockage du Serveur d'administration. Si vous spécifiez un dossier situé sur un disque flash ou un disque dur externe sur le dossier de destination pour cette option, cet appareil de stockage de masse contiendra toujours la dernière version des mises à jour.
3. Sur les appareils déconnectés, configurez l'application de sécurité (par exemple, Kaspersky Endpoint Security for Windows) pour recevoir les mises à jour à partir d'un dossier local ou d'une ressource partagée, comme un serveur FTP ou un dossier partagé.
4. Copiez les fichiers de mise à jour du disque amovible dans le dossier local ou dans la ressource partagée à utiliser comme source de mise à jour.
5. Sur l'appareil déconnecté qui nécessite l'installation des mises à jour, démarrez la tâche de mise à jour de Kaspersky Endpoint Security for Windows.

Une fois que la tâche de mise à jour est terminée, les bases de données et les modules logiciels de Kaspersky sont à jour sur l'appareil.

Sauvegarde et restauration des plug-ins Web

Kaspersky Security Center Web Console vous permet de sauvegarder l'état actuel d'un plug-in Web pour pouvoir restaurer l'état enregistré ultérieurement. Par exemple, vous pouvez sauvegarder un plug-in Web avant de le mettre à jour vers une version plus récente. Après la mise à jour, si la nouvelle version ne répond pas à vos exigences ou à vos attentes, vous pouvez restaurer la version précédente du plug-in Web à partir de la sauvegarde.

Pour sauvegarder les plug-ins Web :

1. Dans le menu principal, accédez à **Paramètres** → **Plug-ins Web**.
2. Dans la section **Plug-ins Web**, sélectionnez les plug-ins Web que vous souhaitez sauvegarder, puis cliquez sur le bouton **Créer une copie de sauvegarde**.

Les plug-ins Web sélectionnés sont sauvegardés. Vous pouvez afficher les sauvegardes créées sur l'onglet **Sauvegardes**.

Pour restaurer un plug-in Web à partir d'une sauvegarde :

1. Dans le menu principal, accédez à la section **Paramètres** → **Sauvegardes**.
2. Dans la section **Sauvegardes**, sélectionnez la sauvegarde du plug-in Web que vous souhaitez restaurer, puis cliquez sur le bouton **Restaurer depuis la Sauvegarde**.

Le plug-in Web est restauré à partir de la sauvegarde sélectionnée.

Réglage des points de distribution et des passerelles de connexion

La structure des groupes d'administration dans Kaspersky Security Center exerce les fonctions suivantes :

- Désignation de la zone d'action des stratégies.

  Il existe une autre méthode d'application des paramètres nécessaires sur les appareils : le recours aux *profils de stratégie*. Dans ce cas, vous définissez la zone d'action des stratégies avec des tags, les emplacements des appareils dans les unités organisationnelles Active Directory ou l'appartenance aux groupes de sécurité Active Directory.

- Désignation de la zone d'action des tâches de groupe.

  Il y existe une méthode de désignation de la zone d'action des tâches de groupe qui ne repose pas sur la hiérarchie des groupes d'administration : l'utilisation de tâche pour des sélections d'appareils et des ensembles d'appareils.

- Désignation des privilèges d'accès aux appareils et aux Serveurs d'administration secondaires et virtuels

- Ceci assigne les points de distribution.

Lors de la mise en place de la structure de groupes d'administration, il faut prendre en considération la topologie du réseau de l'entreprise pour garantir la désignation optimale des points de distribution. La distribution optimale des points de distribution permet de diminuer le trafic réseau à l'intérieur du réseau de l'entreprise.

En fonction de la structure organisationnelle de l'entreprise et de la topologie des réseaux, les configurations typiques suivantes de structure des groupes d'administration existent :

- Un bureau

- plusieurs petits bureaux isolés

Les appareils fonctionnant comme points de distribution doivent être protégés, y compris physiquement contre tout accès non autorisé.

Configuration typique des points de distribution : un bureau simple

Dans la configuration typique " un bureau ", tous les appareils se trouvent sur le réseau de l'entreprise et se " voient ". Le réseau de l'entreprise peut comprendre plusieurs " parties " mises en évidence (des réseaux ou des segments de réseau) et reliées par des canaux étroits.

Les moyens suivants de construction de la structure de groupes d'administration existent :

- Construction de la structure des groupes d'administration en tenant compte de la topologie du réseau. La structure des groupes d'administration ne doit pas obligatoirement refléter exactement la topologie du réseau. Il suffit que quelques groupes d'administration correspondent à des parties du réseau mises en évidence. Les points de distribution peuvent être désignés automatiquement ou manuellement.

- Construction de la structure des groupes d'administration qui ne reflète pas la topologie du réseau. Dans ce cas, vous devez désactiver la désignation automatique des points de distribution et désigner dans chaque partie du réseau mise en évidence un ou plusieurs appareils en tant que points de distribution sur le groupe d'administration racine, par exemple, sur le groupe **Appareils administrés**. Tous les points de distribution se trouvent au même niveau et possèdent la même zone d'action, à savoir tous les appareils du réseau de l'entreprise. Chaque Agent d'administration se connecte dans ce cas au point de distribution qui possède l'itinéraire le plus court. L'utilitaire tracert permet de définir l'itinéraire d'accès au point de distribution.

Configuration typique des points de distribution : plusieurs petits bureaux isolés

Cette configuration typique correspond à plusieurs petits bureaux distants, potentiellement connectés au siège principal via Internet. Chacun de ces bureaux distants se trouve au-delà du NAT. Autrement dit, la connexion d'un bureau distant à un autre est impossible. Ils sont isolés.

La configuration doit absolument se refléter dans la structure des groupes d'administration : pour chacun des bureaux distants. il faut créer un groupe d'administration distinct (les groupes **Bureau 1**, **Bureau 2** sur l'illustration ci-après).

Bureaux distants affichés dans la structure des groupes d'administration

Sur chaque groupe d'administration correspondant à un bureau, il faut désigner un ou plusieurs points de distribution. Les points de distribution doivent être des appareils du bureau distant dotés d'espace suffisant sur le disque. Ainsi, les appareils qui se trouvent par exemple dans le groupe **Bureau 1** vont contacter les points de distribution assignés au groupe d'administration **Bureau 1**.

Si certains utilisateurs se déplacent d'un bureau à l'autre avec des ordinateurs portables, il faut sélectionner dans chaque bureau distant, en plus des points de distribution cités ci-dessus, deux ou plusieurs appareils et les assigner comme points de distribution pour le groupe d'administration de niveau supérieur (le groupe **Groupe racine pour les bureaux** dans l'illustration ci-dessus).

Exemple : Par exemple, voici un ordinateur portable qui se trouve dans le groupe d'administration **Bureau 1**, mais qui est déplacé physiquement dans le bureau qui correspond au groupe **Bureau 2**. Après le déplacement, l'Agent d'administration sur l'ordinateur portable tente de contacter les points de distribution assignés au groupe **Bureau 1**, mais ceux-ci ne sont pas accessibles. Alors l'Agent d'administration commence à contacter les points de distribution désignés pour le groupe **Groupe racine pour les bureaux**. Étant donné que les bureaux distants sont isolés les uns des autres, seules les requêtes d'accès aux points de distribution assignés au groupe d'administration **Groupe racine pour les bureaux** aboutissent lorsque l'Agent d'administration tente d'accéder aux points de distribution dans le groupe **Bureau 2**. Autrement dit, l'ordinateur portable demeure dans le groupe d'administration qui correspond à son bureau d'origine, mais il utilise malgré tout le point de distribution du bureau où il se trouve physiquement à l'heure actuelle.

À propos des points de distribution

Vous pouvez affecter un appareil administré en tant que point de distribution manuellement ou automatiquement.

Si vous affectez manuellement un appareil administré en tant que point de distribution, vous pouvez sélectionner n'importe quel appareil de votre réseau.

Si vous attribuez automatiquement des points de distribution, Kaspersky Security Center ne peut sélectionner que l'appareil administré qui remplit les conditions suivantes :

- L'appareil dispose d'au moins 50 Go d'espace disque libre.
- L'appareil administré est directement connecté à Kaspersky Security Center (et non via la passerelle).
- L'appareil administré n'est pas un ordinateur portable.

> Si votre réseau ne possède pas d'appareils répondant aux conditions spécifiées, Kaspersky Security Center n'attribuera automatiquement aucun appareil en tant que point de distribution.

Assignation automatique des points de distribution

Nous vous recommandons d'assigner les points de distribution automatiquement. Dans ce cas, Kaspersky Security Center choisira lui-même les appareils à désigner comme points de distribution.

Pour assigner automatiquement des points de distribution :

1. Dans le menu principal, cliquez sur l'icône des paramètres ( ) en regard du nom du Serveur d'administration requis.

   La fenêtre des propriétés du Serveur d'administration s'ouvre.

2. Sous l'onglet **Général**, sélectionnez la section **Points de distribution**.

3. Sélectionnez l'option **Attribuer automatiquement les points de distribution**.

   > Si l'assignation automatique d'appareils comme points de distribution est activée, vous ne pouvez pas configurer les points de distribution manuellement ni modifier la liste des points de distribution.

4. Cliquez sur le bouton **Enregistrer**.

Le Serveur d'administration assigne et configure automatiquement les points de distribution.

Assignation manuelle des points de distribution

Kaspersky Security Center permet de désigner manuellement des appareils comme points de distribution.

Nous vous recommandons d'assigner les points de distribution automatiquement. Dans ce cas, Kaspersky Security Center choisira lui-même les appareils à désigner comme points de distribution. Cependant, si vous souhaitez, pour quelque raison que ce soit, refuser la désignation automatique des points de distribution (si vous souhaitez, par exemple, utiliser des serveurs prévus à cet effet), vous pouvez désigner les points de distribution manuellement, après avoir évalué leur quantité et leur configuration.

Les appareils fonctionnant comme points de distribution doivent être protégés, y compris physiquement contre tout accès non autorisé.

Pour désigner manuellement un appareil comme point de distribution :

1. Dans le menu principal, cliquez sur l'icône des paramètres ( ) en regard du nom du Serveur d'administration requis.

   La fenêtre des propriétés du Serveur d'administration s'ouvre.

2. Sous l'onglet **Général**, sélectionnez la section **Points de distribution**.

3. Sélectionnez l'option **Attribuer manuellement les points de distribution**.

4. Cliquez sur le bouton **Désigner**.

5. Sélectionner l'appareil dont vous voulez faire un point de distribution.

   Lors de la sélection de l'appareil, prenez en compte les particularités de fonctionnement des points de distribution et les exigences pour l'appareil qui joue le rôle de point de distribution.

6. Sélectionnez le groupe d'administration que vous voulez inclure dans le champ du point de distribution sélectionné.

7. Cliquez sur le bouton **OK**.

   Le point de distribution que vous avez ajouté sera affiché dans la liste des points de distribution, dans la section **Points de distribution**.

8. Cliquez sur le nouveau point de distribution dans la liste pour ouvrir la fenêtre de ses propriétés.

9. Configurez le point de distribution dans la fenêtre des propriétés :

- Dans la section **Général**, indiquez les paramètres d'interaction entre le point de distribution et les appareils clients :

  - **Port SSL**

    Le numéro du port SSL utilisé pour la connexion sécurisée des appareils clients au point de distribution via le protocole SSL.

    Le numéro de port est de 13000 par défaut.

  - **Utiliser la multidiffusion**

    Si cette option est activée, la multidiffusion pour la diffusion automatique des paquets d'installation sur les appareils clients du groupe sera utilisée.

    La diffusion IP multidiffusion réduit le temps nécessaire à l'installation d'une application à partir d'un paquet d'installation sur un groupe d'appareils clients, mais prolonge le temps d'installation lorsque vous installez une application sur un seul appareil client.

  - **Adresse IP de multidiffusion**

    Adresse IP sur laquelle est exécuté l'envoi diffusion multiadresse. L'adresse IP peut être indiquée dans l'intervalle 224.0.0.0 – 239.255.255.255

    Par défaut, Kaspersky Security Center attribue automatiquement une adresse IP de multidiffusion unique dans la plage donnée.

  - **Numéro du port IP de multidiffusion**

    Numéro du port de diffusion multiadresse.

    Le numéro de port est de 15001 par défaut. Dans le cas où le point de distribution tourne sur un appareil sur lequel est également installé un Serveur d'administration, le numéro de port par défaut pour la connexion SSL est 13001.

  - **Adresse du point de distribution pour les appareils distants**

    Adresse IPv4 via laquelle les appareils distants se connectent au point de distribution.

  - **Déployer les mises à jour**

Les mises à jour sont distribuées aux appareils administrés à partir des sources suivantes :

- Ce point de distribution si cette option est activée.
- Autres points de distribution, Serveur d'administration ou serveurs de mise à jour Kaspersky si cette option est désactivée.

Si vous utilisez des points de distribution pour déployer des mises à jour, vous pouvez économiser du trafic parce que vous réduisez le nombre de téléchargements. Vous pouvez aussi alléger la charge sur le Serveur d'administration et répartir la charge entre les points de distribution. Vous pouvez calculer le nombre de points de distribution de votre réseau pour optimiser le trafic et la charge.

Si vous désactivez cette option, le nombre de téléchargements de mises à jour et de charges sur le Serveur d'administration peut augmenter. Cette option est activée par défaut.

- **Déployer les paquets d'installation**

Les paquets d'installation sont distribuées aux appareils administrés à partir des sources suivantes :

- Ce point de distribution si cette option est activée.
- Autres points de distribution, Serveur d'administration ou serveurs de mise à jour Kaspersky si cette option est désactivée.

Si vous utilisez des points de distribution pour déployer des paquets d'installation, vous pouvez économiser du trafic parce que vous réduisez le nombre de téléchargements. Vous pouvez aussi alléger la charge sur le Serveur d'administration et répartir la charge entre les points de distribution. Vous pouvez calculer le nombre de points de distribution de votre réseau pour optimiser le trafic et la charge.

Si vous désactivez cette option, le nombre de téléchargements de paquets d'installation et de charges sur le Serveur d'administration peut augmenter. Cette option est activée par défaut.

- **Exécuter le serveur push**

Dans Kaspersky Security Center, un point de distribution peut servir de serveur push pour les appareils administrés via le protocole mobile et pour les appareils administrés par l'Agent d'administration. Par exemple, un serveur push doit être activé si vous souhaitez pouvoir forcer la synchronisation des appareils KasperskyOS avec le Serveur d'administration. Un serveur push a la même portée d'appareils administrés que le point de distribution sur lequel le serveur push est activé. Si plusieurs points de distribution sont affectés au même groupe d'administration, vous pouvez activer le serveur push sur chacun des points de distribution. Dans ce cas, le Serveur d'administration équilibre la charge entre les points de distribution.

- **Port du serveur push**

Le numéro de port pour le serveur push. Vous pouvez préciser le numéro de tout port inoccupé.

- Dans la section **Zone d'action**, indiquez la zone dans laquelle le point de distribution va distribuer des mises à jour (groupes d'administration et/ou emplacement réseau).

Seuls les appareils administrés sous Windows peuvent définir l'emplacement réseau. La définition de l'emplacement réseau est inaccessible pour les appareils administrés sous d'autres systèmes d'exploitation.

- Si le point de distribution fonctionne sur un ordinateur autre que le Serveur d'administration, dans la section **Source de mises à jour**, vous pouvez sélectionner une source de mises à jour pour le point de distribution :

  - **Source des mises à jour**

    Sélectionnez une source de mises à jour pour le point de distribution :

    - Pour que le point de distribution récupère les mises à jour du Serveur d'administration, sélectionnez **Récupérer depuis le Serveur d'administration**.
    - Pour autoriser le point de distribution à recevoir les mises à jour à l'aide d'une tâche, sélectionnez **Utiliser la tâche d'obtention des mises à jour** de téléchargement des mises à jour, puis spécifiez une tâche *Télécharger les mises à jour dans les référentiels des points de distribution* :
      - Si une telle tâche existe déjà sur l'appareil, sélectionnez-la dans la liste.
      - Si aucune tâche de ce type n'existe encore sur l'appareil, cliquez sur le lien **Créer la tâche** pour créer une tâche. Ceci permet de lancer l'Assistant de création d'une tâche. Suivez les instructions de l'assistant.

  - **Télécharger les fichiers diff**

    Cette option active la fonction de téléchargement des fichiers diff.

    Cette option est activée par défaut.

- Si vos points de distribution utilisent un serveur proxy pour se connecter à Internet, vous pouvez renseigner les paramètres suivants dans la sous-section **Paramètres de connexion Internet** :

  - **Utiliser un serveur proxy**

    Si la case est cochée, le champ de saisie permet de configurer la connexion au serveur proxy.

    Celle-ci est décochée par défaut.

  - **Adresse du serveur proxy**

    Adresse du serveur proxy.

  - **Numéro de port**

    Numéro du port utilisé pour la connexion.

  - **Ne pas utiliser le serveur proxy pour les adresses locales**

    Si cette option est activée, le serveur proxy ne sera pas utilisé lors de la connexion aux appareils sur le réseau local.

    Cette option est Inactif par défaut.

  - **Authentification du serveur proxy**

Si la case est cochée, les champs de saisie permettent d'indiquer les identifiants pour l'authentification sur le serveur proxy.

Celle-ci est décochée par défaut.

- Nom d'utilisateur

  Le compte utilisateur au nom duquel la connexion au serveur proxy sera effectuée.

- Mot de passe

  Mot de passe du compte utilisateur au nom duquel la tâche sera lancée.

- Dans la section **Proxy KSN**, vous pouvez configurer l'application afin qu'elle utilise le point de distribution pour transmettre les requêtes KSN depuis les appareils administrés :

  - Activer le proxy KSN du côté du point de distribution

    Le service KSN proxy est exécuté sur l'appareil qui est utilisé en tant que points de distribution. Utilisez cette fonction pour rediffuser et optimiser le trafic sur le réseau.

    Le point de distribution envoie les statistiques KSN, lesquelles sont répertoriées dans la Déclaration de Kaspersky Security Network, à Kaspersky. Par défaut, la Déclaration KSN se trouve dans %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\ksneula.

    Cette option est Inactif par défaut. L'activation de cette option prend effet uniquement si les options **Utiliser le Serveur d'administration comme serveur proxy** et **J'accepte les termes du Kaspersky Security Network** sont activées dans la fenêtre Propriétés du Serveur d'administration.

    Vous pouvez affecter un nœud d'un cluster actif-passif à un point de distribution et activer le serveur proxy KSN sur ce nœud.

  - Transférer les requêtes KSN au Serveur d'administration

    Le point de distribution transfère les requêtes KSN depuis les appareils administrés vers le Serveur d'administration.

    Cette option est activée par défaut.

  - Accéder à KSN Cloud/KPSN directement via Internet

    Le point de distribution transfère les requêtes KSN depuis les appareils administrés vers le Cloud KSN ou KPSN. Les requêtes KSN générées sur le point de distribution lui-même sont également envoyées directement à KSN Cloud ou à KPSN.

    Les points de distribution sur lesquels l'Agent d'administration version 11 (ou antérieure) est installé ne peuvent pas accéder directement à KPSN. Si vous souhaitez reconfigurer les points de distribution pour envoyer des demandes KSN à KPSN, activez l'option **&Transférer les demandes KSN au Serveur d'administration** pour chaque point de distribution.

    Les points de distribution sur lesquels l'Agent d'administration version 12 (ou version ultérieure) est installé peuvent accéder directement à KPSN.

  - Ignorer les paramètres du serveur proxy lors de la connexion à KPSN

Activez cette option, si les paramètres du serveur proxy sont configurés dans les propriétés du point de distribution ou dans la stratégie de l'Agent d'administration, mais que votre architecture réseau exige que vous utilisiez directement un KPSN. Dans le cas contraire, les requêtes des applications administrées ne peuvent pas atteindre le KPSN.

Cette option est disponible si vous sélectionnez l'option **Accéder à KSN Cloud/KPSN directement via Internet**.

- **Port**

  Le numéro du port TCP que les appareils administrés utilisent pour se connecter au serveur proxy KSN. Le numéro du port par défaut est 13111.

- **Utiliser le port UDP**

  Si vous avez besoin que les appareils administrés se connectent au serveur proxy KSN via un port UDP, activez l'option **Utiliser le port UDP** et indiquez le Numéro de port UDP. Cette option est activée par défaut.

- **Port UDP**

  Le numéro du port UDP que les appareils administrés utilisent pour se connecter au serveur proxy KSN. Par défaut, la connexion au serveur proxy KSN est exécutée via le port UDP 15111.

- Si le point de distribution fonctionne sur une machine autre que le Serveur d'administration, dans la section **Passerelle de connexion**, vous pouvez configurer le point de distribution pour qu'il agisse comme une passerelle pour la connexion entre les instances de l'Agent d'administration et le Serveur d'administration :

  - **Passerelle de connexion**

    Si une connexion directe entre le Serveur d'administration et les Agents d'administration ne peut pas être établie en raison de l'organisation de votre réseau, vous pouvez utiliser le point de distribution comme passerelle de connexion entre le Serveur d'administration et les Agents d'administration.

    Activez cette option si vous avez besoin que le point de distribution agisse comme une passerelle de connexion entre les Agents d'administration et le Serveur d'administration. Cette option est Inactif par défaut.

  - **Établir la connexion avec la passerelle depuis le Serveur d'administration (si la passerelle est placée dans la zone démilitarisée)**

    Si le Serveur d'administration se trouve en dehors de la zone démilitarisée (DMZ), sur le réseau local, les Agents d'administration installés sur les appareils distants ne peuvent pas se connecter au Serveur d'administration. Vous pouvez utiliser un point de distribution comme passerelle de connexion avec une connectivité inversée (le Serveur d'administration établit une connexion au point de distribution).

    Activez cette option si vous devez connecter le Serveur d'administration à la passerelle de connexion dans la DMZ.

  - **Ouvrir le port local pour Kaspersky Security Center Web Console**

Activez cette option si vous avez besoin de la passerelle de connexion en DMZ pour ouvrir un port pour Web Console qui se trouve en DMZ ou sur Internet. Indiquez le numéro de port qui sera utilisé pour la connexion de Web Console au point de distribution. Le numéro de port par défaut est 13299.

Cette option est disponible si vous activez l'option **Établir la connexion avec la passerelle depuis le Serveur d'administration (si la passerelle est placée dans la zone démilitarisée)**.

Lors de la connexion des appareils mobiles au Serveur d'administration via le point de distribution agissant comme passerelle de connexion, vous pouvez activer les options suivantes :

- **Ouvrir le port pour les appareils mobiles (authentification SSL du Serveur d'administration uniquement)**

  Activez cette option si vous avez besoin que la passerelle de connexion ouvre un port pour les appareils mobiles et indiquez le numéro de port que les appareils mobiles utiliseront pour la connexion au point de distribution. Le numéro de port par défaut est 13292. L'appareil mobile vérifie le certificat du Serveur d'administration. Lors de l'établissement de la connexion, seul le Serveur d'administration est authentifié.

- **Ouvrir le port pour les appareils mobiles (authentification SSL bidirectionnelle)**

  Activez cette option si vous avez besoin d'une passerelle de connexion pour ouvrir un port qui sera utilisé pour l'authentification bidirectionnelle du Serveur d'administration et des appareils mobiles. L'appareil mobile vérifiera le certificat du Serveur d'administration, et le Serveur d'administration vérifiera le certificat de l'appareil mobile. Définissez les paramètres suivants :

  - Numéro de port que les appareils mobiles utiliseront pour se connecter au point de distribution. Le numéro de port par défaut est 13293.
  - Noms de domaine DNS de la passerelle de connexion qui seront utilisés par les appareils mobiles. Séparez les noms de domaine par des virgules. Les noms de domaine indiqués seront inclus dans le certificat du point de distribution. Si les noms de domaine utilisés par les appareils mobiles ne correspondent pas au nom usuel dans le certificat du point de distribution, les appareils mobiles ne se connectent pas au point de distribution.

    Le nom de domaine DNS par défaut est le nom de domaine complet de la passerelle de connexion.

Dans les deux cas, la vérification des certificats est effectuée lors de l'établissement d'une session TLS sur le point de distribution uniquement. Les certificats ne sont pas transmis pour être vérifiés par le Serveur d'administration. Après l'établissement d'une session TLS avec l'appareil mobile, le point de distribution utilise le certificat du Serveur d'administration pour créer un tunnel de synchronisation entre l'appareil mobile et le Serveur d'administration. Si vous ouvrez le port pour l'authentification SSL bidirectionnelle, le seul moyen de distribuer le certificat d'appareil mobile est d'utiliser un paquet d'installation.

- Configurez les paramètres de sondage par le point de distribution des domaines Windows, Active Directory et des plages IP :

  - **Domaines Windows**

    Vous pouvez autoriser la recherche d'appareils pour les domaines Windows et programmer la recherche.

  - **Contrôleurs de domaine**

Vous pouvez autoriser le sondage du réseau pour Active Directory et programmer le sondage.

Si vous utilisez un point de distribution Windows, vous pouvez sélectionner une des options suivantes :

- **Sonder le domaine actuel Active Directory**.
- **Sonder la forêt de domaines Active Directory**.
- **Sonder les domaines indiqués Active Directory**. Si vous choisissez cette option, ajoutez un ou plusieurs domaines Active Directory à la liste.

Si vous utilisez un point de distribution Linux avec l'Agent d'administration version 15 installé, vous ne pouvez interroger que les domaines Active Directory dont vous spécifiez l'adresse et les informations d'identification de l'utilisateur. Les sondages du domaine Active Directory actuel et de la forêt de domaines Active Directory ne sont pas disponibles.

Vous pouvez activer la découverte d'appareils pour les contrôleurs de domaine.

Si vous sélectionnez l'option **Activer le sondage du contrôleur de domaine**, vous pouvez sélectionner des contrôleurs de domaine pour le sondage et également spécifier le calendrier de sondage pour eux.

Si vous utilisez un point de distribution Linux, dans la section **Sonder les domaines indiqués**, cliquez sur **Ajouter**, puis spécifiez l'adresse et les informations d'identification de l'utilisateur du contrôleur de domaine.

Si vous utilisez un point de distribution Windows, vous pouvez sélectionner une des options suivantes :

- **Sonder le domaine actuel**
- **Sonder toute la forêt de domaines**
- **Sonder les domaines indiqués**

- Plages IP

Vous pouvez activer la recherche d'appareils pour les plages IPv4 et les réseaux IPv6.

Si vous activez l'option **Autoriser le sondage de la plage**, vous pouvez ajouter des plages d'analyse et définir les programmations pour celles-ci. Vous pouvez ajouter des plages IP à la liste des plages analysées.

Si vous activez l'option **Utiliser Zeroconf pour sonder les réseaux IPv6**, le point de distribution sonde automatiquement le réseau IPv6 en utilisant la mise en réseau sans configuration (également appelée *Zeroconf*). Dans ce cas, les plages IP spécifiées sont ignorées car le point de distribution sonde l'ensemble du réseau. L'option **Utiliser Zeroconf pour sonder les réseaux IPv6** est disponible si le point de distribution fonctionne sous Linux. Pour utiliser le sondage Zeroconf IPv6, vous devez installer l'utilitaire avahi-browse sur le point de distribution.

- Dans la section **Avancé**, indiquez le dossier que le point de distribution doit utiliser pour l'enregistrement des données diffusées :
  - Utiliser le dossier par défaut

Lors du choix de cette option, le dossier avec l'Agent d'administration installé sur le point de distribution sera utilisé pour enregistrer les données.

- **Utiliser le dossier spécifié**

  Lors du choix de cette option, il est possible d'indiquer dans le champ situé ci-dessous le chemin d'accès au dossier. Le dossier peut être local sur le point de distribution ou distant, sur n'importe lequel des appareils faisant partie du réseau de l'entreprise.

  Le compte utilisateur, sous lequel l'Agent d'administration est lancé sur le point de distribution, doit posséder l'accès au dossier indiqué pour lecture et écriture.

10. Cliquez sur le bouton **OK**.

Les appareils sélectionnés sont comme des points de distribution.

Modifier la liste des points de distribution pour un groupe d'administration

Vous pouvez voir la liste des points de distribution assignés à un groupe d'administration spécifique et y ajouter ou en éliminer des points de distribution.

Pour voir et modifier la liste des points de distribution assignés à un groupe d'administration :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Appareils administrés**.
2. Dans le champ **Chemin d'accès actif** au-dessus de la liste des appareils administrés, cliquez sur le lien vers le chemin.
3. Dans le volet de gauche qui s'ouvre, sélectionnez un groupe d'administration pour lequel vous souhaitez afficher les points de distribution attribués.

   Cela active l'option de menu **Points de distribution**.
4. Dans le menu principal, accédez à **Ressources (Appareils)** → **Points de distribution**.
5. Pour ajouter de nouveaux points de distribution pour le groupe d'administration, cliquez sur le bouton **Désigner** au-dessus de la liste des appareils administrés et sélectionnez les appareils dans le volet qui s'ouvre.
6. Pour supprimer les points de distribution attribués, sélectionnez les appareils dans la liste et cliquez sur le bouton **Désaffecter**.

Selon vos modifications, des nouveaux points de distribution sont ajoutés à la liste ou des points de distribution existants sont supprimés de la liste.

Synchronisation forcée

Bien que Kaspersky Security Center synchronise automatiquement l'état, les paramètres, les tâches et les politiques pour les appareils administrés, dans certains cas, vous voudrez peut-être exécuter la synchronisation pour un appareil spécifique de manière forcée. Vous pouvez exécuter une synchronisation forcée pour les appareils suivants :

- Appareils sur lesquels l'Agent d'administration est installé
- Appareils fonctionnant sous KasperskyOS

  Avant d'exécuter la synchronisation forcée pour un appareil KasperskyOS, assurez-vous que l'appareil est inclus dans la portée d'un point de distribution et qu'un serveur push est activé sur le point de distribution.
- Appareils iOS
- Appareils Android

  Avant d'exécuter la synchronisation forcée pour un appareil Android, vous devez configurer Firebase Cloud Messaging.

Synchronisation d'un seul appareil

Pour forcer la synchronisation entre le Serveur d'administration et l'appareil administré, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Appareils administrés**.
2. Cliquez sur le nom de l'appareil que vous souhaitez synchroniser avec le Serveur d'administration.

   La fenêtre des propriétés s'ouvre avec la section **Général** sélectionnée.
3. Cliquez sur le bouton **Forcer la synchronisation**.

L'application synchronise l'appareil administré avec le Serveur d'administration.

Synchronisation de plusieurs appareils

Pour forcer la synchronisation entre le Serveur d'administration et plusieurs appareils administrés, procédez comme suit :

1. Ouvrez la liste des appareils d'un groupe d'administration ou une sélection d'appareils :
   - Dans le menu principal, sélectionnez **Ressources (Appareils)** → **Appareils administrés**, cliquez sur le lien vers le chemin d'accès dans le champ **Chemin d'accès actif** au-dessus de la liste des appareils administrés, puis sélectionnez le groupe d'administration qui contient les appareils à synchroniser.
   - Exécutez une sélection d'appareils pour afficher la liste des appareils.
2. Cochez les cases en regard des appareils que vous souhaitez synchroniser avec le Serveur d'administration.

3. Au-dessus de la liste des appareils administrés, cliquez sur le bouton points de suspension (...), puis sur le bouton **Forcer la synchronisation**.

   L'application synchronise les appareils sélectionnés avec le Serveur d'administration.

4. Dans la liste des appareils, assurez-vous que l'heure de la dernière connexion au Serveur d'administration a changé à l'heure actuelle pour les appareils sélectionnés. Si l'heure n'a pas changé, mettez à jour le contenu de la page en cliquant sur le bouton **Actualiser**.

Les appareils sélectionnés sont synchronisés avec le Serveur d'administration.

Consultation de l'heure d'une remise de la stratégie

Après avoir modifié une stratégie pour une application de Kaspersky sur le Serveur d'administration, l'administrateur peut vérifier si la stratégie modifiée a été remise à un appareil administré défini. Une stratégie peut être remise lors d'une synchronisation normale ou forcée.

Pour voir la date et l'heure de remise d'une stratégie d'application sur un appareil administré, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Appareils administrés**.
2. Cliquez sur le nom de l'appareil que vous souhaitez synchroniser avec le Serveur d'administration.

   La fenêtre des propriétés s'ouvre avec la section **Général** sélectionnée.

3. Sélectionnez la l'onglet **Applications**.
4. Sélectionnez l'application pour laquelle vous souhaitez consulter la date de synchronisation des stratégies.

   La fenêtre de la stratégie de l'application s'ouvre avec la section **Général** sélectionnée, et affiche la date et l'heure de remise de la stratégie.

Activation d'un serveur push

Dans Kaspersky Security Center, un point de distribution peut servir de serveur push pour les appareils administrés via le protocole mobile et pour les appareils administrés par l'Agent d'administration. Par exemple, un serveur push doit être activé si vous souhaitez pouvoir forcer la synchronisation des appareils KasperskyOS avec le Serveur d'administration. Un serveur push a la même portée d'appareils administrés que le point de distribution sur lequel le serveur push est activé. Si plusieurs points de distribution sont affectés au même groupe d'administration, vous pouvez activer le serveur push sur chacun des points de distribution. Dans ce cas, le Serveur d'administration équilibre la charge entre les points de distribution.

Vous souhaiterez peut-être utiliser des points de distribution comme serveurs push pour vous assurer qu'il existe une connexion permanente entre un appareil administré et le Serveur d'administration. Une connexion permanente est nécessaire pour certaines opérations, telles que l'exécution et l'arrêt des tâches locales, la réception de statistiques pour une application administrée ou la création d'un tunnel. Si vous utilisez un point de distribution comme serveur push, vous n'avez pas besoin d'utiliser l'option **Maintenir la connexion au Serveur d'administration** option sur les appareils administrés ou envoyer des paquets au port UDP de l'Agent d'administration.

Un serveur push prend en charge jusqu'à 50 000 connexions simultanées.

Pour activer le serveur push sur un point de distribution :

1. Dans le menu principal, cliquez sur l'icône paramètres ( ) en face du nom du Serveur d'administration requis.
   La fenêtre des propriétés du Serveur d'administration s'ouvre.
2. Sous l'onglet **Général**, sélectionnez la section **Points de distribution**.
3. Cliquez sur le nom du point de distribution sur lequel vous souhaitez activer le serveur push.
   La fenêtre Propriétés du point de distribution s'affiche.
4. Dans la section **Général**, activez l'option **Exécuter le serveur push**.
5. Dans le champ **Port du serveur push**, saisissez le numéro de port. Vous pouvez préciser le numéro de tout port inoccupé.
6. Dans le champ **Adresse des hôtes distants**, indiquez l'adresse IP ou le nom de l'appareil du point de distribution.
7. Cliquez sur le bouton **OK**.

Le serveur push est activé sur le point de distribution sélectionné.

Gestion des applications tierces sur les appareils client

Cette section décrit les fonctions de Kaspersky Security Center associées à l'administration des applications tierces installées sur les appareils client.

Installation des mises à jour du logiciel tiers

Kaspersky Security Center permet d'administrer les mises à jour du logiciel tiers installé sur les appareils administrés et de corriger les vulnérabilités dans les applications de Microsoft et d'autres éditeurs du logiciel à l'aide de l'installation des mises à jour nécessaires.

Kaspersky Security Center recherche des mises à jour par la tâche *Recherche de vulnérabilités et de mises à jour requises*. Une fois cette tâche terminée, le Serveur d'administration reçoit la liste des vulnérabilités détectées et des mises à jour requises pour les logiciels tiers installés sur les appareils que vous avez spécifiés dans les propriétés de la tâche. Après la consultation des informations sur les mises à jour disponibles, vous pouvez exécuter l'installation des mises à jour sur les appareils.

La mise à jour de certaines applications Kaspersky Security Center s'effectue par la suppression de la version précédente de l'application et par l'installation d'une nouvelle version.

Une interaction utilisateur peut être requise lorsque vous mettez à jour une application tierce ou corrigez une vulnérabilité dans une application tierce sur un appareil administré. Par exemple, l'utilisateur peut être invité à fermer l'application tierce si elle est actuellement ouverte.

Pour des raisons de sécurité, toutes les mises à jour du logiciel tiers que vous installez à l'aide de la fonction de la gestion des vulnérabilités et des correctifs sont automatiquement analysées à la recherche d'applications malveillantes par les technologies de Kaspersky. Ces technologies sont utilisées pour la vérification automatique des fichiers et incluent la recherche de virus, l'analyse statique, l'analyse dynamique, l'analyse comportementale dans l'environnement sandbox et machine learning.

Les experts de Kaspersky n'effectuent pas d'analyse manuelle des mises à jour du logiciel tiers pouvant être installées par la fonction de la gestion des vulnérabilités et des correctifs. De plus, les experts de Kaspersky ne recherchent pas de vulnérabilités (connues ou inconnues) ou de fonctionnalités non documentées dans ces mises à jour, et n'effectuent pas d'autres types d'analyse des mises à jour que ceux indiqués dans le paragraphe ci-dessus.

Tâches pour l'installation des mises à jour de logiciels tiers

Lorsque les métadonnées des mises à jour de logiciels tiers sont téléchargées dans le stockage, vous pouvez installer les mises à jour sur les appareils clients en utilisant les tâches suivantes :

- La tâche *Installation des mises à jour requises et correction des vulnérabilités*

  La tâche *Installation des mises à jour requises et correction des vulnérabilités* est utilisée pour installer les mises à jour des applications de Microsoft, y compris les mises à jour fournies par le service Windows Update et les mises à jour des logiciels d'autres fournisseurs. Notez que cette tâche ne peut être créée que si vous disposez de la licence pour la fonctionnalité Gestion des vulnérabilités et des correctifs.

  Lorsque cette tâche est terminée, les mises à jour sont installées automatiquement sur les appareils administrés. Lorsque les métadonnées des nouvelles mises à jour sont téléchargées dans le stockage du Serveur d'administration, Kaspersky Security Center vérifie si les mises à jour répondent aux critères spécifiés dans les règles de mise à jour. Toutes les nouvelles mises à jour qui répondent aux critères seront téléchargées et installées automatiquement lors de la prochaine exécution de la tâche.

- La tâche *Installation des mises à jour Windows Update*

  La tâche *Installation des mises à jour Windows Update* ne nécessite pas de licence, mais elle peut être utilisée pour installer uniquement les mises à jour de Windows Update.

  Lorsque cette tâche est terminée, seules les mises à jour spécifiées dans les propriétés de la tâche sont installées. À l'avenir, si vous souhaitez installer les nouvelles mises à jour téléchargées dans le stockage du Serveur d'administration, vous devez ajouter les mises à jour requises à la liste des mises à jour dans la tâche existante ou créer une nouvelle tâche Installation des mises à jour Windows Update.

Utilisation du Serveur d'administration comme serveur WSUS

Les informations sur les mises à jour Microsoft Windows disponibles sont transmises en provenance du centre des mises à jour Windows. Le Serveur d'administration peut être utilisé comme serveur Windows Update (WSUS). Pour utiliser le Serveur d'administration comme serveur WSUS, vous devez créer la tâche Synchronisation des mises à jour Windows Update et sélectionner l'option **Utiliser le Serveur d'administration comme serveur WSUS** dans la stratégie de l'Agent d'administration. Après la configuration de la synchronisation des données avec Windows Update, le Serveur d'administration, avec une fréquence définie, fournit les mises à jour aux services Windows Update sur les appareils en mode centralisé.

Scénario : mise à jour des logiciels tiers

Cette section fournit un scénario pour la mise à jour des logiciels tiers installés sur les appareils client. Les logiciels tiers comprennent des applications de Microsoft et d'autres fournisseurs de logiciels. Les mises à jour des applications de Microsoft sont fournies par le service Windows Update.

Prérequis

Le Serveur d'administration doit être connecté à Internet pour installer les mises à jour de logiciels tiers autres que les logiciels Microsoft.

Par défaut, une connexion Internet n'est pas requise pour que le Serveur d'administration installe les mises à jour logicielles Microsoft sur les appareils administrés. Les appareils administrés peuvent ainsi télécharger les mises à jour logicielles Microsoft directement à partir des serveurs Microsoft Update ou à partir de Windows Server lorsque Microsoft Windows Server Update Services (WSUS) est déployé sur le réseau de votre organisation. Le Serveur d'administration doit être connecté à Internet lorsque vous utilisez le Serveur d'administration comme serveur WSUS.

Étapes

La mise à jour du logiciel tiers s'effectue fait par étapes :

1. **Recherche des mises à jour requises**

   Pour rechercher les mises à jour logicielles tierces requises pour les appareils administrés, exécutez la tâche *Recherche de vulnérabilités et de mises à jour requises*. Une fois cette tâche terminée, Kaspersky Security Center reçoit la liste des vulnérabilités détectées et des mises à jour requises pour les logiciels tiers installés sur les appareils que vous avez spécifiés dans les propriétés de la tâche.

   La tâche *Recherche de vulnérabilités et de mises à jour requises* est créée automatiquement par l'Assistant de configuration initiale du Serveur d'administration. Si vous n'avez pas exécuté l'assistant, créez la tâche ou exécutez l'assistant de démarrage rapide de l'application maintenant.

   Instructions pour :

   - Console d'administration : Recherche de vulnérabilités dans les applications, Planification de la tâche Recherche de vulnérabilités et des mises à jour requises
   - Kaspersky Security Center Web Console : création d'une tâche Recherche de vulnérabilités et de mises à jour requises, paramètres de Recherche de vulnérabilités et de mises à jour requises

2. **Analyser la liste des mises à jour trouvées**

   Consultez la liste des **Mises à jour du logiciel** et décidez des mises à jour que vous souhaitez installer. Pour consulter les informations détaillées de chaque mise à jour, cliquez sur le nom de la mise à jour dans la liste. Pour chaque mise à jour de la liste, vous pouvez également consulter les statistiques de l'installation de la mise à jour sur les appareils client.

   Instructions pour :

   - Console d'administration : Affichage des informations sur les mises à jour disponibles
   - Kaspersky Security Center Web Console : Affichage des informations sur les mises à jour logicielles tierces disponibles

3. **Configuration de l'installation des mises à jour**

   Une fois que Kaspersky Security Center a reçu la liste des mises à jour logicielles tierces, vous pouvez les installer sur les appareils client à l'aide de la tâche *Installation des mises à jour requises et correction des vulnérabilités* ou de la tâche *Installation des mises à jour Windows Update*. Créez une de ces tâches. Vous pouvez créer ces tâches sous l'onglet **Tâches** ou à l'aide de la liste **Mises à jour du logiciel**.

   La tâche *Installation des mises à jour requises et correction des vulnérabilités* est utilisée pour installer les mises à jour des applications de Microsoft, y compris les mises à jour fournies par le service Windows Update et les mises à jour des logiciels d'autres fournisseurs. Notez que cette tâche ne peut être créée que si vous disposez de la licence pour la fonctionnalité Gestion des vulnérabilités et des correctifs.

La tâche *Installation des mises à jour Windows Update* ne nécessite pas de licence, mais elle peut être utilisée pour installer uniquement les mises à jour de Windows Update.

Pour installer certaines mises à jour logicielles, vous devez accepter le Contrat de licence utilisateur final (CLUF) du logiciel en cours d'installation. Si vous refusez le CLUF, la mise à jour logicielle ne sera pas installée.

Vous pouvez lancer une tâche d'installation de mise à jour selon la planification. Lorsque vous définissez la planification de la tâche, assurez-vous que la tâche d'installation de la mise à jour est lancée une fois que la tâche *Recherche de vulnérabilités et de mises à jour requises* est terminée.

Instructions pour :

- Console d'administration : Correction des vulnérabilités dans les applications, Affichage des informations sur les mises à jour disponibles
- Kaspersky Security Center Web Console : Création de la tâche Installation des mises à jour requises et correction des vulnérabilités, Création de la tâche Installation des mises à jour Windows Update, Affichage des informations sur les mises à jour logicielles tierces disponibles

4. **Planification des tâches**

Pour vous assurer que la liste des mises à jour est toujours d'actualité, planifiez la tâche *Recherche de vulnérabilités et de mises à jour requises* pour exécuter automatiquement la tâche de temps à autre. Par défaut, la tâche *Recherche de vulnérabilités et de mises à jour requises* est configurée pour démarrer manuellement.

Si vous avez créé la tâche *Installation des mises à jour requises et correction des vulnérabilités*, vous pouvez la planifier pour qu'elle soit exécutée à la même fréquence que la tâche *Recherche de vulnérabilités et de mises à jour requises* ou à une fréquence moindre. Lors de la planification de la tâche *Installation des mises à jour Windows Update*, notez qu'avant de démarrer cette tâche, vous devez définir la liste des mises à jour à chaque fois.

Lors de la planification des tâches, assurez-vous qu'une tâche d'installation de la mise à jour est lancée une fois que la tâche *Recherche de vulnérabilités et de mises à jour requises* est terminée.

5. **Approbation et refus des mises à jour logicielles (facultatif)**

Si vous avez créé la tâche Installation des mises à jour requises et correction des vulnérabilités, vous pouvez spécifier des règles pour l'installation des mises à jour dans les propriétés de la tâche. Si vous avez créé la tâche Installation des mises à jour Windows Update, ignorez cette étape.

Pour chaque règle, vous pouvez définir les mises à jour à installer en fonction de l'état de la mise à jour : *Non défini*, *Approuvé* ou *Rejeté*. Par exemple, vous pouvez créer une tâche spécifique pour les serveurs et définir une règle pour cette tâche afin de n'autoriser l'installation que des mises à jour de Windows Update et uniquement celles qui disposent de l'état *Approuvé*. Ensuite, vous définissez manuellement l'état *Approuvé* pour les mises à jour que vous souhaitez installer. Dans ce cas, les mises à jour Windows Update qui disposent de l'état *Non défini* ou *Rejeté* ne seront pas installées sur les serveurs que vous avez spécifiés dans la tâche.

L'utilisation de l'état *Approuvé* pour gérer l'installation des mises à jour est efficace pour un petit nombre de mises à jour. Pour installer plusieurs mises à jour, utilisez les règles que vous pouvez configurer dans la tâche *Installation des mises à jour requises et correction des vulnérabilités*. Nous vous recommandons de définir l'état *Approuvé* uniquement pour les mises à jour particulières qui ne répondent pas aux critères spécifiés dans les règles. Lorsque vous approuvez manuellement une grande quantité de mises à jour, les performances du Serveur d'administration diminuent, ce qui peut entraîner une surcharge du Serveur d'administration.

Par défaut, les mises à jour logicielles téléchargées sont à l'état *Non défini*. Vous pouvez modifier l'état en *Approuvé* ou *Rejeté* dans la liste **Mises à jour du logiciel** (**Opérations** → **Gestion des correctifs** → **Mises à jour du logiciel**).

Instructions pour :

- Console d'administration : Approbation et refus des mises à jour logicielles
- Kaspersky Security Center Web Console : Approbation et refus des mises à jour logicielles tierces

6. **Configuration du Serveur d'administration pour qu'il fonctionne comme serveur Windows Server Update Services (WSUS) (facultatif)**

   Par défaut, les mises à jour Windows Update sont téléchargées sur les appareils administrés à partir des serveurs Microsoft. Vous pouvez modifier ce paramètre pour utiliser le Serveur d'administration comme serveur WSUS. Dans ce cas, le Serveur d'administration synchronise les données de mise à jour avec Windows Update à la fréquence indiquée et fournit des mises à jour en mode centralisé à Windows Update sur les appareils en réseau.

   Pour utiliser le Serveur d'administration comme serveur WSUS, créez la tâche Synchronisation des mises à jour Windows Update et cochez la case **Utiliser le Serveur d'administration comme serveur WSUS** dans la stratégie de l'Agent d'administration.

   Instructions pour :

   - Console d'administration : Synchronisation des mises à jour Windows Update avec le Serveur d'administration, Configuration des mises à jour Windows dans une stratégie de l'Agent d'administration
   - Kaspersky Security Center Web Console : Création de la tâche Synchronisation des mises à jour Windows Update

7. **Exécution d'une tâche d'installation des mises à jour**

   Démarrez la tâche *Installation des mises à jour requises et correction des vulnérabilités* ou la tâche *Installation des mises à jour Windows Update*. Lorsque vous démarrez ces tâches, les mises à jour sont téléchargées et installées sur les appareils administrés. Une fois la tâche terminée, assurez-vous qu'elle possède le statut *Terminée* dans la liste des tâches.

8. **Création du rapport des résultats de l'installation des mises à jour de logiciels tiers (facultatif)**

   Pour consulter les statistiques détaillées concernant l'installation des mises à jour, créez le **Rapport sur les résultats de l'installation des mises à jour du logiciel tiers**.

   Instructions pour :

   - Console d'administration : création et affichage d'un rapport
   - Kaspersky Security Center Web Console : génération et affichage d'un rapport

Résultats

Si vous avez créé et configuré la tâche *Installation des mises à jour requises et correction des vulnérabilités*, les mises à jour sont installées automatiquement sur les appareils administrés. Lorsque de nouvelles mises à jour sont téléchargées dans le stockage du Serveur d'administration, Kaspersky Security Center vérifie si elles répondent aux critères spécifiés dans les règles de mise à jour. Toutes les nouvelles mises à jour qui répondent aux critères seront installées automatiquement lors de la prochaine exécution de la tâche.

Si vous avez créé la tâche *Installation des mises à jour Windows Update*, seules les mises à jour spécifiées dans les propriétés de la tâche *Installation des mises à jour Windows Update* sont installées. À l'avenir, si vous souhaitez installer les nouvelles mises à jour téléchargées dans le stockage du Serveur d'administration, vous devez ajouter les mises à jour requises à la liste des mises à jour dans la tâche existante ou créer une nouvelle tâche *Installation des mises à jour Windows Update*.

Installation des mises à jour du logiciel tiers

Vous pouvez installer des mises à jour du logiciel tiers sur des appareils administrés en utilisant et en exécutant l'une des tâches suivantes :

- *Installation des mises à jour requises et correction des vulnérabilités*

  La tâche *Installation des mises à jour requises et correction des vulnérabilités* ne peut être créée que si vous disposez d'une licence pour la fonctionnalité Gestion des vulnérabilités et des correctifs. Vous pouvez utiliser cette tâche pour installer les mises à jour Windows Update fournies par Microsoft et les mises à jour des logiciels d'autres fournisseurs.

- *Installation des mises à jour Windows Update*

  Vous pouvez utiliser la tâche *Installation des mises à jour Windows Update* pour installer uniquement les mises à jour Windows Update.

Une interaction utilisateur peut être requise lorsque vous mettez à jour une application tierce ou corrigez une vulnérabilité dans une application tierce sur un appareil administré. Par exemple, l'utilisateur peut être invité à fermer l'application tierce si elle est actuellement ouverte.

Vous pouvez également créer une tâche pour installer les mises à jour requises comme suit :

- En ouvrant la liste des mises à jour et en définissant les mises à jour à installer.

  En conséquence, une nouvelle tâche d'installation des mises à jour sélectionnées est créée. En option, vous pouvez ajouter les mises à jour sélectionnées à une tâche existante.

- En exécutant l'Assistant d'installation de la mise à jour.

  L'Assistant d'installation de la mise à jour est accessible uniquement en présence d'une licence pour le fonctionnement de Gestion des vulnérabilités et des correctifs.

  L'Assistant simplifie la création et la configuration d'une tâche d'installation de mise à jour et vous permet d'éliminer la création de tâches redondantes contenant les mêmes mises à jour à installer.

Installation de mises à jour logicielles tierces à l'aide de la liste des mises à jour

Pour installer des mises à jour du logiciel tiers à l'aide de la liste des mises à jour, procédez comme suit :

1. Ouvrez l'une des listes des mises à jour :

   - Pour ouvrir la liste générale des mises à jour, dans le menu principal, accédez à **Opérations → Gestion des correctifs → Mises à jour du logiciel**.
   - Pour ouvrir la liste des mises à jour d'un appareil administré, dans le menu principal, accédez à **Ressources (Appareils) → Appareils administrés →** <nom de l'appareil> **→ Avancé → Mises à jour disponibles**.
   - Pour ouvrir la liste des mises à jour d'une application en particulier, dans le menu principal, accédez à **Opérations → Applications tierces → Registre des applications →** <nom de l'application> **→ Mises à jour disponibles**.

   Une liste des mises à jour disponibles s'affiche.

2. cochez les cases en regard des mises à jour que vous souhaitez installer.

3. Cliquez sur le bouton **Installer les mises à jour**.

   Pour installer certaines mises à jour logicielles, vous devez accepter le Contrat de licence utilisateur final (CLUF). Si vous refusez le CLUF, la mise à jour logicielle n'est pas installée.

4. Sélectionnez l'une des options ci-dessous :

   - **Nouvelle tâche**

     Ceci permet de lancer l'Assistant de création d'une tâche. Si vous disposez d'une licence pour le fonctionnement de Gestion des vulnérabilités et des correctifs, la tâche *Installation des mises à jour requises et correction des vulnérabilités* est présélectionnée. Si vous ne disposez pas de licence, la tâche *Installation des mises à jour Windows Update* est présélectionnée. Suivez les étapes de l'Assistant pour terminer la création de la tâche.

   - **Installer la mise à jour (ajouter une règle à la tâche indiquée)**

     Sélectionnez une tâche à laquelle vous souhaitez ajouter les mises à jour sélectionnées. Si vous disposez d'une licence pour le fonctionnement de Gestion des vulnérabilités et des correctifs, sélectionnez une tâche *Installation des mises à jour requises et correction des vulnérabilités*. Une nouvelle règle pour installer les mises à jour sélectionnées sera automatiquement ajoutée à la tâche sélectionnée. Si vous ne disposez pas de licence, sélectionnez la tâche *Installation des mises à jour Windows Update*. Les mises à jour sélectionnées seront ajoutées aux propriétés de la tâche.

     La fenêtre de propriétés de la tâche s'affiche. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications.

   Si vous avez choisi de créer une tâche, la tâche est créée et affichée dans la liste des tâches à l'endroit suivant : **Ressources (Appareils) → Tâches**. Si vous avez choisi d'ajouter les mises à jour à une tâche existante, les mises à jour sont enregistrées dans les propriétés de la tâche.

Pour installer des mises à jour de logiciel tiers, démarrez la tâche *Installation des mises à jour requises et correction des vulnérabilités* ou la tâche *Installation des mises à jour Windows Update*. Vous pouvez lancer n'importe laquelle de ces tâches manuellement ou spécifier des paramètres de planification dans les propriétés de la tâche que vous lancez. Lorsque vous définissez la planification de la tâche, assurez-vous que la tâche d'installation de la mise à jour est lancée une fois que la tâche *Recherche de vulnérabilités et de mises à jour requises* est terminée.

Installation de mises à jour logicielles tierces à l'aide de l'Assistant d'installation de la mise à jour

L'Assistant d'installation de la mise à jour est accessible uniquement en présence d'une licence pour le fonctionnement de Gestion des vulnérabilités et des correctifs.

Pour créer une tâche d'installation des mises à jour logicielles tierces à l'aide de l'Assistant d'installation de la mise à jour, procédez comme suit :

1. Dans le menu principal, accédez à **Opérations → Gestion des correctifs → Mises à jour du logiciel**.

   Une liste des mises à jour disponibles s'affiche.

2. Cochez la case en regard de la mise à jour que vous souhaitez installer.

3. Cliquez sur le bouton **Lancer l'Assistant d'installation de la mise à jour**.

   L'Assistant d'installation de la mise à jour démarre. La page **Sélection de la tâche d'installation de la mise à jour** affiche la liste de toutes les tâches existantes des types suivants :

   - *Installation des mises à jour requises et correction des vulnérabilités*
   - *Installation des mises à jour Windows Update*
   - *Corriger les vulnérabilités*

   Vous ne pouvez pas modifier les tâches des deux derniers types pour installer de nouvelles mises à jour. Pour installer de nouvelles mises à jour, vous ne pouvez utiliser que les tâches *Installation des mises à jour requises et correction des vulnérabilités*.

4. Si vous souhaitez que l'Assistant affiche uniquement les tâches qui installent la mise à jour que vous avez sélectionnée, activez l'option **Afficher uniquement les tâches d'installation de mise à jour**.

5. Choisissez la manière dont vous voulez procéder :

   - Pour démarrer une tâche, cochez la case en regard du nom de la tâche, puis cliquez sur le bouton **Démarrer**.
   - Pour ajouter une nouvelle règle à une tâche existante :

     a. Cochez la case en regard du nom de la tâche, puis cliquez sur le bouton **Ajouter une règle**.

     b. Sur la page qui s'ouvre, configurez la nouvelle règle :

     - **Règle d'installation des mises à jour du niveau d'importance sélectionné**

       Parfois, les mises à jour du logiciel peuvent nuire à l'expérience de l'utilisateur. Dans ce cas, il se peut que vous décidiez d'installer uniquement les mises à jour critiques au fonctionnement du logiciel et d'ignorer les autres.

       Quand cette option est activée, les mises à jour corrigent uniquement les vulnérabilités dont le niveau de gravité, tel que défini par Kaspersky, est égal ou supérieur au niveau de la mise à jour sélectionnée (**Moyenne**, **Élevé** ou **Critique**). Les vulnérabilités dont le niveau de gravité est inférieur à la valeur sélectionnée ne sont pas corrigées.

       Si cette option est désactivée, les mises à jour corrigent toutes les vulnérabilités, quel que soit le niveau de gravité.

       Cette option est Inactif par défaut.

     - **Règle d'installation des mises à jour du niveau d'importance sélectionné selon MSRC**

       Parfois, les mises à jour logicielles peuvent nuire à l'expérience de l'utilisateur. Dans ce cas, il se peut que vous décidiez d'installer uniquement les mises à jour critiques au fonctionnement du logiciel et d'ignorer les autres.

       Quand cette option est activée (disponible uniquement pour les mises à jour Windows), les mises à jour corrigent uniquement les vulnérabilités dont le niveau de gravité tel que défini par Microsoft Security Response Center (MSRC) est égal ou supérieur à la valeur sélectionnée dans la liste (**Bas**, **Moyen**, **Élevé** ou **Critique**). Les vulnérabilités dont le niveau de gravité est inférieur à la valeur sélectionnée ne sont pas corrigées.

       Si cette option est désactivée, les mises à jour corrigent toutes les vulnérabilités, quel que soit le niveau de gravité.

       Cette option est Inactif par défaut.

     - **Règle d'installation des mises à jour de cet éditeur**

       Cette option est disponible uniquement pour les mises à jour d'applications tierces. Kaspersky Security Center installe uniquement les mises à jour relatives aux applications créées par le même fournisseur que la mise à jour sélectionnée. Les mises à jour et les mises à jour refusées pour des applications créées par d'autres fournisseurs ne sont pas installées.

       Cette option est Inactif par défaut.

     - **Règle d'installation des mises à jour de type**
     - **Règle d'installation de la mise à jour sélectionnée**

- **Approuver les mises à jour sélectionnées**

  La mise à jour sélectionnée est approuvée pour l'installation. Activez cette option si certaines règles appliquées de l'installation de la mise à jour autorisent l'installation des mises à jour confirmées uniquement.

  Cette option est Inactif par défaut.

- **Installer automatiquement toutes les mises à jour précédentes des applications nécessaires à l'installation des mises à jour sélectionnées**

  Conservez cette option si vous acceptez l'installation de versions de l'application intermédiaires quand l'impose l'installation des mises à jour sélectionnées.

  Si vous désactivez cette option, seules les versions sélectionnées des applications sont installées. Désactivez cette option si vous souhaitez mettre à jour les applications d'une manière directe, sans tenter d'installer les versions successives. S'il est impossible d'installer les mises à jour sélectionnées sans installer les versions antérieures de l'application, la mise à jour de l'application échoue.

  Admettons que la version 3 d'une application est installée sur un appareil et vous souhaitez réaliser la mise à jour jusque la version 5, mais la version 5 de cette application peut être installée uniquement sur la version 4. Quand cette option est installée, le logiciel installe d'abord la version 4, puis la version 5. Si l'option est désactivée, le logiciel ne parvient pas à mettre l'application à jour.

  Cette option est activée par défaut.

c. Cliquez sur le bouton **Ajouter**.

- Pour créer une tâche, procédez comme suit :

  a. Cliquez sur le bouton **Nouvelle tâche**.

  b. Sur la page qui s'ouvre, configurez la nouvelle règle :

  - **Règle d'installation des mises à jour du niveau d'importance sélectionné**

    Parfois, les mises à jour du logiciel peuvent nuire à l'expérience de l'utilisateur. Dans ce cas, il se peut que vous décidiez d'installer uniquement les mises à jour critiques au fonctionnement du logiciel et d'ignorer les autres.

    Quand cette option est activée, les mises à jour corrigent uniquement les vulnérabilités dont le niveau de gravité, tel que défini par Kaspersky, est égal ou supérieur au niveau de la mise à jour sélectionnée (**Moyenne**, **Élevé** ou **Critique**). Les vulnérabilités dont le niveau de gravité est inférieur à la valeur sélectionnée ne sont pas corrigées.

    Si cette option est désactivée, les mises à jour corrigent toutes les vulnérabilités, quel que soit le niveau de gravité.

    Cette option est Inactif par défaut.

  - **Règle d'installation des mises à jour du niveau d'importance sélectionné selon MSRC**

Parfois, les mises à jour logicielles peuvent nuire à l'expérience de l'utilisateur. Dans ce cas, il se peut que vous décidiez d'installer uniquement les mises à jour critiques au fonctionnement du logiciel et d'ignorer les autres.

Quand cette option est activée (disponible uniquement pour les mises à jour Windows), les mises à jour corrigent uniquement les vulnérabilités dont le niveau de gravité tel que défini par Microsoft Security Response Center (MSRC) est égal ou supérieur à la valeur sélectionnée dans la liste (**Bas**, **Moyen**, **Élevé** ou **Critique**). Les vulnérabilités dont le niveau de gravité est inférieur à la valeur sélectionnée ne sont pas corrigées.

Si cette option est désactivée, les mises à jour corrigent toutes les vulnérabilités, quel que soit le niveau de gravité.

Cette option est Inactif par défaut.

- Règle d'installation des mises à jour de cet éditeur

  Cette option est disponible uniquement pour les mises à jour d'applications tierces. Kaspersky Security Center installe uniquement les mises à jour relatives aux applications créées par le même fournisseur que la mise à jour sélectionnée. Les mises à jour et les mises à jour refusées pour des applications créées par d'autres fournisseurs ne sont pas installées.

  Cette option est Inactif par défaut.

- **Règle d'installation des mises à jour de type**

- **Règle d'installation de la mise à jour sélectionnée**

- Approuver les mises à jour sélectionnées

  La mise à jour sélectionnée est approuvée pour l'installation. Activez cette option si certaines règles appliquées de l'installation de la mise à jour autorisent l'installation des mises à jour confirmées uniquement.

  Cette option est Inactif par défaut.

- Installer automatiquement toutes les mises à jour précédentes des applications nécessaires à l'installation des mises à jour sélectionnées

  Conservez cette option si vous acceptez l'installation de versions de l'application intermédiaires quand l'impose l'installation des mises à jour sélectionnées.

  Si vous désactivez cette option, seules les versions sélectionnées des applications sont installées. Désactivez cette option si vous souhaitez mettre à jour les applications d'une manière directe, sans tenter d'installer les versions successives. S'il est impossible d'installer les mises à jour sélectionnées sans installer les versions antérieures de l'application, la mise à jour de l'application échoue.

  Admettons que la version 3 d'une application est installée sur un appareil et vous souhaitez réaliser la mise à jour jusque la version 5, mais la version 5 de cette application peut être installée uniquement sur la version 4. Quand cette option est installée, le logiciel installe d'abord la version 4, puis la version 5. Si l'option est désactivée, le logiciel ne parvient pas à mettre l'application à jour.

  Cette option est activée par défaut.

c. Cliquez sur le bouton **Ajouter**.

Si vous avez choisi de démarrer une tâche, vous pouvez fermer l'assistant. La tâche se poursuivra en mode arrière-plan. Il n'y a rien d'autre à faire.

Si vous avez choisi d'ajouter une règle à une tâche existante, la fenêtre des propriétés de la tâche s'ouvre. La nouvelle règle est déjà ajoutée aux propriétés de la tâche. Vous pouvez afficher ou modifier la règle ou d'autres paramètres de tâche. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications.

Si vous avez choisi de créer une tâche, vous continuez à créer la tâche dans l'assistant de création d'une tâche. La nouvelle règle que vous avez ajoutée dans l'Assistant d'installation de la mise à jour s'affiche dans l'Assistant de création d'une tâche. Lorsque vous terminez l'Assistant, la tâche *Installation des mises à jour requises et correction des vulnérabilités* est ajoutée à la liste des tâches.

Création de la tâche Recherche de vulnérabilités et des mises à jour requises

Grâce à la tâche Recherche de vulnérabilités et de mises à jour requises, Kaspersky Security Center reçoit la liste des vulnérabilités détectées et des mises à jour requises pour les logiciels tiers installés sur les appareils administrés.

La tâche Recherche de vulnérabilités et de mises à jour requises est créée automatiquement lorsque l'Assistant de configuration initiale de l'application est en cours d'exécution. Si vous n'aviez pas exécuté l'assistant, vous pouvez créer la tâche manuellement.

Pour créer la tâche Recherche de vulnérabilités et de mises à jour requises, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Tâches**.
2. Cliquez sur **Ajouter**.

   Ceci permet de lancer l'assistant de création d'une tâche. Suivez les étapes de l'Assistant.
3. Pour l'application Kaspersky Security Center, sélectionnez le type de tâche **Recherche de vulnérabilités et de mises à jour requises**.
4. Spécifiez le nom de la tâche créée. Le nom de la tâche ne peut pas contenir plus de 100 symboles et contenir de symboles spéciaux ("*<>?\:|).
5. Sélectionnez les appareils auxquels les tâches seront affectées.
6. Si vous souhaitez modifier les paramètres de la tâche par défaut, activez l'option **Ouvrir les détails de la tâche à la fin de la création** sur la page **Fin de la création de la tâche**. Si vous n'activez pas cette tâche, la tâche est créée selon les paramètres par défaut. Vous pourrez modifier ces paramètres par défaut plus tard, à tout moment.
7. Cliquez sur le bouton **Créer**.

   La tâche est créée et s'affiche dans la liste des tâches.
8. Cliquez sur le nom de la tâche créée pour ouvrir la fenêtre de propriétés de la tâche.
9. Dans la fenêtre des propriétés de la tâche, indiquez les paramètres généraux de la tâche.

10. Dans l'onglet **Paramètres de l'application**, indiquez les paramètres suivants :

- **Rechercher les vulnérabilités et les mises à jour indiquées par Microsoft**

  Lors de la recherche de vulnérabilités et de mises à jour, Kaspersky Security Center utilise les informations sur les mises à jour Microsoft applicables à partir de la source des mises à jour Microsoft disponibles à ce moment là.

  Par exemple, pensez à désactiver cette option si vous avez différentes tâches avec différents paramètres pour les mises à jour Microsoft et les mises à jour d'applications tierces.

  Cette option est activée par défaut.

  Les informations sur les mises à jour facultatives de Microsoft Windows Update ne sont pas envoyées au Serveur d'administration.

- **Se connecter au serveur de mise à jour pour mettre à jour les données**

L'Agent de mises à jour Windows sur un appareil administré se connecte à la source des mises à jour Microsoft. Les serveurs suivants peuvent servir de source de mises à jour Microsoft :

- Serveur d'administration de Kaspersky Security Center (voir les paramètres de stratégie de l'Agent d'administration)
- Serveur Windows sur lequel Microsoft Windows Server Update Services (WSUS) est déployé dans le réseau de votre organisation
- Serveurs de mises à jour Microsoft

Si cette option est activée, l'Agent de mises à jour Windows sur un appareil administré se connecte à la source de mise à jour Microsoft pour actualiser les informations relatives aux mises à jour Microsoft Windows applicables.

Si cette option est désactivée, l'Agent de mises à jour Windows sur un appareil administré utilise les informations relatives aux mises à jour Microsoft Windows obtenues antérieurement auprès de la source des mises à jour Microsoft.

La connexion à la source des mises à jour Microsoft peut requérir beaucoup de ressources. Pensez à désactiver cette option si vous définissez une connexion régulière à cette source de mises à jour dans une autre tâche ou dans les propriétés de la stratégie de l'Agent d'administration, dans la section **Mises à jour et vulnérabilités du logiciel**. Si vous ne souhaitez pas désactiver cette option, pour réduire la surcharge, vous pouvez configurer la planification des tâches pour randomiser le délai de démarrage des tâches dans les 360 minutes.

Cette option est activée par défaut.

La combinaison des options suivantes des paramètres de la stratégie de l'Agent d'administration définit le mode d'obtention des mises à jour :

- L'Agent de mises à jour Windows sur un appareil administré se connecte au Serveur de mises à jour pour obtenir les mises à jour uniquement si l'option **Se connecter au serveur de mise à jour pour mettre à jour les données** est activée dans les propriétés de la tâche *Recherche de vulnérabilités et de mises à jour requises* et si l'option **Mode de recherche des mises à jour Windows Update** est définie sur **Actif** dans les paramètres de la stratégie de l'Agent d'administration.
- Si vous n'avez pas besoin de l'Agent d'administration pour établir une connexion à la source des mises à jour Microsoft Windows et télécharger les mises à jour lors de l'exécution de la tâche *Recherche de vulnérabilités*, vous pouvez définir l'option **Mode de recherche des mises à jour Windows Update** sur **Passif**, tandis que l'option **Se connecter au serveur de mise à jour pour mettre à jour les données** doit rester activée. Cela vous permet d'économiser des ressources et d'utiliser les mises à jour de Windows déjà reçues pour vérifier la présence de vulnérabilités. Vous pouvez utiliser le mode passif si vous configurez la réception des mises à jour Microsoft Windows différemment. Si la réception des mises à jour Microsoft Windows n'est pas configurée d'une autre manière, ne définissez pas l'option du **Mode de recherche des mises à jour Windows Update** sur **Passif**, car dans ce cas, les informations sur les mises à jour ne seront jamais reçues.
- Quel que soit l'état de l'option **Se connecter au serveur de mise à jour pour mettre à jour les données** (activé ou désactivé), si l'option **Mode de recherche des mises à jour Windows Update** est définie sur **Désactivé**, Kaspersky Security Center ne demande aucune information sur les mises à jour.

- Rechercher les vulnérabilités et les mises à jour de tiers indiquées par Kaspersky

Si cette option est activée, Kaspersky Security Center recherche des vulnérabilités et les mises à jour requises des produits tiers (applications développées par des éditeurs d'application autres que Kaspersky et Microsoft) dans le Registre Windows et dans les dossiers définis sous **Indiquez les chemins pour la recherche avancée des applications dans le système de fichiers**. La liste complète des produits tiers pris en charge est administrée par Kaspersky.

Si cette option est désactivée, Kaspersky Security Center ne recherche pas les vulnérabilités et les mises à jour requises pour les applications tiers. Par exemple, pensez à désactiver cette option si vous avez différentes tâches avec différents paramètres pour les mises à jour Microsoft Windows et les mises à jour d'applications tierces.

Cette option est activée par défaut.

- **Indiquez les chemins d'accès pour la recherche avancée des applications dans le système de fichiers**

  Les dossiers dans lesquels Kaspersky Security Center recherche des produits tiers qui requièrent une correction de la vulnérabilité et l'installation d'une mise à jour. Vous pouvez utiliser des variables système.

  Indiquez les dossiers dans lesquels les applications doivent être installées. Par défaut, la liste contient les dossiers système dans lesquels la majorité des applications sont installées.

- **Activer le diagnostic avancé**

  Quand cette fonction est activée, l'Agent d'administration enregistre des fichiers de trace même si l'écriture de fichiers de trace est désactivée pour l'Agent d'administration dans l'utilitaire de diagnostic à distance Kaspersky Security Center. Les traces sont enregistrées dans deux fichiers en alternance la taille de chacun de ces fichiers est déterminée par la valeur paramètre **Taille maximale (Mo) des fichiers de diagnostic avancé**. Quand les deux fichiers sont remplis, l'Agent d'administration écrit à nouveau dans ceux-ci. Les fichiers avec les traces sont stockés dans le dossier %WINDIR%\Temp. Ces fichiers sont accessibles dans l'utilitaire de diagnostic à distance, vous pouvez les télécharger ou les supprimer à cet endroit.

  Quand cette fonction est désactivée, l'Agent d'administration enregistre les traces conformément aux paramètres définis dans l'utilitaire de diagnostic à distance Kaspersky Security Center. Aucune trace complémentaire n'est écrite.

  Lors de la création d'une tâche, il n'est pas nécessaire d'activer le diagnostic avancé. Par contre, vous pouvez activer cette fonction plus tard si, par exemple, une tâche échoue sur certains appareils et que vous souhaitez obtenir des informations complémentaires lors d'une autre exécution de la tâche.

  Cette option est Inactif par défaut.

- **Taille maximale (Mo) des fichiers de diagnostic avancé**

  La valeur par défaut est de 100 Mo, mais elle peut se situer entre 1 et 2 048 Mo. Il peut arriver qu'un expert du Support Technique de Kaspersky vous demande de modifier la valeur par défaut lorsque les informations reprises dans les fichiers de diagnostic avancés que vous avez envoyés ne suffisent pas pour résoudre le problème.

11. Cliquez sur le bouton **Enregistrer**.

La tâche est créée et configurée.

Si les résultats de la tâche contiennent un avertissement concernant l'erreur 0x80240033 " Erreur de l'agent de mise à jour Windows 80240033 (" Les conditions de licence n'ont pas pu être téléchargées ") ", vous pouvez résoudre ce problème via le registre Windows.

La tâche Recherche de vulnérabilités et de mises à jour requises est créée

La tâche *Recherche de vulnérabilités et de mises à jour requises* est créée automatiquement lorsque l'assistant de démarrage rapide de l'application est en cours d'exécution. Si vous n'aviez pas exécuté l'assistant, vous pouvez créer la tâche manuellement.

En plus des paramètres de la tâche générale, vous pouvez indiquer les paramètres suivants lors de la création de la tâche *Recherche de vulnérabilités et de mises à jour requises*, ou plus tard, lorsque vous configurez les propriétés de la tâche créée :

- **Rechercher les vulnérabilités et les mises à jour indiquées par Microsoft**

  Lors de la recherche de vulnérabilités et de mises à jour, Kaspersky Security Center utilise les informations sur les mises à jour Microsoft applicables à partir de la source des mises à jour Microsoft disponibles à ce moment là.

  Par exemple, pensez à désactiver cette option si vous avez différentes tâches avec différents paramètres pour les mises à jour Microsoft et les mises à jour d'applications tierces.

  Cette option est activée par défaut.

  Les informations sur les mises à jour facultatives de Microsoft Windows Update ne sont pas envoyées au Serveur d'administration.

- **Se connecter au serveur de mise à jour pour mettre à jour les données**

L'Agent de mises à jour Windows sur un appareil administré se connecte à la source des mises à jour Microsoft. Les serveurs suivants peuvent servir de source de mises à jour Microsoft :

- Serveur d'administration de Kaspersky Security Center (voir les paramètres de stratégie de l'Agent d'administration)
- Serveur Windows sur lequel Microsoft Windows Server Update Services (WSUS) est déployé dans le réseau de votre organisation
- Serveurs de mises à jour Microsoft

Si cette option est activée, l'Agent de mises à jour Windows sur un appareil administré se connecte à la source de mise à jour Microsoft pour actualiser les informations relatives aux mises à jour Microsoft Windows applicables.

Si cette option est désactivée, l'Agent de mises à jour Windows sur un appareil administré utilise les informations relatives aux mises à jour Microsoft Windows obtenues antérieurement auprès de la source des mises à jour Microsoft.

La connexion à la source des mises à jour Microsoft peut requérir beaucoup de ressources. Pensez à désactiver cette option si vous définissez une connexion régulière à cette source de mises à jour dans une autre tâche ou dans les propriétés de la stratégie de l'Agent d'administration, dans la section **Mises à jour et vulnérabilités du logiciel**. Si vous ne souhaitez pas désactiver cette option, pour réduire la surcharge, vous pouvez configurer la planification des tâches pour randomiser le délai de démarrage des tâches dans les 360 minutes.

Cette option est activée par défaut.

La combinaison des options suivantes des paramètres de la stratégie de l'Agent d'administration définit le mode d'obtention des mises à jour :

- L'Agent de mises à jour Windows sur un appareil administré se connecte au Serveur de mises à jour pour obtenir les mises à jour uniquement si l'option **Se connecter au serveur de mise à jour pour mettre à jour les données** est activée dans les propriétés de la tâche *Recherche de vulnérabilités et de mises à jour requises* et si l'option **Mode de recherche des mises à jour Windows Update** est définie sur **Actif** dans les paramètres de la stratégie de l'Agent d'administration.
- Si vous n'avez pas besoin de l'Agent d'administration pour établir une connexion à la source des mises à jour Microsoft Windows et télécharger les mises à jour lors de l'exécution de la tâche *Recherche de vulnérabilités*, vous pouvez définir l'option **Mode de recherche des mises à jour Windows Update** sur **Passif**, tandis que l'option **Se connecter au serveur de mise à jour pour mettre à jour les données** doit rester activée. Cela vous permet d'économiser des ressources et d'utiliser les mises à jour de Windows déjà reçues pour vérifier la présence de vulnérabilités. Vous pouvez utiliser le mode passif si vous configurez la réception des mises à jour Microsoft Windows différemment. Si la réception des mises à jour Microsoft Windows n'est pas configurée d'une autre manière, ne définissez pas l'option du **Mode de recherche des mises à jour Windows Update** sur **Passif**, car dans ce cas, les informations sur les mises à jour ne seront jamais reçues.
- Quel que soit l'état de l'option **Se connecter au serveur de mise à jour pour mettre à jour les données** (activé ou désactivé), si l'option **Mode de recherche des mises à jour Windows Update** est définie sur **Désactivé**, Kaspersky Security Center ne demande aucune information sur les mises à jour.

- **Rechercher les vulnérabilités et les mises à jour de tiers indiquées par Kaspersky**

  Si cette option est activée, Kaspersky Security Center recherche des vulnérabilités et les mises à jour requises des produits tiers (applications développées par des éditeurs d'application autres que Kaspersky et Microsoft) dans le Registre Windows et dans les dossiers définis sous **Indiquez les chemins pour la recherche avancée des applications dans le système de fichiers**. La liste complète des produits tiers pris en charge est administrée par Kaspersky.

  Si cette option est désactivée, Kaspersky Security Center ne recherche pas les vulnérabilités et les mises à jour requises pour les applications tiers. Par exemple, pensez à désactiver cette option si vous avez différentes tâches avec différents paramètres pour les mises à jour Microsoft Windows et les mises à jour d'applications tierces.

  Cette option est activée par défaut.

- **Indiquez les chemins d'accès pour la recherche avancée des applications dans le système de fichiers**

  Les dossiers dans lesquels Kaspersky Security Center recherche des produits tiers qui requièrent une correction de la vulnérabilité et l'installation d'une mise à jour. Vous pouvez utiliser des variables système.

  Indiquez les dossiers dans lesquels les applications doivent être installées. Par défaut, la liste contient les dossiers système dans lesquels la majorité des applications sont installées.

- **Activer le diagnostic avancé**

  Quand cette fonction est activée, l'Agent d'administration enregistre des fichiers de trace même si l'écriture de fichiers de trace est désactivée pour l'Agent d'administration dans l'utilitaire de diagnostic à distance Kaspersky Security Center. Les traces sont enregistrées dans deux fichiers en alternance la taille de chacun de ces fichiers est déterminée par la valeur paramètre **Taille maximale (Mo) des fichiers de diagnostic avancé**. Quand les deux fichiers sont remplis, l'Agent d'administration écrit à nouveau dans ceux-ci. Les fichiers avec les traces sont stockés dans le dossier %WINDIR%\Temp. Ces fichiers sont accessibles dans l'utilitaire de diagnostic à distance, vous pouvez les télécharger ou les supprimer à cet endroit.

  Quand cette fonction est désactivée, l'Agent d'administration enregistre les traces conformément aux paramètres définis dans l'utilitaire de diagnostic à distance Kaspersky Security Center. Aucune trace complémentaire n'est écrite.

  Lors de la création d'une tâche, il n'est pas nécessaire d'activer le diagnostic avancé. Par contre, vous pouvez activer cette fonction plus tard si, par exemple, une tâche échoue sur certains appareils et que vous souhaitez obtenir des informations complémentaires lors d'une autre exécution de la tâche.

  Cette option est Inactif par défaut.

- **Taille maximale (Mo) des fichiers de diagnostic avancé**

  La valeur par défaut est de 100 Mo, mais elle peut se situer entre 1 et 2 048 Mo. Il peut arriver qu'un expert du Support Technique de Kaspersky vous demande de modifier la valeur par défaut lorsque les informations reprises dans les fichiers de diagnostic avancés que vous avez envoyés ne suffisent pas pour résoudre le problème.

Recommandations sur la planification des tâches

Lors de la planification de la tâche *Recherche de vulnérabilités et de mises à jour requises*, assurez-vous que les deux options **Lancer les tâches non exécutées** et **Adopter un décalage aléatoire automatique pour les lancements de tâche** sont activées.

Par défaut, la tâche *Recherche de vulnérabilités et de mises à jour requises* est configurée pour démarrer manuellement. Si le règlement de travail de la société prévoit la désactivation des appareils à ce moment, la tâche *Recherche de vulnérabilités et de mises à jour requises* est lancée après l'activation de l'appareil, c'est-à-dire le matin du lendemain. Ce comportement est à éviter car la recherche de vulnérabilités peut augmenter la charge sur le processeur et le sous-système de disque de l'appareil. Vous devez configurer une programmation optimale de cette tâche sur la base du règlement de travail adopté par l'entreprise.

Création de la tâche Installer les mises à jour requises et corriger les vulnérabilités

> La tâche *Installation des mises à jour requises et correction des vulnérabilités* est accessible uniquement en présence d'une licence pour le fonctionnement de Gestion des vulnérabilités et des correctifs.

La tâche *Installation des mises à jour requises et correction des vulnérabilités* est utilisée pour effectuer les mises à jour et réparer les vulnérabilités de logiciels tiers, y compris les logiciels Microsoft, installés sur les appareils administrés. Cette tâche vous permet d'installer plusieurs mises à jour et de corriger différentes vulnérabilités en fonction de certaines règles.

Pour installer des mises à jour ou corriger des vulnérabilités à l'aide de la tâche *Installation des mises à jour requises et correction des vulnérabilités*, vous pouvez effectuer l'une des opérations suivantes :

- Exécutez l'assistant d'installation des mises à jour ou l'assistant de correction des vulnérabilités.
- Créez une tâche *Installation des mises à jour requises et correction des vulnérabilités*.
- Ajoutez une règle pour l'installation de la mise à jour à une tâche *Installation des mises à jour requises et correction des vulnérabilités* existante.

Pour créer une tâche Installation des mises à jour requises et correction des vulnérabilités :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Tâches**.
2. Cliquez sur **Ajouter**.

   Ceci permet de lancer l'assistant de création d'une tâche. Suivez les étapes de l'assistant.
3. Pour l'application Kaspersky Security Center, sélectionnez le type de tâche **Installation des mises à jour requises et correction des vulnérabilités**.

   Si la tâche ne s'affiche pas, vérifiez si votre compte dispose des privilèges **Lire**, **Modifier** et **Exécuter** pour la zone fonctionnelle **Administration du système** : **Gestion des vulnérabilités et des correctifs** Vous ne pouvez pas créer et configurer la tâche *Installation des mises à jour requises et correction des vulnérabilités* sans ces droits d'accès.
4. Spécifiez le nom de la tâche créée. Le nom de la tâche ne peut pas contenir plus de 100 symboles et contenir de symboles spéciaux ("*<>?\:|).
5. Sélectionnez les appareils auxquels les tâches seront affectées.

6. Indiquez les règles d'installation des mises à jour, puis définissez les paramètres suivants :

- **Commencer l'installation au moment du redémarrage ou de l'arrêt de l'appareil**

  Si cette option est activée, les mises à jour sont installées lors du redémarrage ou de l'arrêt de l'appareil. Dans le cas contraire, les mises à jour sont installées selon la programmation.

  Utilisez cette option si l'installation des mises à jour peut avoir un impact sur les performances de l'appareil.

  Cette option est Inactif par défaut.

- **Installer les modules système général requis**

  Si cette option est activée, l'application, avant d'installer une mise à jour, installe automatiquement tous les composants généraux système (prérequis) requis pour l'installation de la mise à jour. Par exemple, il peut s'agir des mises à jour du système d'exploitation.

  Si cette option est désactivée, vous devrez peut-être installer les prérequis manuellement.

  Cette option est Inactif par défaut.

- **Autoriser l'installation de nouvelles versions de l'application lors des mises à jour**

  Si cette option est activée, les mises à jour sont autorisées lorsqu'elles entraînent l'installation d'une nouvelle version d'un logiciel.

  Si cette option est désactivée, le logiciel n'est pas mis à jour. Vous pouvez alors installer les nouvelles versions du logiciel manuellement ou via un autre tâche. Par exemple, vous pouvez utiliser cette option si l'infrastructure de votre entreprise n'est pas prise en charge par une nouvelle version du logiciel ou si vous souhaitez vérifier une mise à jour dans une infrastructure d'essai.

  Cette option est activée par défaut.

  La mise à jour d'une application peut provoquer un dysfonctionnement des applications dépendantes installées sur les appareils clients.

- **Télécharger les mises à jour sur l'appareil sans les installer**

  Quand cette option est activée, l'application télécharge les mises à jour sur l'appareil, mais ne les installe pas automatiquement. Vous pouvez installer les mises à jour manuellement par la suite.

  Les mises à jour Microsoft sont téléchargées dans le stockage Windows système. Les mises à jour des produits tiers (applications développées par des éditeurs d'application autres que Kaspersky et Microsoft) sont téléchargées dans le dossier indiqué dans le champ **Télécharger les mises à jour sur**.

  Si cette option est désactivée, les mises à jour sont installées automatiquement sur l'appareil.

  Cette option est Inactif par défaut.

- **Télécharger les mises à jour sur**

  Ce dossier est utilisé dans le cadre du téléchargement des mises à jour de produits tiers (applications développées par des éditeurs de logiciels autres que Kaspersky et Microsoft).

- **Activer le diagnostic avancé**

Quand cette fonction est activée, l'Agent d'administration enregistre des fichiers de trace même si l'écriture de fichiers de trace est désactivée pour l'Agent d'administration dans l'utilitaire de diagnostic à distance Kaspersky Security Center. Les traces sont enregistrées dans deux fichiers en alternance la taille de chacun de ces fichiers est déterminée par la valeur paramètre **Taille maximale (Mo) des fichiers de diagnostic avancé**. Quand les deux fichiers sont remplis, l'Agent d'administration écrit à nouveau dans ceux-ci. Les fichiers avec les traces sont stockés dans le dossier %WINDIR%\Temp. Ces fichiers sont accessibles dans l'utilitaire de diagnostic à distance, vous pouvez les télécharger ou les supprimer à cet endroit.

Quand cette fonction est désactivée, l'Agent d'administration enregistre les traces conformément aux paramètres définis dans l'utilitaire de diagnostic à distance Kaspersky Security Center. Aucune trace complémentaire n'est écrite.

Lors de la création d'une tâche, il n'est pas nécessaire d'activer le diagnostic avancé. Par contre, vous pouvez activer cette fonction plus tard si, par exemple, une tâche échoue sur certains appareils et que vous souhaitez obtenir des informations complémentaires lors d'une autre exécution de la tâche.

Cette option est Inactif par défaut.

- **Taille maximale (Mo) des fichiers de diagnostic avancé**

  La valeur par défaut est de 100 Mo, mais elle peut se situer entre 1 et 2 048 Mo. Il peut arriver qu'un expert du Support Technique de Kaspersky vous demande de modifier la valeur par défaut lorsque les informations reprises dans les fichiers de diagnostic avancés que vous avez envoyés ne suffisent pas pour résoudre le problème.

7. Définissez les paramètres de redémarrage du système d'exploitation :

- **Ne pas redémarrer l'appareil**

  Les appareils clients ne redémarrent pas automatiquement après l'opération. Pour arrêter le fonctionnement, il faut redémarrer l'appareil (par exemple, manuellement ou à l'aide d'une tâche d'administration des appareils). Les informations sur la nécessité du redémarrage sont enregistrées dans les résultats de la tâche et dans l'état de l'appareil. Cette option convient aux tâches d' sur les serveurs et autres appareils pour lesquels la continuité des opérations est critique.

- **Redémarrer l'appareil**

  Dans ce cas, le redémarrage des appareils clients est toujours exécuté automatiquement, si celui-ci est requis pour terminer l'opération. Cette option convient aux tâches d' sur des appareils pour lesquels des interruptions périodiques sont admises (débranchement, redémarrage).

- **Confirmer l'action auprès de l'utilisateur**

  Le message qui signale que l'appareil client doit être redémarré manuellement s'affiche sur l'écran de l'appareil. Pour cette option, il est possible de configurer des paramètres avancés : le texte du message pour l'utilisateur, la fréquence du message, ainsi que le délai à l'issue duquel le redémarrage sera forcé (sans confirmation de l'utilisateur). Cette option convient le mieux pour les postes de travail sur lesquels les utilisateurs doivent pouvoir sélectionner l'heure de redémarrage qui leur convient le mieux.

  Cette option est sélectionnée par défaut.

- **Répéter la demande toutes les (min.)**

  Quand cette option est activée, l'application invite l'utilisateur à redémarrer le système d'exploitation selon la fréquence indiquée.

  Cette option est activée par défaut. L'intervalle par défaut est de 5 minutes. La valeur peut être comprise entre 1 et 1 440 minutes.

  Si cette option est désactivée, l'invite est affichée une seule fois.

- **Redémarrer le système au bout de (min.)**

  Après avoir averti l'utilisateur, l'application force le redémarrage du système d'exploitation à l'issue de l'intervalle défini.

  Cette option est activée par défaut. Le délai par défaut est de 30 minutes. La valeur peut être comprise entre 1 et 1 440 minutes.

- **Délai d'attente avant la fermeture forcée des ap&plications dans les sessions bloquées (min)**

  Arrêt forcé des applications lorsque l'appareil de l'utilisateur est verrouillé (arrêt manuel ou automatique après une période d'inactivité).

  Si cette option est activée, les applications en cours sur l'appareil verrouillé seront fermées de force à la fin du délai indiqué dans le champ situé à côté de la case.

  Si cette option est activée, les applications en cours sur l'appareil verrouillé ne seront pas fermées.

  Cette option est Inactif par défaut.

8. Si vous souhaitez modifier les paramètres de la tâche par défaut, activez l'option **Ouvrir les détails de la tâche à la fin de la création** sur la page **Fin de la création de la tâche**. Si vous n'activez pas cette tâche, la tâche est créée selon les paramètres par défaut. Vous pourrez modifier ces paramètres par défaut plus tard, à tout moment.

9. Cliquez sur le bouton **Terminer**.

   La tâche est créée et s'affiche dans la liste des tâches.

10. Cliquez sur le nom de la tâche créée pour ouvrir la fenêtre de propriétés de la tâche.

11. Dans la fenêtre des propriétés de la tâche, indiquez les paramètres généraux de la tâche en fonction de vos besoins.

12. Cliquez sur le bouton **Enregistrer**.

    La tâche est créée et configurée.

Si les résultats de la tâche contiennent un avertissement concernant l'erreur 0x80240033 " Erreur de l'agent de mise à jour Windows 80240033 (" Les conditions de licence n'ont pas pu être téléchargées ") ", vous pouvez résoudre ce problème via le registre Windows.

Ajout de règles pour l'installation de la mise à jour

Cette fonctionnalité est accessible uniquement en présence d'une licence pour le fonctionnement de Gestion des vulnérabilités et des correctifs.

Lors de l'installation de mises à jour logicielles ou de la correction de vulnérabilités dans les applications à l'aide de la tâche *Installation des mises à jour requises et correction des vulnérabilités*, vous devez définir les règles pour l'installation de la mise à jour. Ces règles déterminent les mises à jour à installer et les vulnérabilités à corriger.

Les paramètres exacts dépendent de l'objet pour lequel vous ajoutez une règle : pour toutes les mises à jour, pour les mises à jour Windows Update ou pour les mises à jour d'applications tierces (applications développées par des éditeurs autres que Kaspersky et Microsoft). Lors de l'ajout d'une règle pour des mises à jour Windows Update ou des mises à jour d'applications tierces, vous pouvez sélectionner des applications spécifiques et les versions de l'application pour lesquelles vous souhaitez installer les mises à jour. Lors de l'ajout d'une règle pour toutes les mises à jour, vous pouvez sélectionner les mises à jour spécifiques que vous souhaitez installer et les vulnérabilités que vous souhaitez éliminer via l'installation des mises à jour.

Vous pouvez ajouter une règle pour l'installation de la mise à jour comme suit :

- En ajoutant une règle lors de la création d'une nouvelle tâche Installation des mises à jour requises et correction des vulnérabilités.
- En ajoutant une règle sous l'onglet **Paramètres de l'application** dans la fenêtre des propriétés d'une tâche *Installation des mises à jour requises et correction des vulnérabilités* existante.
- Via l'assistant d'installation des mises à jour ou l'assistant de correction des vulnérabilités.

Pour ajouter une nouvelle règle pour toutes les mises à jour, procédez comme suit :

1. Cliquez sur le bouton **Ajouter**.

   L'Assistant de création de règles se lance. Parcourez les étapes de l'assistant à l'aide du bouton **Suivant**.

2. Sur la page **Type de règle**, sélectionnez **Règle pour toutes les mises à jour**.

3. Sur la page **Critères généraux**, utilisez les listes déroulantes pour définir les paramètres suivants :

   - **Définir les mises à jour à installer**

     Sélectionnez les mises à jour qui doivent être installées sur les appareils clients :

     - **Installer uniquement les mises à jour confirmées**. Cette option installe uniquement les mises à jour confirmées.
     - **Installer toutes les mises à jour (sauf les mises à jour rejetées)**. Cette option installe les mises à jour avec l'état *Approuvé* ou *Non défini*.
     - **Installer toutes les mises à jour (y compris les mises à jour rejetées)**. Ceci installe toutes les mises à jour, quel que soit leur état d'approbation. Sélectionnez cette option avec prudence. Par exemple, utilisez cette option si vous souhaitez vérifier l'installation de certaines mises à jour rejetées dans une infrastructure d'essai.

   - **Corriger les vulnérabilités de niveau de gravité égal ou supérieur à**

     Parfois, les mises à jour du logiciel peuvent nuire à l'expérience de l'utilisateur. Dans ce cas, il se peut que vous décidiez d'installer uniquement les mises à jour critiques au fonctionnement du logiciel et d'ignorer les autres.

     Quand cette option est activée, les mises à jour corrigent uniquement les vulnérabilités dont le niveau de gravité tel que défini par Kaspersky est égal ou supérieur à la valeur sélectionnée dans la liste (**Moyenne**, **Élevé** ou **Critique**). Les vulnérabilités dont le niveau de gravité est inférieur à la valeur sélectionnée ne sont pas corrigées.

     Si cette option est désactivée, les mises à jour corrigent toutes les vulnérabilités, quel que soit le niveau de gravité.

     Cette option est Inactif par défaut.

4. Sur la page **Mises à jour**, sélectionnez les mises à jour à installer :

- **Installer toutes les mises à jour convenables**

  Installez toutes les mises à jour du logiciel qui répondent aux critères définis à la page **Critères généraux** de l'assistant. Sélectionné par défaut.

- **Installer uniquement les mises à jour depuis la liste**

  Installer uniquement les mises à jour du logiciel que vous sélectionnez manuellement dans la liste. Cette liste contient toutes les mises à jour du logiciel disponibles.

  Par exemple, vous pouvez sélectionner des mises à jour spécifiques dans les cas suivants : pour vérifier leur installation dans un environnement d'essai, pour mettre à jour uniquement les applications critiques ou pour mettre à jour uniquement certaines applications.

  - **&Installer automatiquement toutes les mises à jour précédentes des applications nécessaires à l'installation des mises à jour sélectionnées**

    Conservez cette option si vous acceptez l'installation de versions de l'application intermédiaires quand l'impose l'installation des mises à jour sélectionnées.

    Si vous désactivez cette option, seules les versions sélectionnées des applications sont installées. Désactivez cette option si vous souhaitez mettre à jour les applications d'une manière directe, sans tenter d'installer les versions successives. S'il est impossible d'installer les mises à jour sélectionnées sans installer les versions antérieures de l'application, la mise à jour de l'application échoue.

    Admettons que la version 3 d'une application est installée sur un appareil et vous souhaitez réaliser la mise à jour jusque la version 5, mais la version 5 de cette application peut être installée uniquement sur la version 4. Quand cette option est installée, le logiciel installe d'abord la version 4, puis la version 5. Si l'option est désactivée, le logiciel ne parvient pas à mettre l'application à jour.

    Cette option est activée par défaut.

5. Sur la page **Vulnérabilités**, sélectionnez les vulnérabilités que seront corrigées suite à l'installation des mises à jour sélectionnées :

- **Corriger toutes les vulnérabilités qui correspondent aux autres critères**

  Corrigez toutes les vulnérabilités qui satisfont les critères définis à la page **Critères généraux** de l'assistant. Sélectionné par défaut.

- **Corriger uniquement les vulnérabilités depuis la liste**

  Corrigez uniquement les vulnérabilités que vous sélectionnez manuellement dans la liste. Cette liste contient toutes les vulnérabilités détectées.

  Par exemple, vous pouvez sélectionner des vulnérabilités spécifiques dans les cas suivants : pour vérifier les corrections dans un environnement d'essai, pour corriger les vulnérabilités uniquement dans les applications critiques ou pour corriger les vulnérabilités uniquement dans certaines applications.

6. La page **Nom** permet de renseigner le nom de la règle ajoutée. Vous pouvez changer ce nom plus tard dans la section **Paramètres** de la fenêtre des propriétés de la tâche créée.

Une fois que l'assistant de création de règles a terminé, la nouvelle règle est ajoutée et s'affiche dans la liste des règles de l'assistant de création d'une tâche ou dans les propriétés de la tâche.

Pour ajouter une nouvelle règle pour les mises à jour de Windows Update, procédez comme suit :

1. Cliquez sur le bouton **Ajouter**.

   L'Assistant de création de règles se lance. Parcourez les étapes de l'assistant à l'aide du bouton **Suivant**.

2. Sur la page **Type de règle**, sélectionnez **Règle pour les mises à jour Windows Update**.

3. Dans la fenêtre **Conditions générales**, configurez les paramètres suivants :

   - **Définir les mises à jour à installer**

     Sélectionnez les mises à jour qui doivent être installées sur les appareils clients :

     - **Installer uniquement les mises à jour confirmées**. Cette option installe uniquement les mises à jour confirmées.
     - **Installer toutes les mises à jour (sauf les mises à jour rejetées)**. Cette option installe les mises à jour avec l'état *Approuvé* ou *Non défini*.
     - **Installer toutes les mises à jour (y compris les mises à jour rejetées)**. Ceci installe toutes les mises à jour, quel que soit leur état d'approbation. Sélectionnez cette option avec prudence. Par exemple, utilisez cette option si vous souhaitez vérifier l'installation de certaines mises à jour rejetées dans une infrastructure d'essai.

   - **Corriger les vulnérabilités de niveau de gravité égal ou supérieur à**

     Parfois, les mises à jour du logiciel peuvent nuire à l'expérience de l'utilisateur. Dans ce cas, il se peut que vous décidiez d'installer uniquement les mises à jour critiques au fonctionnement du logiciel et d'ignorer les autres.

     Quand cette option est activée, les mises à jour corrigent uniquement les vulnérabilités dont le niveau de gravité tel que défini par Kaspersky est égal ou supérieur à la valeur sélectionnée dans la liste (**Moyenne**, **Élevé** ou **Critique**). Les vulnérabilités dont le niveau de gravité est inférieur à la valeur sélectionnée ne sont pas corrigées.

     Si cette option est désactivée, les mises à jour corrigent toutes les vulnérabilités, quel que soit le niveau de gravité.

     Cette option est Inactif par défaut.

   - **Corriger les vulnérabilités qui présentent un niveau de gravité selon MSRC égal ou supérieur à**

     Parfois, les mises à jour du logiciel peuvent nuire à l'expérience de l'utilisateur. Dans ce cas, il se peut que vous décidiez d'installer uniquement les mises à jour critiques au fonctionnement du logiciel et d'ignorer les autres.

     Quand cette option est activée, les mises à jour corrigent uniquement les vulnérabilités dont le niveau de gravité tel que défini par Microsoft Security Response Center (MSRC) est égal ou supérieur à la valeur sélectionnée dans la liste (**Bas**, **Moyenne**, **Élevé** ou **Critique**). Les vulnérabilités dont le niveau de gravité est inférieur à la valeur sélectionnée ne sont pas corrigées.

     Si cette option est désactivée, les mises à jour corrigent toutes les vulnérabilités, quel que soit le niveau de gravité.

     Cette option est Inactif par défaut.

4. Sur la page **Applications**, sélectionnez les applications et les versions des applications pour lesquelles vous voulez installer les mises à jour. Toutes les applications sont cochées par défaut.

5. Sur la page **Catégorie des mises à jour**, sélectionnez les catégories des mises à jour à installer. Ces catégories sont les mêmes que dans le catalogue Microsoft Update. Toutes les catégories sont cochées par défaut.

6. La page **Nom** permet de renseigner le nom de la règle ajoutée. Vous pouvez changer ce nom plus tard dans la section **Paramètres** de la fenêtre des propriétés de la tâche créée.

Une fois que l'assistant de création de règles a terminé, la nouvelle règle est ajoutée et s'affiche dans la liste des règles de l'assistant de création d'une tâche ou dans les propriétés de la tâche.

Pour ajouter une règle pour les mises à jour des produits tiers, procédez comme suit :

1. Cliquez sur le bouton **Ajouter**.

   L'Assistant de création de règles se lance. Parcourez les étapes de l'assistant à l'aide du bouton **Suivant**.

2. Sur la page **Type de règle**, sélectionnez **Règles pour les mises à jour tierces**.

3. Dans la fenêtre **Conditions générales**, configurez les paramètres suivants :

   - **Définir les mises à jour à installer**

     Sélectionnez les mises à jour qui doivent être installées sur les appareils clients :

     - **Installer uniquement les mises à jour confirmées**. Cette option installe uniquement les mises à jour confirmées.
     - **Installer toutes les mises à jour (sauf les mises à jour rejetées)**. Cette option installe les mises à jour avec l'état *Approuvé* ou *Non défini*.
     - **Installer toutes les mises à jour (y compris les mises à jour rejetées)**. Ceci installe toutes les mises à jour, quel que soit leur état d'approbation. Sélectionnez cette option avec prudence. Par exemple, utilisez cette option si vous souhaitez vérifier l'installation de certaines mises à jour rejetées dans une infrastructure d'essai.

   - **Corriger les vulnérabilités de niveau de gravité égal ou supérieur à**

     Parfois, les mises à jour du logiciel peuvent nuire à l'expérience de l'utilisateur. Dans ce cas, il se peut que vous décidiez d'installer uniquement les mises à jour critiques au fonctionnement du logiciel et d'ignorer les autres.

     Quand cette option est activée, les mises à jour corrigent uniquement les vulnérabilités dont le niveau de gravité tel que défini par Kaspersky est égal ou supérieur à la valeur sélectionnée dans la liste (**Moyenne**, **Élevé** ou **Critique**). Les vulnérabilités dont le niveau de gravité est inférieur à la valeur sélectionnée ne sont pas corrigées.

     Si cette option est désactivée, les mises à jour corrigent toutes les vulnérabilités, quel que soit le niveau de gravité.

     Cette option est Inactif par défaut.

4. Sur la page **Applications**, sélectionnez les applications et les versions des applications pour lesquelles vous voulez installer les mises à jour. Toutes les applications sont cochées par défaut.

5. La page **Nom** permet de renseigner le nom de la règle ajoutée. Vous pouvez changer ce nom plus tard dans la section Paramètres de la fenêtre des propriétés de la tâche créée.

Une fois que l'assistant de création de règles a terminé, la nouvelle règle est ajoutée et s'affiche dans la liste des règles de l'assistant de création d'une tâche ou dans les propriétés de la tâche.

Création de la tâche Installation des mises à jour Windows Update

La tâche *Installation des mises à jour Windows Update* vous permet d'installer les mises à jour logicielles fournies par le service Windows Update sur les appareils administrés.

Si vous ne disposez pas d'une licence pour le fonctionnement de Gestion des vulnérabilités et des correctifs, vous ne pouvez pas créer de nouvelles tâches de type *Installation des mises à jour Windows Update*. Pour installer de nouvelles mises à jour, vous pouvez les ajouter à une tâche *Installation des mises à jour Windows Update* existante. Il est conseillé d'utiliser la tâche *Installation des mises à jour requises et correction des vulnérabilités* plutôt que la tâche *Installation des mises à jour Windows Update*. La tâche *Installation des mises à jour requises et correction des vulnérabilités* vous permet d'installer plusieurs mises à jour et de corriger automatiquement plusieurs vulnérabilités, selon les règles que vous définissez. En outre, cette tâche vous permet d'installer des mises à jour de fournisseurs de logiciels autres que Microsoft.

Une interaction utilisateur peut être requise lorsque vous mettez à jour une application tierce ou corrigez une vulnérabilité dans une application tierce sur un appareil administré. Par exemple, l'utilisateur peut être invité à fermer l'application tierce si elle est actuellement ouverte.

Pour créer la tâche Installation des mises à jour Windows Update :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Tâches**.
2. Cliquez sur **Ajouter**.

   Ceci permet de lancer l'assistant de création d'une tâche. Parcourez les étapes de l'Assistant à l'aide du bouton **Suivant**.
3. Pour l'application Kaspersky Security Center, sélectionnez le type de tâche **Installation des mises à jour Windows Update**.
4. Spécifiez le nom de la tâche créée.

   Le nom de la tâche ne peut pas contenir plus de 100 symboles et contenir de symboles spéciaux ("*<>?\:|).
5. Sélectionnez les appareils auxquels les tâches seront affectées.
6. Cliquez sur le bouton **Ajouter**.

   La liste des mises à jour s'ouvre.
7. Sélectionnez les mises à jour Windows Update que vous souhaitez installer, puis cliquez sur **OK**.

8. Définissez les paramètres de redémarrage du système d'exploitation :

- **Ne pas redémarrer l'appareil**

  Les appareils clients ne redémarrent pas automatiquement après l'opération. Pour arrêter le fonctionnement, il faut redémarrer l'appareil (par exemple, manuellement ou à l'aide d'une tâche d'administration des appareils). Les informations sur la nécessité du redémarrage sont enregistrées dans les résultats de la tâche et dans l'état de l'appareil. Cette option convient aux tâches d' sur les serveurs et autres appareils pour lesquels la continuité des opérations est critique.

- **Redémarrer l'appareil**

  Dans ce cas, le redémarrage des appareils clients est toujours exécuté automatiquement, si celui-ci est requis pour terminer l'opération. Cette option convient aux tâches d' sur des appareils pour lesquels des interruptions périodiques sont admises (débranchement, redémarrage).

- **Confirmer l'action auprès de l'utilisateur**

  Le message qui signale que l'appareil client doit être redémarré manuellement s'affiche sur l'écran de l'appareil. Pour cette option, il est possible de configurer des paramètres avancés : le texte du message pour l'utilisateur, la fréquence du message, ainsi que le délai à l'issue duquel le redémarrage sera forcé (sans confirmation de l'utilisateur). Cette option convient le mieux pour les postes de travail sur lesquels les utilisateurs doivent pouvoir sélectionner l'heure de redémarrage qui leur convient le mieux.

  Cette option est sélectionnée par défaut.

- **Répéter la demande toutes les (min.)**

  Quand cette option est activée, l'application invite l'utilisateur à redémarrer le système d'exploitation selon la fréquence indiquée.

  Cette option est activée par défaut. L'intervalle par défaut est de 5 minutes. La valeur peut être comprise entre 1 et 1 440 minutes.

  Si cette option est désactivée, l'invite est affichée une seule fois.

- **Redémarrer le système au bout de (min.)**

  Après avoir averti l'utilisateur, l'application force le redémarrage du système d'exploitation à l'issue de l'intervalle défini.

  Cette option est activée par défaut. Le délai par défaut est de 30 minutes. La valeur peut être comprise entre 1 et 1 440 minutes.

- **Forcer la fermeture des applications dans les sessions bloquées**

Les applications en cours d'exécution peuvent empêcher le redémarrage de l'appareil client. Par exemple, si un document est en train d'être modifié dans un logiciel de traitement de texte et qu'il n'est pas enregistré, l'application n'autorise pas le redémarrage de l'appareil.

Quand cette option est activée, l'arrêt forcé de ces applications sur un appareil verrouillé doit avoir lieu avant de pouvoir redémarrer l'appareil. Les utilisateurs pourraient perdre toute modification qui n'a pas été enregistrée à ce moment.

Si cette option est désactivée, un appareil verrouillé n'est pas redémarré. L'état de la tâche sur cet appareil indique qu'il faut redémarrer l'appareil. Les utilisateurs doivent quitter manuellement toutes les applications en cours d'exécution sur les appareils verrouillés, puis redémarrer ces appareils.

Cette option est Inactif par défaut.

9. Définissez les paramètres du compte :

- **Compte par défaut**

  La tâche sera lancée sous le même compte utilisateur sous lequel l'application, exécutant cette tâche, a été installée et lancée.

  Cette option est sélectionnée par défaut.

- **Indiquer un compte**

  Remplissez les champs **Compte utilisateur** et **Mot de passe** pour définir les détails d'un compte à partir duquel la tâche est exécutée. Le compte doit disposer de droits suffisants pour cette tâche.

- **Compte utilisateur**

  Le compte utilisateur au nom duquel la tâche sera lancée.

- **Mot de passe**

  Mot de passe du compte utilisateur au nom duquel la tâche sera lancée.

10. Si vous souhaitez modifier les paramètres de la tâche par défaut, activez l'option **Ouvrir les détails de la tâche à la fin de la création** sur la page **Fin de la création de la tâche**. Si vous n'activez pas cette tâche, la tâche est créée selon les paramètres par défaut. Vous pourrez modifier ces paramètres par défaut plus tard, à tout moment.

11. Cliquez sur le bouton **Terminer**.

    La tâche est créée et s'affiche dans la liste des tâches.

12. Cliquez sur le nom de la tâche créée pour ouvrir la fenêtre de propriétés de la tâche.

13. Dans la fenêtre des propriétés de la tâche, indiquez les paramètres généraux de la tâche en fonction de vos besoins.

14. Cliquez sur le bouton **Enregistrer**.

La tâche est créée et configurée.

Consultation des informations sur les mises à jour du logiciel tiers disponibles

Vous pouvez consulter la liste des mises à jour disponibles pour les logiciels tiers, y compris les logiciels Microsoft installés sur les appareils client.

Pour consulter la liste des mises à jour disponibles pour les applications tierces installées sur les appareils client,

Dans le menu principal, accédez à **Opérations → Gestion des correctifs → Mises à jour du logiciel**.

Une liste des mises à jour disponibles s'affiche.

Vous pouvez indiquer un filtre pour consulter la liste des mises à jour du logiciel. Cliquez sur l'icône **Filtrer** ( ) dans le coin supérieur droit de la liste des mises à jour du logiciel pour gérer le filtre. Vous pouvez également sélectionner l'un des filtres prédéfinis dans la liste déroulante **Filtres prédéfinis** située au-dessus de la liste des vulnérabilités dans les applications.

Pour consulter les propriétés de la mise à jour, procédez comme suit :

1. Cliquez sur le nom de la mise à jour du logiciel concernée.
2. La fenêtre des propriétés de la mise à jour s'ouvre. Cette fenêtre affiche des informations regroupées sous les onglets suivants :

   - **Général**

     Cet onglet affiche les détails généraux de la mise à jour sélectionnée :

     - Mettre à jour l'état d'approbation (peut être modifié manuellement en sélectionnant un nouvel état dans la liste déroulante)
     - Catégorie Windows Server Update Services (WSUS) à laquelle appartient la mise à jour
     - Date et heure d'enregistrement de la mise à jour
     - Date et heure de création de la mise à jour
     - Niveau d'importance de la mise à jour
     - Exigences d'installation imposées par la mise à jour
     - Famille d'applications à laquelle appartient la mise à jour
     - Application à laquelle la mise à jour s'applique
     - Numéro de révision de la mise à jour

   - **Attributs**

Cet onglet affiche un ensemble d'attributs que vous pouvez utiliser pour en savoir plus à propos de la mise à jour sélectionnée. Cet ensemble diffère selon que la mise à jour est publiée par Microsoft ou par un fournisseur tiers.

L'onglet affiche les informations suivantes pour une mise à jour Microsoft :

- Niveau d'importance de la mise à jour, d'après Microsoft Security Response Center (MSRC)
- Lien vers l'article de Microsoft Knowledge Base décrivant la mise à jour
- Lien vers l'article de Microsoft Security Bulletin décrivant la mise à jour
- Identifiant de la mise à jour

L'onglet affiche les informations suivantes pour une mise à jour tierce :

- Que la mise à jour soit un correctif ou un paquet de distribution complet
- Langue de localisation de la mise à jour
- Si la mise à jour est installée automatiquement ou manuellement
- Si la mise à jour a été révoquée après avoir été appliquée
- Lien pour télécharger la mise à jour

- **Appareils**

  Cet onglet affiche une liste des appareils sur lesquels la mise à jour sélectionnée a été installée.

- **Vulnérabilités à corriger**

  Cet onglet affiche une liste de vulnérabilités que la mise à jour sélectionnée peut corriger.

- **Croisement de mises à jour**

  Cet onglet affiche les croisements possibles entre différentes mises à jour publiées pour la même application, c'est-à-dire si la mise à jour sélectionnée peut remplacer d'autres mises à jour (disponible pour les mises à jour Microsoft uniquement).

- **Tâches d'installation de la mise à jour**

  Cet onglet affiche une liste de tâches dont la zone d'action comprend l'installation de la mise à jour sélectionnée. L'onglet vous permet également de créer une nouvelle tâche d'installation à distance pour la mise à jour.

Pour consulter les statistiques de l'installation d'une mise à jour :

1. cochez la case à côté de la mise à jour du logiciel requise.
2. Cliquez sur le bouton **Statistiques de l'état de l'installation des mises à jour**.

Le diagramme des états de l'installation des mises à jour s'affiche. Cliquer sur un état ouvre une liste des appareils sur lesquels la mise à jour présente l'état sélectionné.

Vous pouvez consulter les informations sur les mises à jour du logiciel disponibles pour les logiciels tiers, y compris les logiciels Microsoft installés sur l'appareil administré sélectionné exécutant Windows.

Pour consulter la liste des mises à jour disponibles pour les logiciels tiers installés sur l'appareil administré sélectionné :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Appareils administrés**.

   La liste des appareils administrés s'affiche.

2. Dans la liste des appareils administrés, cliquez sur le lien portant le nom de l'appareil pour lequel vous souhaitez afficher les mises à jour du logiciel.

   La fenêtre des propriétés de l'appareil sélectionné s'affiche.

3. Dans la fenêtre des propriétés de l'appareil sélectionné, ouvrez l'onglet **Avancé**.

4. Dans le volet gauche, sélectionnez la section **Mises à jour disponibles**. Si vous souhaitez uniquement afficher les mises à jour installées, activez l'option **Afficher les mises à jour installées**.

La liste des mises à jour du logiciel tiers disponibles pour l'appareil sélectionné s'affiche.

Exportation de la liste des mises à jour du logiciel disponibles vers un fichier

Vous pouvez exporter la liste des mises à jour du logiciel tiers, y compris les logiciels Microsoft, qui s'affiche actuellement vers les fichiers au format CSV ou TXT. Vous pouvez par exemple utiliser ces fichiers pour les envoyer à votre responsable de la sécurité de l'information ou les stocker à des fins statistiques.

Pour exporter vers un fichier texte la liste des mises à jour disponibles pour les logiciels tiers installés sur tous les appareils administrés, procédez comme suit :

1. Dans le menu principal, accédez à **Opérations** → **Gestion des correctifs** → **Mises à jour du logiciel**.

   La page affiche une liste des mises à jour disponibles pour les logiciels tiers installés sur tous les appareils administrés.

2. Cliquez sur le bouton **Exporter vers un fichier TXT** ou **Exporter vers un fichier CSV** en fonction du format que vous préférez exporter.

Le fichier contenant la liste des mises à jour disponibles pour les logiciels tiers, y compris les logiciels Microsoft, est téléchargé sur l'appareil que vous utilisez actuellement.

Pour exporter vers un fichier texte la liste des mises à jour disponibles pour les logiciels tiers installés sur les appareils administrés sélectionnés, procédez comme suit :

1. Ouvrez la liste des mises à jour du logiciel tiers disponibles sur l'appareil administré sélectionné.
2. Sélectionnez les mises à jour dans les applications que vous souhaitez exporter.

   Ignorez cette étape si vous souhaitez exporter une liste complète des mises à jour.

   Si vous souhaitez exporter la liste complète des mises à jour, seules les mises à jour affichées sur la page actuelle seront exportées.

   Si vous souhaitez uniquement exporter les mises à jour installées, cochez la case **Afficher les mises à jour installées**.
3. Cliquez sur le bouton **Exporter vers un fichier TXT** ou **Exporter vers un fichier CSV** en fonction du format que vous préférez exporter.

Le fichier contenant la liste des mises à jour des logiciels tiers, y compris les logiciels Microsoft, installés sur l'appareil administré sélectionné est téléchargé sur l'appareil que vous utilisez en ce moment.

Approuver et refuser les mises à jour du logiciel tiers

Lorsque vous configurez la tâche *Installation des mises à jour requises et correction des vulnérabilités*, vous pouvez créer une règle qui exige un état particulier des mises à jour qui doivent être installées. Par exemple, une règle de mise à jour peut permettre l'installation des éléments suivants :

- Les mises à jour approuvées uniquement
- Les mises à jour approuvées et non définies uniquement
- Toutes les mises à jour peu importe l'état de la mise à jour

Vous pouvez approuver les mises à jour à installer et refuser les mises à jour qui ne doivent pas installer.

L'utilisation de l'état *Approuvé* pour gérer l'installation des mises à jour est efficace pour un petit nombre de mises à jour. Pour installer plusieurs mises à jour, utilisez les règles que vous pouvez configurer dans la tâche *Installation des mises à jour requises et correction des vulnérabilités*. Nous vous recommandons de définir l'état *Approuvé* uniquement pour les mises à jour particulières qui ne répondent pas aux critères spécifiés dans les règles. Lorsque vous approuvez manuellement une grande quantité de mises à jour, les performances du Serveur d'administration diminuent, ce qui peut entraîner une surcharge du Serveur d'administration.

Pour approuver ou refuser une ou plusieurs mises à jour :

1. Dans le menu principal, accédez à **Opérations → Gestion des correctifs → Mises à jour du logiciel**.

   Une liste des mises à jour disponibles s'affiche.
2. Sélectionnez les mises à jour que vous souhaitez approuver ou refuser.
3. Cliquez sur **Approuver** pour approuver les mises à jour sélectionnées ou sur **Refuser** pour les refuser.

   Par défaut, la valeur *Non défini* est cochée.

Les mises à jour sélectionnées ont les états que vous avez définis.

En option, vous pouvez modifier l'état d'approbation dans les propriétés d'une mise à jour en particulier.

Pour approuver ou refuser une mise à jour dans ses propriétés, procédez comme suit :

1. Dans le menu principal, accédez à **Opérations → Gestion des correctifs → Mises à jour du logiciel**.

   Une liste des mises à jour disponibles s'affiche.

2. Cliquez sur le nom de la mise à jour que vous souhaitez approuver ou refuser.

   La fenêtre de propriétés de la mise à jour s'affiche.

3. Dans la section **Général**, sélectionnez un état pour la mise à jour en modifiant l'option **État d'approbation de la mise à jour**. Vous pouvez sélectionner l'état *Approuvée*, *Rejetée* ou *Non défini*.

4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications.

La mise à jour sélectionnée présente l'état que vous avez défini.

Si vous attribuez l'état **Rejetée** aux mises à jour du logiciel tiers, ces mises à jour ne sont pas installées sur les appareils où elles ont été planifiées mais pas encore installées. Les mises à jour seront conservées sur les appareils où elles ont déjà été installées. Si vous devez les supprimer, vous pouvez réaliser l'opération manuellement localement.

Création de la tâche Synchronisation des mises à jour Windows Update

La tâche *Synchronisation des mises à jour Windows Update* est accessible uniquement en présence d'une licence pour le fonctionnement de Gestion des vulnérabilités et des correctifs.

La tâche *Synchronisation des mises à jour Windows Update* est requise si vous souhaitez utiliser le Serveur d'administration comme serveur WSUS. Dans ce cas, le Serveur d'administration télécharge les mises à jour Windows dans la base de données et fournit les mises à jour de Windows Update sur les appareils clients en mode centralisé via les Agents d'administration. Si le réseau n'utilise pas de serveur WSUS, chaque appareil client télécharge indépendamment les mises à jour Microsoft depuis des serveurs externes.

La tâche *Synchronisation des mises à jour Windows Update* télécharge uniquement les métadonnées à partir des serveurs Microsoft. Kaspersky Security Center télécharge les mises à jour lorsque vous exécutez une tâche d'installation de mise à jour et uniquement les mises à jour que vous sélectionnez pour l'installation.

Pendant l'exécution de la tâche **Synchronisation des mises à jour Windows Update**, l'application reçoit la liste des mises à jour actuelles depuis le serveur de mises à jour de Microsoft. Kaspersky Security Center définit ensuite la liste des mises à jour obsolètes. Lors du lancement suivant de la tâche **Recherche de vulnérabilités et de mises à jour requises**, Kaspersky Security Center identifie toutes les mises à jour obsolètes et détermine leur délai de suppression. Lors du lancement suivant de la tâche **Synchronisation des mises à jour Windows Update**, les mises à jour identifiées 30 jours auparavant comme devant être supprimées sont effectivement supprimées. Kaspersky Security Center effectue également une analyse complémentaire pour la suppression des mises à jour identifiées plus de 180 jours auparavant comme devant être supprimées.

Au terme de l'exécution de la tâche **Synchronisation des mises à jour Windows Update** et de la suppression des mises à jour obsolètes, les codes de hachage des fichiers des mises à jour supprimées peuvent persister dans la base de données, au même titre que les fichiers correspondants dans les fichiers %AllUsersProfile%\Application Data\KasperskyLab\adminkit\1093\.working\wusfiles (s'ils ont été préalablement téléchargés). Vous pouvez exécuter la tâche **Maintenance du Serveur d'administration** pour supprimer ces entrées obsolètes de la base de données, ainsi que les fichiers correspondants.

Pour créer la tâche Synchronisation des mises à jour Windows Update :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Tâches**.
2. Cliquez sur **Ajouter**.

   Ceci permet de lancer l'assistant de création d'une tâche. Suivez les étapes de l'Assistant.
3. Pour l'application Kaspersky Security Center, sélectionnez le type de tâche **Synchronisation des mises à jour Windows Update**.
4. Spécifiez le nom de la tâche créée. Le nom de la tâche ne peut pas contenir plus de 100 symboles et contenir de symboles spéciaux ("*<>?\:|).
5. Activez l'option **Télécharger les mises à jour rapides** si vous souhaitez que les fichiers de mise à jour rapides soient téléchargés lors de l'exécution de la tâche.

   Quand Kaspersky Security Center synchronise les mises à jour avec les serveurs Microsoft Windows Update Servers, les informations relatives à l'ensemble des fichiers sont enregistrées dans la base de données du Serveur d'administration. De même, tous les fichiers indispensables à la mise à jour sont téléchargés sur le disque en cas d'interaction avec l'Agent de mises à jour Windows. Plus particulièrement, Kaspersky Security Center enregistre les informations relatives aux fichiers de mises à jour express dans la base de données et les télécharge en fonction des besoins. Le téléchargement des fichiers de mises à jour express provoque la réduction de l'espace disponible sur le disque.

   Pour limiter la réduction de l'espace de disque et réduire le trafic, désactivez l'option **Télécharger les mises à jour rapides**.
6. Sélectionnez les applications pour lesquelles vous souhaitez télécharger des mises à jour.

   Si la case **Toutes les applications** est cochée, les mises à jour sont téléchargées pour toutes les applications existantes, ainsi que pour les applications susceptibles d'être éditées à l'avenir.
7. Sélectionnez les catégories de mises à jour que vous souhaitez télécharger sur le Serveur d'administration.

   Si la case **Toutes les catégories** est cochée, les mises à jour sont téléchargées pour toutes les catégories de mises à jour disponibles, ainsi que pour les catégories qui pourraient apparaître à l'avenir.
8. Sélectionnez les versions linguistiques de mises à jour que vous souhaitez télécharger sur le Serveur d'administration. Sélectionnez l'une des options ci-dessous :

   - **Télécharger toutes les langues, y compris les nouvelles langues**

     Si cette option a été sélectionnée, toutes les langues disponibles de localisation des mises à jour seront téléchargées sur le Serveur d'administration. Cette option est sélectionnée par défaut.

   - **Télécharger les langues sélectionnées**

     Si cette option a été sélectionnée, la liste permet de sélectionner les langues de localisation des mises à jour à télécharger sur le Serveur d'administration.

9. Définissez le compte à utiliser lors de l'exécution de la tâche. Sélectionnez l'une des options ci-dessous :

   - **Compte par défaut**

     La tâche sera lancée sous le même compte utilisateur sous lequel l'application, exécutant cette tâche, a été installée et lancée.

     Cette option est sélectionnée par défaut.

   - **Indiquer un compte**

     Remplissez les champs **Compte utilisateur** et **Mot de passe** pour définir les détails d'un compte à partir duquel la tâche est exécutée. Le compte doit disposer de droits suffisants pour cette tâche.

10. Si vous souhaitez modifier les paramètres de la tâche par défaut, activez l'option **Ouvrir les détails de la tâche à la fin de la création** sur la page **Fin de la création de la tâche**. Si vous n'activez pas cette tâche, la tâche est créée selon les paramètres par défaut. Vous pourrez modifier ces paramètres par défaut plus tard, à tout moment.

11. Cliquez sur le bouton **Terminer**.

    La tâche est créée et s'affiche dans la liste des tâches.

12. Cliquez sur le nom de la tâche créée pour ouvrir la fenêtre de propriétés de la tâche.

13. Dans la fenêtre des propriétés de la tâche, indiquez les paramètres généraux de la tâche en fonction de vos besoins.

14. Cliquez sur le bouton **Enregistrer**.

La tâche est créée et configurée.

Mise à jour automatique des applications tierces

Certaines applications tierces peuvent être mises à jour automatiquement. Le fournisseur de l'application définit si l'application prend en charge ou non la fonctionnalité de mise à jour automatique. Si une application tierce installée sur un appareil administré prend en charge la mise à jour automatique, vous pouvez définir le paramètre de mise à jour automatique dans les propriétés de l'application. Une fois que vous avez modifié le paramètre de mise à jour automatique, les Agents d'administration appliquent le nouveau paramètre sur chaque appareil administré sur lequel l'application est installée.

Le paramètre de mise à jour automatique est indépendant des autres objets et paramètres de la fonctionnalité de la gestion des vulnérabilités et des correctifs. Par exemple, ce paramètre ne dépend pas d'un état d'approbation de mise à jour ou des tâches d'installation de mise à jour, comme *Installation des mises à jour requises et correction des vulnérabilités*, *Installation des mises à jour Windows Update* et *Corriger les vulnérabilités*.

Pour configurer le paramètre de mise à jour automatique pour une application tierce, procédez comme suit :

1. Dans le menu principal, accédez à **Opérations → Applications tierces → Registre des applications**.

2. Cliquez sur le nom de l'application pour laquelle vous souhaitez modifier le paramètre de mise à jour automatique.

   Pour simplifier la recherche, vous pouvez filtrer la liste par la colonne **État des mises à jour automatiques**.

   La fenêtre de propriétés de l'application s'affiche.

3. Dans la section **Général**, sélectionnez une valeur pour le paramètre suivant :

   État des mises à jour automatiques

   Sélectionnez l'une des options ci-dessous :

   - **Non défini**

     La fonctionnalité de mise à jour automatique est désactivée. Kaspersky Security Center installe les mises à jour d'applications tierces à l'aide des tâches suivantes : *Installation des mises à jour requises et correction des vulnérabilités*, *Installation des mises à jour Windows Update* et *Corriger les vulnérabilités*.

   - **Autorisé**

     Une fois que le fournisseur a publié une mise à jour pour l'application, cette mise à jour est installée automatiquement sur les appareils administrés. Il n'y a rien d'autre à faire.

   - **Bloqué**

     Les mises à jour de l'application ne sont pas installées automatiquement. Kaspersky Security Center installe les mises à jour d'applications tierces à l'aide des tâches suivantes : *Installation des mises à jour requises et correction des vulnérabilités*, *Installation des mises à jour Windows Update* et *Corriger les vulnérabilités*.

4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications.

Le paramètre de mise à jour automatique est appliqué à l'application sélectionnée.

Correction des vulnérabilités logicielles tierces

Cette section décrit les fonctions de Kaspersky Security Center associées à la correction des vulnérabilités dans les logiciels installés sur les appareils administrés.

Scénario : Recherche et correction des vulnérabilités dans les logiciels tiers

Cette section fournit un scénario de recherche et de réparation des vulnérabilités sur les appareils administrés sous Windows. Vous pouvez rechercher et corriger les vulnérabilités dans les applications du système d'exploitation et dans les logiciels tiers, y compris les logiciels Microsoft.

Prérequis

- Kaspersky Security Center est déployé dans votre entreprise.
- Il existe des appareils administrés sous Windows dans votre organisation.
- Une connexion Internet est requise pour que le Serveur d'administration puisse effectuer les tâches suivantes :
  - Pour dresser une liste des correctifs recommandés pour les vulnérabilités des logiciels Microsoft. La liste est créée et régulièrement mise à jour par des spécialistes de Kaspersky.
  - Pour corriger les vulnérabilités de logiciels tiers autres que les logiciels Microsoft.

Étapes

La recherche et la correction des vulnérabilités logicielles s'effectuent par étapes :

1. **Recherche de vulnérabilités dans les logiciels installés sur les appareils administrés**

   Pour rechercher les vulnérabilités dans les logiciels installés sur les appareils administrés, exécutez la tâche *Recherche de vulnérabilités et de mises à jour requises*. Une fois cette tâche terminée, Kaspersky Security Center reçoit la liste des vulnérabilités détectées et des mises à jour requises pour les logiciels tiers installés sur les appareils que vous avez spécifiés dans les propriétés de la tâche.

   La tâche *Recherche de vulnérabilités et de mises à jour requises* est créée automatiquement par l'Assistant de configuration initiale de l'application Kaspersky Security Center. Si vous n'aviez pas exécuté l'Assistant, démarrez-le maintenant ou créez la tâche manuellement.

   Instructions pour :

   - Console d'administration : Recherche de vulnérabilités dans les applications, Planification de la tâche Recherche de vulnérabilités et des mises à jour requises
   - Kaspersky Security Center Web Console : création d'une tâche Recherche de vulnérabilités et de mises à jour requises, paramètres de Recherche de vulnérabilités et de mises à jour requises

2. **Analyser la liste des vulnérabilités logicielles détectées**

   Consultez la liste **Vulnérabilités dans les applications** et décidez quelles vulnérabilités doivent être corrigées. Pour consulter les informations détaillées de chaque vulnérabilité, cliquez sur le nom de la vulnérabilité dans la liste. Pour chaque vulnérabilité de la liste, vous pouvez également consulter les statistiques de la vulnérabilité sur les appareils administrés.

   Instructions pour :

   - Console d'administration : consultation des informations concernant les vulnérabilités logicielles, consultation des statistiques des vulnérabilités sur les appareils administrés
   - Kaspersky Security Center Web Console : Affichage des informations sur les vulnérabilités logicielles, Affichage des statistiques des vulnérabilités sur les appareils administrés

3. **Configuration de la correction des vulnérabilités**

   Lorsque des vulnérabilités sont détectées dans les applications, vous pouvez les corriger sur les appareils administrés à l'aide de la tâche *Installation des mises à jour requises et correction des vulnérabilités* ou de la tâche *Corriger les vulnérabilités*.

   La tâche *Installation des mises à jour requises et correction des vulnérabilités* est utilisée pour effectuer les mises à jour et réparer les vulnérabilités de logiciels tiers, y compris les logiciels Microsoft, installés sur les appareils administrés. Cette tâche vous permet d'installer plusieurs mises à jour et de corriger différentes vulnérabilités en fonction de certaines règles. Notez que cette tâche ne peut être créée que si vous disposez de la licence pour la fonctionnalité Gestion des vulnérabilités et des correctifs. Pour corriger les vulnérabilités dans les applications, la tâche *Installation des mises à jour requises et correction des vulnérabilités* utilise les mises à jour logicielles recommandées.

   La tâche *Corriger les vulnérabilités* ne nécessite pas l'option de licence pour la fonction Gestion des vulnérabilités et des correctifs. Pour utiliser cette tâche, vous devez spécifier manuellement les correctifs servant à corriger les vulnérabilités du logiciel tiers répertorié dans les paramètres de la tâche. La tâche *Corriger les vulnérabilités* utilise les correctifs recommandés pour les logiciels Microsoft et les correctifs utilisateurs pour les logiciels tiers.

   Vous pouvez démarrer l'Assistant de correction des vulnérabilités qui crée automatiquement l'une de ces tâches ou vous pouvez créer l'une de ces tâches manuellement.

   Instructions pour :

- Console d'administration : Sélection des correctifs utilisateur pour les vulnérabilités dans le logiciel tiers, Correction des vulnérabilités dans les applications
- Kaspersky Security Center Web Console : Sélection des correctifs utilisateur pour les vulnérabilités dans le logiciel tiers, Correction des vulnérabilités dans le logiciels tiers, Création de la tâche Installation des mises à jour requises et correction des vulnérabilités

4. **Planification des tâches**

   Pour vous assurer que la liste des vulnérabilités est toujours d'actualité, planifiez la tâche *Recherche de vulnérabilités et de mises à jour requises* pour l'exécuter automatiquement de temps à autre. La fréquence moyenne recommandée est d'une fois par semaine.

   Si vous avez créé la tâche *Installation des mises à jour requises et correction des vulnérabilités*, vous pouvez la planifier pour qu'elle soit exécutée à la même fréquence que la tâche *Recherche de vulnérabilités et de mises à jour requises* ou à une fréquence moindre. Lors de la planification de la tâche *Corriger les vulnérabilités*, notez que vous devez sélectionner des correctifs pour les logiciels Microsoft ou définir des correctifs utilisateur pour les logiciels tiers à chaque fois avant de démarrer la tâche.

   Lors de la planification des tâches, assurez-vous qu'une tâche pour corriger la vulnérabilité démarre une fois que la tâche *Recherche de vulnérabilités et de mises à jour requises* est terminée.

5. **Ignorer les vulnérabilités dans les applications (facultatif)**

   Vous pouvez si vous les souhaitez ignorer les vulnérabilités dans les applications à corriger sur tous les appareils administrés ou seulement sur les appareils administrés sélectionnés.

   Instructions pour :

   - Console d'administration : ignorer les vulnérabilités dans les applications
   - Kaspersky Security Center Web Console : ignorer les vulnérabilités dans les applications

6. **Exécution d'une tâche de correction de la vulnérabilité**

   Démarrez la tâche *Installation des mises à jour requises et correction des vulnérabilités* ou la tâche *Corriger la vulnérabilité*. Lorsque la tâche est terminée, assurez-vous qu'elle possède le statut *Terminée* dans la liste des tâches.

7. **Créer le rapport sur les résultats de la correction des vulnérabilités dans les applications (facultatif)**

   Pour consulter les statistiques détaillées concernant la correction des vulnérabilités, générez le rapport sur les vulnérabilités. Le rapport affiche des informations sur les vulnérabilités dans les applications non corrigées. Ainsi, vous pouvez vous faire une idée de la recherche et la correction des vulnérabilités dans les logiciels tiers, y compris les logiciels Microsoft, dans votre organisation.

   Instructions pour :

   - Console d'administration : création et affichage d'un rapport
   - Kaspersky Security Center Web Console : génération et affichage d'un rapport

8. **Vérification de la configuration de la recherche et de la correction des vulnérabilités dans les logiciels tiers**

   Assurez-vous d'avoir effectué les tâches suivantes :

   - Obtenu et vérifié la liste des vulnérabilités logicielles sur les appareils administrés
   - Ignoré les vulnérabilités dans les applications que vous souhaitiez ignorer
   - Configuré la tâche de correction des vulnérabilités

- Planifié les tâches de recherche et de correction des vulnérabilités logicielles pour qu'elles démarrent en séquence
- Vérifié que la tâche de correction des vulnérabilités dans les applications a été exécutée

Résultats

Si vous avez créé et configuré la tâche *Installation des mises à jour requises et correction des vulnérabilités*, les vulnérabilités sont corrigées automatiquement sur les appareils administrés. Lorsque la tâche est exécutée, elle met en corrélation la liste des mises à jour logicielles disponibles avec les règles spécifiées dans les paramètres de la tâche. Toutes les mises à jour logicielles qui répondent aux critères des règles seront téléchargées dans le stockage du Serveur d'administration et seront installées pour corriger les vulnérabilités dans les applications.

Si vous avez créé la tâche *Corriger les vulnérabilités*, seules les vulnérabilités dans les applications des logiciels Microsoft sont corrigées.

À propos de la recherche et de la correction des vulnérabilités dans les applications

Kaspersky Security Center détecte et répare les vulnérabilités dans les applications sur les appareils administrés exécutant des familles de systèmes d'exploitation Microsoft Windows. Les vulnérabilités sont détectées dans le système d'exploitation et les logiciels tiers, y compris les logiciels Microsoft.

La fonctionnalité des mises à jour (y compris la fourniture de mises à jour des signatures antivirus et des bases de code) ainsi que la fonctionnalité KSN peuvent ne pas être disponibles dans le logiciel aux États-Unis.

Recherche des vulnérabilités dans les applications

Pour rechercher des vulnérabilités dans les applications, Kaspersky Security Center utilise les caractéristiques de la base de données des vulnérabilités connues. Cette base de données est créée par les spécialistes de Kaspersky. Elle contient des informations sur les vulnérabilités, telles que la description, la date de détection et le niveau de gravité de la vulnérabilité. Vous pouvez recevoir des informations sur les vulnérabilités dans les applications sur le site Kaspersky.

Kaspersky Security Center utilise la tâche *Recherche de vulnérabilités et de mises à jour requises* pour détecter d'éventuelles vulnérabilités logicielles.

Dans certains cas, les vulnérabilités détectées dans un système d'exploitation Microsoft Windows peuvent être corrigées à l'aide d'une des méthodes suivantes :

- Installation d'une mise à jour pour le système d'exploitation.
- Mise à niveau du système d'exploitation vers une version plus récente (par exemple, de Windows 10 vers Windows 11).

Dans ce scénario, Kaspersky Security Center affiche deux entrées pour la même vulnérabilité.

Correction des vulnérabilités logicielles

Pour corriger les vulnérabilités dans les applications, Kaspersky Security Center utilise les mises à jour logicielles publiées par les fournisseurs de logiciels. Les métadonnées des mises à jour logicielles sont téléchargées sur le stockage du Serveur d'administration après l'exécution des tâches suivantes :

- *Téléchargement des mises à jour sur le stockage du Serveur d'administration*. Cette tâche est destinée à télécharger les métadonnées des mises à jour pour Kaspersky et les logiciels tiers. Cette tâche est créée automatiquement par l'Assistant de configuration initiale de l'application Kaspersky Security Center. Vous pouvez créer manuellement la tâche Télécharger les mises à jour dans le stockage du Serveur d'administration.

- *Synchronisation des mises à jour Windows Update*. Cette tâche est destinée à télécharger les métadonnées des mises à jour pour les logiciels Microsoft.

Les mises à jour logicielles visant à corriger les vulnérabilités peuvent être représentées sous forme de paquets de distribution complets ou de correctifs. Les mises à jour logicielles qui corrigent des vulnérabilités dans les applications sont appelées *correctifs*. L'installation *des correctifs recommandés* est préconisée par les spécialistes Kaspersky. L'installation *des correctifs utilisateur* est manuellement spécifiée par les utilisateurs. Pour installer un correctif utilisateur, vous devez créer un paquet d'installation contenant ce correctif.

Si vous détenez la licence de Kaspersky Security Center assortie de la fonctionnalité Gestion des vulnérabilités et des correctifs, pour corriger les vulnérabilités dans les applications, vous pouvez utiliser la tâche *Installation des mises à jour requises et correction des vulnérabilités*. Cette tâche corrige automatiquement de nombreuses vulnérabilités en installant les correctifs recommandés. Pour cette tâche, vous pouvez configurer manuellement certaines règles pour corriger plusieurs vulnérabilités.

Si vous ne détenez pas la licence de Kaspersky Security Center assortie de la fonctionnalité Gestion des vulnérabilités et des correctifs, pour corriger les vulnérabilités dans les applications, vous pouvez utiliser la tâche *Corriger les vulnérabilités*. À l'aide de cette tâche, vous pouvez corriger les vulnérabilités en installant les correctifs recommandés pour les logiciels Microsoft et les correctifs utilisateur pour les autres logiciels tiers.

Pour des raisons de sécurité, toutes les mises à jour logicielles tierces que vous installez à l'aide de la fonction de la gestion des vulnérabilités et des correctifs sont automatiquement analysées à la recherche de logiciels malveillants par les technologies de Kaspersky. Ces technologies sont utilisées pour la vérification automatique des fichiers et incluent la recherche de virus, l'analyse statique, l'analyse dynamique, l'analyse comportementale dans l'environnement sandbox et machine learning.

Les experts de Kaspersky n'effectuent pas d'analyse manuelle des mises à jour du logiciel tiers pouvant être installées par la fonction de la gestion des vulnérabilités et des correctifs. De plus, les experts de Kaspersky ne recherchent pas de vulnérabilités (connues ou inconnues) ou de fonctionnalités non documentées dans ces mises à jour, et n'effectuent pas d'autres types d'analyse des mises à jour que ceux indiqués dans le paragraphe ci-dessus.

Une interaction utilisateur peut être requise lorsque vous mettez à jour une application tierce ou corrigez une vulnérabilité dans une application tierce sur un appareil administré. Par exemple, l'utilisateur peut être invité à fermer l'application tierce si elle est actuellement ouverte.

Pour corriger certaines vulnérabilités dans les applications, vous devrez accepter le Contrat de licence utilisateur final (CLUF) du logiciel en cours d'installation si l'acceptation du CLUF est demandée. Si vous refusez le CLUF, la vulnérabilité logicielle ne sera pas corrigée.

Correction des vulnérabilités logicielles tierces

Une fois que vous avez obtenu la liste des vulnérabilités dans les applications, vous pouvez les corriger sur les appareils administrés qui fonctionnent sous Windows. Vous pouvez corriger les vulnérabilités dans les applications du système d'exploitation et des logiciels tiers, y compris les logiciels Microsoft, en créant et en exécutant la tâche *Corriger les vulnérabilités* ou la tâche *Installation des mises à jour requises et correction des vulnérabilités*.

Une interaction utilisateur peut être requise lorsque vous mettez à jour une application tierce ou corrigez une vulnérabilité dans une application tierce sur un appareil administré. Par exemple, l'utilisateur peut être invité à fermer l'application tierce si elle est actuellement ouverte.

Vous pouvez également créer une tâche pour corriger les vulnérabilités dans les applications comme suit :

- En ouvrant la liste des vulnérabilités et en indiquant les vulnérabilités à corriger.

  En conséquence, une nouvelle tâche de correction des vulnérabilités dans les applications est créée. En option, vous pouvez ajouter les vulnérabilités sélectionnées à une tâche existante.

- En exécutant l'Assistant de correction des vulnérabilités.

  L'Assistant de correction des vulnérabilités est accessible uniquement en présence d'une licence pour le fonctionnement de Gestion des vulnérabilités et des correctifs.

  L'Assistant simplifie la création et la configuration d'une tâche de correction de vulnérabilité et vous permet d'éliminer la création de tâches redondantes contenant les mêmes mises à jour à installer.

Correction des vulnérabilités dans les applications en utilisant la liste des vulnérabilités

Pour corriger les vulnérabilités dans les applications :

1. Ouvrez l'une des listes de vulnérabilités :

   - Pour ouvrir la liste générale des vulnérabilités, dans le menu principal, accédez à **Opérations** → **Gestion des correctifs** → **Vulnérabilités dans les applications**.
   - Pour ouvrir la liste des vulnérabilités d'un appareil administré, accédez à **Ressources (Appareils)** → **Appareils administrés** → <nom de l'appareil> → **Avancé** → **Vulnérabilités dans les applications**.
   - Pour ouvrir la liste des vulnérabilités d'une application en particulier, accédez à **Opérations** → **Applications tierces** → **Registre des applications** → <nom de l'application> → **Vulnérabilités**.

   Une page contenant une liste des vulnérabilités dans les applications tierces s'affiche.

2. Sélectionnez une ou plusieurs vulnérabilités dans la liste, puis cliquez sur le bouton **Corriger la vulnérabilité**.

   Si une mise à jour logicielle recommandée pour corriger l'une des vulnérabilités sélectionnées ne figure pas dans la liste, un message d'information s'affiche.

   Pour corriger certaines vulnérabilités dans les applications, vous devrez accepter le Contrat de licence utilisateur final (CLUF) du logiciel en cours d'installation si l'acceptation du CLUF est demandée. Si vous refusez le CLUF, la vulnérabilité dans l'application ne sera pas corrigée.

3. Sélectionnez l'une des options ci-dessous :

   - **Nouvelle tâche**

     Ceci permet de lancer l'Assistant de création d'une tâche. Si vous disposez d'une licence pour le fonctionnement de Gestion des vulnérabilités et des correctifs, la tâche *Installation des mises à jour requises et correction des vulnérabilités* est présélectionnée. Si vous ne disposez pas de licence, la tâche *Corriger les vulnérabilités* est présélectionnée. Suivez les étapes de l'Assistant pour terminer la création de la tâche.

   - **Corriger la vulnérabilité (ajouter une règle à la tâche indiquée)**

     Sélectionnez une tâche à laquelle vous souhaitez ajouter les vulnérabilités sélectionnées. Si vous disposez d'une licence pour le fonctionnement de Gestion des vulnérabilités et des correctifs, sélectionnez une tâche *Installation des mises à jour requises et correction des vulnérabilités*. Une nouvelle règle pour corriger les vulnérabilités sélectionnées sera automatiquement ajoutée à la tâche sélectionnée. Si vous ne disposez pas de licence, sélectionnez la tâche *Corriger les vulnérabilités*. Les vulnérabilités sélectionnées seront ajoutées aux propriétés de la tâche.

     La fenêtre de propriétés de la tâche s'affiche. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications.

   Si vous avez choisi de créer une tâche, la tâche est créée et affichée dans la liste des tâches à l'endroit suivant : **Ressources (Appareils)** → **Tâches**. Si vous avez choisi d'ajouter les vulnérabilités à une tâche existante, les vulnérabilités sont enregistrées dans les propriétés de la tâche.

Pour corriger les vulnérabilités dans les applications tierces, démarrez la tâche *Installation des mises à jour requises et correction des vulnérabilités* ou la tâche *Corriger les vulnérabilités*. Si vous avez créé la tâche *Corriger les vulnérabilités*, vous devez spécifier manuellement les mises à jour du logiciel pour corriger les vulnérabilités dans les applications énumérées dans les paramètres de la tâche.

Correction de vulnérabilités dans les applications à l'aide de l'Assistant de correction des vulnérabilités

L'Assistant de correction des vulnérabilités est accessible uniquement en présence d'une licence pour le fonctionnement de Gestion des vulnérabilités et des correctifs.

Pour corriger les vulnérabilités dans les applications à l'aide de l'Assistant de correction des vulnérabilités, procédez comme suit :

1. Dans le menu principal, accédez à **Opérations → Gestion des correctifs → Vulnérabilités dans les applications**.

   Une page contenant une liste des vulnérabilités des logiciels tiers installés sur les appareils administrés s'affiche.

2. Cochez la case en regard de la vulnérabilité que vous souhaitez corriger.

3. Cliquez sur le bouton **Lancer l'Assistant de correction des vulnérabilités**.

   L'Assistant de correction des vulnérabilités s'ouvre. La page **Sélectionnez la tâche de correction de la vulnérabilité** affiche la liste de toutes les tâches existantes des types suivants :

   - *Installation des mises à jour requises et correction des vulnérabilités*
   - *Installation des mises à jour Windows Update*
   - *Corriger les vulnérabilités*

   Vous ne pouvez pas modifier les deux derniers types de tâches pour installer de nouvelles mises à jour. Pour installer de nouvelles mises à jour, vous ne pouvez utiliser que la tâche *Installation des mises à jour requises et correction des vulnérabilités*.

4. Si vous souhaitez que l'assistant affiche uniquement les tâches qui corrigent la vulnérabilité que vous avez sélectionnée, activez l'option **Afficher uniquement les tâches corrigeant la vulnérabilité sélectionnée**.

5. Choisissez la manière dont vous voulez procéder :

   - Pour démarrer une tâche, cochez la case en regard du nom de la tâche, puis cliquez sur le bouton **Démarrer**.
   - Pour ajouter une nouvelle règle à une tâche existante :

     a. Cochez la case en regard du nom de la tâche, puis cliquez sur le bouton **Ajouter une règle**.

     b. Sur la page qui s'ouvre, configurez la nouvelle règle :

     - Règle de correction des vulnérabilités d'un niveau de gravité défini

       Parfois, les mises à jour du logiciel peuvent nuire à l'expérience de l'utilisateur. Dans ce cas, il se peut que vous décidiez d'installer uniquement les mises à jour critiques au fonctionnement du logiciel et d'ignorer les autres.

       Quand cette option est activée, les mises à jour corrigent uniquement les vulnérabilités dont le niveau de gravité, tel que défini par Kaspersky, est égal ou supérieur au niveau de la mise à jour sélectionnée (**Moyenne**, **Élevé** ou **Critique**). Les vulnérabilités dont le niveau de gravité est inférieur à la valeur sélectionnée ne sont pas corrigées.

       Si cette option est désactivée, les mises à jour corrigent toutes les vulnérabilités, quel que soit le niveau de gravité.

       Cette option est Inactif par défaut.

     - **Règle de correction des vulnérabilités au moyen de mises à jour du même type que la mise à jour définie comme recommandée pour la vulnérabilité sélectionnée** (disponible uniquement pour les vulnérabilités dans les applications Microsoft)
     - **Règle de correction des vulnérabilités dans les applications du fournisseur sélectionné** (disponible uniquement pour les vulnérabilités dans les applications tierces)
     - **Règle de correction d'une vulnérabilité dans toutes les versions de l'application sélectionnée** (disponible uniquement pour les vulnérabilités dans les applications tierces)
     - **Règle de correction de la vulnérabilité sélectionnée**
     - Approuver les mises à jour qui corrigent la vulnérabilité sélectionnée

       La mise à jour sélectionnée est approuvée pour l'installation. Activez cette option si certaines règles appliquées de l'installation de la mise à jour autorisent l'installation des mises à jour confirmées uniquement.

       Cette option est Inactif par défaut.

     c. Cliquez sur le bouton **Ajouter**.

   - Pour créer une tâche, procédez comme suit :

     a. Cliquez sur le bouton **Nouvelle tâche**.

     b. Sur la page qui s'ouvre, configurez la nouvelle règle :

- Règle de correction des vulnérabilités d'un niveau de gravité défini

  Parfois, les mises à jour du logiciel peuvent nuire à l'expérience de l'utilisateur. Dans ce cas, il se peut que vous décidiez d'installer uniquement les mises à jour critiques au fonctionnement du logiciel et d'ignorer les autres.

  Quand cette option est activée, les mises à jour corrigent uniquement les vulnérabilités dont le niveau de gravité, tel que défini par Kaspersky, est égal ou supérieur au niveau de la mise à jour sélectionnée (**Moyenne**, **Élevé** ou **Critique**). Les vulnérabilités dont le niveau de gravité est inférieur à la valeur sélectionnée ne sont pas corrigées.

  Si cette option est désactivée, les mises à jour corrigent toutes les vulnérabilités, quel que soit le niveau de gravité.

  Cette option est Inactif par défaut.

- **Règle de correction des vulnérabilités au moyen de mises à jour du même type que la mise à jour définie comme recommandée pour la vulnérabilité sélectionnée** (disponible uniquement pour les vulnérabilités dans les applications Microsoft)

- **Règle de correction des vulnérabilités dans les applications du fournisseur sélectionné** (disponible uniquement pour les vulnérabilités dans les applications tierces)

- **Règle de correction d'une vulnérabilité dans toutes les versions de l'application sélectionnée** (disponible uniquement pour les vulnérabilités dans les applications tierces)

- **Règle de correction de la vulnérabilité sélectionnée**

- Approuver les mises à jour qui corrigent la vulnérabilité sélectionnée

  La mise à jour sélectionnée est approuvée pour l'installation. Activez cette option si certaines règles appliquées de l'installation de la mise à jour autorisent l'installation des mises à jour confirmées uniquement.

  Cette option est Inactif par défaut.

c. Cliquez sur le bouton **Ajouter**.

Si vous avez choisi de démarrer une tâche, vous pouvez fermer l'assistant. La tâche se poursuivra en mode arrière-plan. Il n'y a rien d'autre à faire.

Si vous avez choisi d'ajouter une règle à une tâche existante, la fenêtre des propriétés de la tâche s'ouvre. La nouvelle règle est déjà ajoutée aux propriétés de la tâche. Vous pouvez afficher ou modifier la règle ou d'autres paramètres de tâche. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications.

Si vous avez choisi de créer une tâche, vous continuez à créer la tâche dans l'assistant de création d'une tâche. La nouvelle règle que vous avez ajoutée dans l'Assistant de correction des vulnérabilités s'affiche dans l'Assistant de création d'une tâche. Lorsque vous terminez l'Assistant, la tâche *Installation des mises à jour requises et correction des vulnérabilités* est ajoutée à la liste des tâches.

Création de la tâche Correction des vulnérabilités

La tâche *Corriger les vulnérabilités* vous permet de corriger les vulnérabilités dans les applications sur les appareils administrés qui fonctionnent sous Windows. Vous pouvez corriger les vulnérabilités dans les applications du logiciel tiers, y compris les logiciels Microsoft.

Si vous ne disposez pas de la licence pour le fonctionnement de Gestion des vulnérabilités et des correctifs, vous ne pouvez pas créer de nouvelles tâches de type *Corriger les vulnérabilités*. Pour corriger de nouvelles vulnérabilités, vous pouvez les ajouter à une tâche *Corriger les vulnérabilités* existante. Il est conseillé d'utiliser la tâche *Installation des mises à jour requises et correction des vulnérabilités* plutôt que la tâche *Corriger les vulnérabilités*. La tâche *Installation des mises à jour requises et correction des vulnérabilités* vous permet d'installer plusieurs mises à jour et de corriger automatiquement plusieurs vulnérabilités, selon les règles que vous définissez.

Une interaction utilisateur peut être requise lorsque vous mettez à jour une application tierce ou corrigez une vulnérabilité dans une application tierce sur un appareil administré. Par exemple, l'utilisateur peut être invité à fermer l'application tierce si elle est actuellement ouverte.

Pour créer la tâche Corriger les vulnérabilités, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Tâches**.
2. Cliquez sur **Ajouter**.

   Ceci permet de lancer l'assistant de création d'une tâche. Parcourez les étapes de l'Assistant à l'aide du bouton **Suivant**.
3. Pour l'application Kaspersky Security Center, sélectionnez le type de tâche **Corriger les vulnérabilités**.
4. Spécifiez le nom de la tâche créée.

   Le nom de la tâche ne peut pas contenir plus de 100 symboles et contenir de symboles spéciaux ("*<>?\:|).
5. Sélectionnez les appareils auxquels les tâches seront affectées.
6. Cliquez sur le bouton **Ajouter**.

   La liste des vulnérabilités s'ouvre.
7. Sélectionnez les vulnérabilités que vous souhaitez corriger, puis cliquez sur **OK**.

   Les vulnérabilités dans les applications Microsoft ont généralement des correctifs recommandés. Aucune action supplémentaire n'est requise pour celles-ci. Pour les vulnérabilités dans les applications d'autres fournisseurs, vous devez d'abord définir un correctif utilisateur pour chaque vulnérabilité que vous souhaitez corriger. Par après, vous pourrez ajouter ces vulnérabilités dans la tâche *Corriger les vulnérabilités*.

8. Définissez les paramètres de redémarrage du système d'exploitation :

- **Ne pas redémarrer l'appareil**

  Les appareils clients ne redémarrent pas automatiquement après l'opération. Pour arrêter le fonctionnement, il faut redémarrer l'appareil (par exemple, manuellement ou à l'aide d'une tâche d'administration des appareils). Les informations sur la nécessité du redémarrage sont enregistrées dans les résultats de la tâche et dans l'état de l'appareil. Cette option convient aux tâches d' sur les serveurs et autres appareils pour lesquels la continuité des opérations est critique.

- **Redémarrer l'appareil**

  Dans ce cas, le redémarrage des appareils clients est toujours exécuté automatiquement, si celui-ci est requis pour terminer l'opération. Cette option convient aux tâches d' sur des appareils pour lesquels des interruptions périodiques sont admises (débranchement, redémarrage).

- **Confirmer l'action auprès de l'utilisateur**

  Le message qui signale que l'appareil client doit être redémarré manuellement s'affiche sur l'écran de l'appareil. Pour cette option, il est possible de configurer des paramètres avancés : le texte du message pour l'utilisateur, la fréquence du message, ainsi que le délai à l'issue duquel le redémarrage sera forcé (sans confirmation de l'utilisateur). Cette option convient le mieux pour les postes de travail sur lesquels les utilisateurs doivent pouvoir sélectionner l'heure de redémarrage qui leur convient le mieux.

  Cette option est sélectionnée par défaut.

- **Répéter la demande toutes les (min.)**

  Quand cette option est activée, l'application invite l'utilisateur à redémarrer le système d'exploitation selon la fréquence indiquée.

  Cette option est activée par défaut. L'intervalle par défaut est de 5 minutes. La valeur peut être comprise entre 1 et 1 440 minutes.

  Si cette option est désactivée, l'invite est affichée une seule fois.

- **Redémarrer le système au bout de (min.)**

  Après avoir averti l'utilisateur, l'application force le redémarrage du système d'exploitation à l'issue de l'intervalle défini.

  Cette option est activée par défaut. Le délai par défaut est de 30 minutes. La valeur peut être comprise entre 1 et 1 440 minutes.

- **Forcer la fermeture des applications dans les sessions bloquées**

Les applications en cours d'exécution peuvent empêcher le redémarrage de l'appareil client. Par exemple, si un document est en train d'être modifié dans un logiciel de traitement de texte et qu'il n'est pas enregistré, l'application n'autorise pas le redémarrage de l'appareil.

Quand cette option est activée, l'arrêt forcé de ces applications sur un appareil verrouillé doit avoir lieu avant de pouvoir redémarrer l'appareil. Les utilisateurs pourraient perdre toute modification qui n'a pas été enregistrée à ce moment.

Si cette option est désactivée, un appareil verrouillé n'est pas redémarré. L'état de la tâche sur cet appareil indique qu'il faut redémarrer l'appareil. Les utilisateurs doivent quitter manuellement toutes les applications en cours d'exécution sur les appareils verrouillés, puis redémarrer ces appareils.

Cette option est Inactif par défaut.

9. Définissez les paramètres du compte :

- **Compte par défaut**

  La tâche sera lancée sous le même compte utilisateur sous lequel l'application, exécutant cette tâche, a été installée et lancée.

  Cette option est sélectionnée par défaut.

- **Indiquer un compte**

  Remplissez les champs **Compte utilisateur** et **Mot de passe** pour définir les détails d'un compte à partir duquel la tâche est exécutée. Le compte doit disposer de droits suffisants pour cette tâche.

- **Compte utilisateur**

  Le compte utilisateur au nom duquel la tâche sera lancée.

- **Mot de passe**

  Mot de passe du compte utilisateur au nom duquel la tâche sera lancée.

10. Si vous souhaitez modifier les paramètres de la tâche par défaut, activez l'option **Ouvrir les détails de la tâche à la fin de la création** sur la page **Fin de la création de la tâche**. Si vous n'activez pas cette tâche, la tâche est créée selon les paramètres par défaut. Vous pourrez modifier ces paramètres par défaut plus tard, à tout moment.

11. Cliquez sur le bouton **Terminer**.

    La tâche est créée et s'affiche dans la liste des tâches.

12. Cliquez sur le nom de la tâche créée pour ouvrir la fenêtre de propriétés de la tâche.

13. Dans la fenêtre des propriétés de la tâche, indiquez les paramètres généraux de la tâche en fonction de vos besoins.

14. Cliquez sur le bouton **Enregistrer**.

La tâche est créée et configurée.

Création de la tâche Installer les mises à jour requises et corriger les vulnérabilités

La tâche *Installation des mises à jour requises et correction des vulnérabilités* est accessible uniquement en présence d'une licence pour le fonctionnement de Gestion des vulnérabilités et des correctifs.

La tâche *Installation des mises à jour requises et correction des vulnérabilités* est utilisée pour effectuer les mises à jour et réparer les vulnérabilités de logiciels tiers, y compris les logiciels Microsoft, installés sur les appareils administrés. Cette tâche vous permet d'installer plusieurs mises à jour et de corriger différentes vulnérabilités en fonction de certaines règles.

Pour installer des mises à jour ou corriger des vulnérabilités à l'aide de la tâche *Installation des mises à jour requises et correction des vulnérabilités*, vous pouvez effectuer l'une des opérations suivantes :

- Exécutez l'assistant d'installation des mises à jour ou l'assistant de correction des vulnérabilités.
- Créez une tâche *Installation des mises à jour requises et correction des vulnérabilités*.
- Ajoutez une règle pour l'installation de la mise à jour à une tâche *Installation des mises à jour requises et correction des vulnérabilités* existante.

Pour créer une tâche Installation des mises à jour requises et correction des vulnérabilités :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Tâches**.
2. Cliquez sur **Ajouter**.

   Ceci permet de lancer l'assistant de création d'une tâche. Suivez les étapes de l'assistant.
3. Pour l'application Kaspersky Security Center, sélectionnez le type de tâche **Installation des mises à jour requises et correction des vulnérabilités**.

   Si la tâche ne s'affiche pas, vérifiez si votre compte dispose des privilèges **Lire**, **Modifier** et **Exécuter** pour la zone fonctionnelle **Administration du système** : **Gestion des vulnérabilités et des correctifs** Vous ne pouvez pas créer et configurer la tâche *Installation des mises à jour requises et correction des vulnérabilités* sans ces droits d'accès.
4. Spécifiez le nom de la tâche créée. Le nom de la tâche ne peut pas contenir plus de 100 symboles et contenir de symboles spéciaux ("*<>?\:|).
5. Sélectionnez les appareils auxquels les tâches seront affectées.

6. Indiquez les règles d'installation des mises à jour, puis définissez les paramètres suivants :

- **Commencer l'installation au moment du redémarrage ou de l'arrêt de l'appareil**

  Si cette option est activée, les mises à jour sont installées lors du redémarrage ou de l'arrêt de l'appareil. Dans le cas contraire, les mises à jour sont installées selon la programmation.

  Utilisez cette option si l'installation des mises à jour peut avoir un impact sur les performances de l'appareil.

  Cette option est Inactif par défaut.

- **Installer les modules système général requis**

  Si cette option est activée, l'application, avant d'installer une mise à jour, installe automatiquement tous les composants généraux système (prérequis) requis pour l'installation de la mise à jour. Par exemple, il peut s'agir des mises à jour du système d'exploitation.

  Si cette option est désactivée, vous devrez peut-être installer les prérequis manuellement.

  Cette option est Inactif par défaut.

- **Autoriser l'installation de nouvelles versions de l'application lors des mises à jour**

  Si cette option est activée, les mises à jour sont autorisées lorsqu'elles entraînent l'installation d'une nouvelle version d'un logiciel.

  Si cette option est désactivée, le logiciel n'est pas mis à jour. Vous pouvez alors installer les nouvelles versions du logiciel manuellement ou via un autre tâche. Par exemple, vous pouvez utiliser cette option si l'infrastructure de votre entreprise n'est pas prise en charge par une nouvelle version du logiciel ou si vous souhaitez vérifier une mise à jour dans une infrastructure d'essai.

  Cette option est activée par défaut.

  > La mise à jour d'une application peut provoquer un dysfonctionnement des applications dépendantes installées sur les appareils clients.

- **Télécharger les mises à jour sur l'appareil sans les installer**

  Quand cette option est activée, l'application télécharge les mises à jour sur l'appareil, mais ne les installe pas automatiquement. Vous pouvez installer les mises à jour manuellement par la suite.

  Les mises à jour Microsoft sont téléchargées dans le stockage Windows système. Les mises à jour des produits tiers (applications développées par des éditeurs d'application autres que Kaspersky et Microsoft) sont téléchargées dans le dossier indiqué dans le champ **Télécharger les mises à jour sur**.

  Si cette option est désactivée, les mises à jour sont installées automatiquement sur l'appareil.

  Cette option est Inactif par défaut.

- **Télécharger les mises à jour sur**

  Ce dossier est utilisé dans le cadre du téléchargement des mises à jour de produits tiers (applications développées par des éditeurs de logiciels autres que Kaspersky et Microsoft).

- **Activer le diagnostic avancé**

Quand cette fonction est activée, l'Agent d'administration enregistre des fichiers de trace même si l'écriture de fichiers de trace est désactivée pour l'Agent d'administration dans l'utilitaire de diagnostic à distance Kaspersky Security Center. Les traces sont enregistrées dans deux fichiers en alternance la taille de chacun de ces fichiers est déterminée par la valeur paramètre **Taille maximale (Mo) des fichiers de diagnostic avancé**. Quand les deux fichiers sont remplis, l'Agent d'administration écrit à nouveau dans ceux-ci. Les fichiers avec les traces sont stockés dans le dossier %WINDIR%\Temp. Ces fichiers sont accessibles dans l'utilitaire de diagnostic à distance, vous pouvez les télécharger ou les supprimer à cet endroit.

Quand cette fonction est désactivée, l'Agent d'administration enregistre les traces conformément aux paramètres définis dans l'utilitaire de diagnostic à distance Kaspersky Security Center. Aucune trace complémentaire n'est écrite.

Lors de la création d'une tâche, il n'est pas nécessaire d'activer le diagnostic avancé. Par contre, vous pouvez activer cette fonction plus tard si, par exemple, une tâche échoue sur certains appareils et que vous souhaitez obtenir des informations complémentaires lors d'une autre exécution de la tâche.

Cette option est Inactif par défaut.

- **Taille maximale (Mo) des fichiers de diagnostic avancé**

  La valeur par défaut est de 100 Mo, mais elle peut se situer entre 1 et 2 048 Mo. Il peut arriver qu'un expert du Support Technique de Kaspersky vous demande de modifier la valeur par défaut lorsque les informations reprises dans les fichiers de diagnostic avancés que vous avez envoyés ne suffisent pas pour résoudre le problème.

7. Définissez les paramètres de redémarrage du système d'exploitation :

- **Ne pas redémarrer l'appareil**

  Les appareils clients ne redémarrent pas automatiquement après l'opération. Pour arrêter le fonctionnement, il faut redémarrer l'appareil (par exemple, manuellement ou à l'aide d'une tâche d'administration des appareils). Les informations sur la nécessité du redémarrage sont enregistrées dans les résultats de la tâche et dans l'état de l'appareil. Cette option convient aux tâches d' sur les serveurs et autres appareils pour lesquels la continuité des opérations est critique.

- **Redémarrer l'appareil**

  Dans ce cas, le redémarrage des appareils clients est toujours exécuté automatiquement, si celui-ci est requis pour terminer l'opération. Cette option convient aux tâches d' sur des appareils pour lesquels des interruptions périodiques sont admises (débranchement, redémarrage).

- **Confirmer l'action auprès de l'utilisateur**

  Le message qui signale que l'appareil client doit être redémarré manuellement s'affiche sur l'écran de l'appareil. Pour cette option, il est possible de configurer des paramètres avancés : le texte du message pour l'utilisateur, la fréquence du message, ainsi que le délai à l'issue duquel le redémarrage sera forcé (sans confirmation de l'utilisateur). Cette option convient le mieux pour les postes de travail sur lesquels les utilisateurs doivent pouvoir sélectionner l'heure de redémarrage qui leur convient le mieux.

  Cette option est sélectionnée par défaut.

- **Répéter la demande toutes les (min.)**

  Quand cette option est activée, l'application invite l'utilisateur à redémarrer le système d'exploitation selon la fréquence indiquée.

  Cette option est activée par défaut. L'intervalle par défaut est de 5 minutes. La valeur peut être comprise entre 1 et 1 440 minutes.

  Si cette option est désactivée, l'invite est affichée une seule fois.

- **Redémarrer le système au bout de (min.)**

  Après avoir averti l'utilisateur, l'application force le redémarrage du système d'exploitation à l'issue de l'intervalle défini.

  Cette option est activée par défaut. Le délai par défaut est de 30 minutes. La valeur peut être comprise entre 1 et 1 440 minutes.

- **Délai d'attente avant la fermeture forcée des ap&plications dans les sessions bloquées (min)**

  Arrêt forcé des applications lorsque l'appareil de l'utilisateur est verrouillé (arrêt manuel ou automatique après une période d'inactivité).

  Si cette option est activée, les applications en cours sur l'appareil verrouillé seront fermées de force à la fin du délai indiqué dans le champ situé à côté de la case.

  Si cette option est activée, les applications en cours sur l'appareil verrouillé ne seront pas fermées.

  Cette option est Inactif par défaut.

8. Si vous souhaitez modifier les paramètres de la tâche par défaut, activez l'option **Ouvrir les détails de la tâche à la fin de la création** sur la page **Fin de la création de la tâche**. Si vous n'activez pas cette tâche, la tâche est créée selon les paramètres par défaut. Vous pourrez modifier ces paramètres par défaut plus tard, à tout moment.

9. Cliquez sur le bouton **Terminer**.

   La tâche est créée et s'affiche dans la liste des tâches.

10. Cliquez sur le nom de la tâche créée pour ouvrir la fenêtre de propriétés de la tâche.

11. Dans la fenêtre des propriétés de la tâche, indiquez les paramètres généraux de la tâche en fonction de vos besoins.

12. Cliquez sur le bouton **Enregistrer**.

    La tâche est créée et configurée.

Si les résultats de la tâche contiennent un avertissement concernant l'erreur 0x80240033 " Erreur de l'agent de mise à jour Windows 80240033 (" Les conditions de licence n'ont pas pu être téléchargées ") ", vous pouvez résoudre ce problème via le registre Windows.

Ajout de règles pour l'installation de la mise à jour

Cette fonctionnalité est accessible uniquement en présence d'une licence pour le fonctionnement de Gestion des vulnérabilités et des correctifs.

Lors de l'installation de mises à jour logicielles ou de la correction de vulnérabilités dans les applications à l'aide de la tâche *Installation des mises à jour requises et correction des vulnérabilités*, vous devez définir les règles pour l'installation de la mise à jour. Ces règles déterminent les mises à jour à installer et les vulnérabilités à corriger.

Les paramètres exacts dépendent de l'objet pour lequel vous ajoutez une règle : pour toutes les mises à jour, pour les mises à jour Windows Update ou pour les mises à jour d'applications tierces (applications développées par des éditeurs autres que Kaspersky et Microsoft). Lors de l'ajout d'une règle pour des mises à jour Windows Update ou des mises à jour d'applications tierces, vous pouvez sélectionner des applications spécifiques et les versions de l'application pour lesquelles vous souhaitez installer les mises à jour. Lors de l'ajout d'une règle pour toutes les mises à jour, vous pouvez sélectionner les mises à jour spécifiques que vous souhaitez installer et les vulnérabilités que vous souhaitez éliminer via l'installation des mises à jour.

Vous pouvez ajouter une règle pour l'installation de la mise à jour comme suit :

- En ajoutant une règle lors de la création d'une nouvelle tâche Installation des mises à jour requises et correction des vulnérabilités.
- En ajoutant une règle sous l'onglet **Paramètres de l'application** dans la fenêtre des propriétés d'une tâche *Installation des mises à jour requises et correction des vulnérabilités* existante.
- Via l'assistant d'installation des mises à jour ou l'assistant de correction des vulnérabilités.

Pour ajouter une nouvelle règle pour toutes les mises à jour, procédez comme suit :

1. Cliquez sur le bouton **Ajouter**.

   L'Assistant de création de règles se lance. Parcourez les étapes de l'assistant à l'aide du bouton **Suivant**.

2. Sur la page **Type de règle**, sélectionnez **Règle pour toutes les mises à jour**.

3. Sur la page **Critères généraux**, utilisez les listes déroulantes pour définir les paramètres suivants :

   - **Définir les mises à jour à installer**

     Sélectionnez les mises à jour qui doivent être installées sur les appareils clients :

     - **Installer uniquement les mises à jour confirmées**. Cette option installe uniquement les mises à jour confirmées.
     - **Installer toutes les mises à jour (sauf les mises à jour rejetées)**. Cette option installe les mises à jour avec l'état *Approuvé* ou *Non défini*.
     - **Installer toutes les mises à jour (y compris les mises à jour rejetées)**. Ceci installe toutes les mises à jour, quel que soit leur état d'approbation. Sélectionnez cette option avec prudence. Par exemple, utilisez cette option si vous souhaitez vérifier l'installation de certaines mises à jour rejetées dans une infrastructure d'essai.

   - **Corriger les vulnérabilités de niveau de gravité égal ou supérieur à**

     Parfois, les mises à jour du logiciel peuvent nuire à l'expérience de l'utilisateur. Dans ce cas, il se peut que vous décidiez d'installer uniquement les mises à jour critiques au fonctionnement du logiciel et d'ignorer les autres.

     Quand cette option est activée, les mises à jour corrigent uniquement les vulnérabilités dont le niveau de gravité tel que défini par Kaspersky est égal ou supérieur à la valeur sélectionnée dans la liste (**Moyenne**, **Élevé** ou **Critique**). Les vulnérabilités dont le niveau de gravité est inférieur à la valeur sélectionnée ne sont pas corrigées.

     Si cette option est désactivée, les mises à jour corrigent toutes les vulnérabilités, quel que soit le niveau de gravité.

     Cette option est Inactif par défaut.

4. Sur la page **Mises à jour**, sélectionnez les mises à jour à installer :

- **Installer toutes les mises à jour convenables**

  Installez toutes les mises à jour du logiciel qui répondent aux critères définis à la page **Critères généraux** de l'assistant. Sélectionné par défaut.

- **Installer uniquement les mises à jour depuis la liste**

  Installer uniquement les mises à jour du logiciel que vous sélectionnez manuellement dans la liste. Cette liste contient toutes les mises à jour du logiciel disponibles.

  Par exemple, vous pouvez sélectionner des mises à jour spécifiques dans les cas suivants : pour vérifier leur installation dans un environnement d'essai, pour mettre à jour uniquement les applications critiques ou pour mettre à jour uniquement certaines applications.

  - **&Installer automatiquement toutes les mises à jour précédentes des applications nécessaires à l'installation des mises à jour sélectionnées**

    Conservez cette option si vous acceptez l'installation de versions de l'application intermédiaires quand l'impose l'installation des mises à jour sélectionnées.

    Si vous désactivez cette option, seules les versions sélectionnées des applications sont installées. Désactivez cette option si vous souhaitez mettre à jour les applications d'une manière directe, sans tenter d'installer les versions successives. S'il est impossible d'installer les mises à jour sélectionnées sans installer les versions antérieures de l'application, la mise à jour de l'application échoue.

    Admettons que la version 3 d'une application est installée sur un appareil et vous souhaitez réaliser la mise à jour jusque la version 5, mais la version 5 de cette application peut être installée uniquement sur la version 4. Quand cette option est installée, le logiciel installe d'abord la version 4, puis la version 5. Si l'option est désactivée, le logiciel ne parvient pas à mettre l'application à jour.

    Cette option est activée par défaut.

5. Sur la page **Vulnérabilités**, sélectionnez les vulnérabilités que seront corrigées suite à l'installation des mises à jour sélectionnées :

- **Corriger toutes les vulnérabilités qui correspondent aux autres critères**

  Corrigez toutes les vulnérabilités qui satisfont les critères définis à la page **Critères généraux** de l'assistant. Sélectionné par défaut.

- **Corriger uniquement les vulnérabilités depuis la liste**

  Corrigez uniquement les vulnérabilités que vous sélectionnez manuellement dans la liste. Cette liste contient toutes les vulnérabilités détectées.

  Par exemple, vous pouvez sélectionner des vulnérabilités spécifiques dans les cas suivants : pour vérifier les corrections dans un environnement d'essai, pour corriger les vulnérabilités uniquement dans les applications critiques ou pour corriger les vulnérabilités uniquement dans certaines applications.

6. La page **Nom** permet de renseigner le nom de la règle ajoutée. Vous pouvez changer ce nom plus tard dans la section **Paramètres** de la fenêtre des propriétés de la tâche créée.

Une fois que l'assistant de création de règles a terminé, la nouvelle règle est ajoutée et s'affiche dans la liste des règles de l'assistant de création d'une tâche ou dans les propriétés de la tâche.

Pour ajouter une nouvelle règle pour les mises à jour de Windows Update, procédez comme suit :

1. Cliquez sur le bouton **Ajouter**.

   L'Assistant de création de règles se lance. Parcourez les étapes de l'assistant à l'aide du bouton **Suivant**.

2. Sur la page **Type de règle**, sélectionnez **Règle pour les mises à jour Windows Update**.

3. Dans la fenêtre **Conditions générales**, configurez les paramètres suivants :

   - **Définir les mises à jour à installer**

     Sélectionnez les mises à jour qui doivent être installées sur les appareils clients :

     - **Installer uniquement les mises à jour confirmées**. Cette option installe uniquement les mises à jour confirmées.
     - **Installer toutes les mises à jour (sauf les mises à jour rejetées)**. Cette option installe les mises à jour avec l'état *Approuvé* ou *Non défini*.
     - **Installer toutes les mises à jour (y compris les mises à jour rejetées)**. Ceci installe toutes les mises à jour, quel que soit leur état d'approbation. Sélectionnez cette option avec prudence. Par exemple, utilisez cette option si vous souhaitez vérifier l'installation de certaines mises à jour rejetées dans une infrastructure d'essai.

   - **Corriger les vulnérabilités de niveau de gravité égal ou supérieur à**

     Parfois, les mises à jour du logiciel peuvent nuire à l'expérience de l'utilisateur. Dans ce cas, il se peut que vous décidiez d'installer uniquement les mises à jour critiques au fonctionnement du logiciel et d'ignorer les autres.

     Quand cette option est activée, les mises à jour corrigent uniquement les vulnérabilités dont le niveau de gravité tel que défini par Kaspersky est égal ou supérieur à la valeur sélectionnée dans la liste (**Moyenne**, **Élevé** ou **Critique**). Les vulnérabilités dont le niveau de gravité est inférieur à la valeur sélectionnée ne sont pas corrigées.

     Si cette option est désactivée, les mises à jour corrigent toutes les vulnérabilités, quel que soit le niveau de gravité.

     Cette option est Inactif par défaut.

   - **Corriger les vulnérabilités qui présentent un niveau de gravité selon MSRC égal ou supérieur à**

     Parfois, les mises à jour du logiciel peuvent nuire à l'expérience de l'utilisateur. Dans ce cas, il se peut que vous décidiez d'installer uniquement les mises à jour critiques au fonctionnement du logiciel et d'ignorer les autres.

     Quand cette option est activée, les mises à jour corrigent uniquement les vulnérabilités dont le niveau de gravité tel que défini par Microsoft Security Response Center (MSRC) est égal ou supérieur à la valeur sélectionnée dans la liste (**Bas**, **Moyenne**, **Élevé** ou **Critique**). Les vulnérabilités dont le niveau de gravité est inférieur à la valeur sélectionnée ne sont pas corrigées.

     Si cette option est désactivée, les mises à jour corrigent toutes les vulnérabilités, quel que soit le niveau de gravité.

     Cette option est Inactif par défaut.

4. Sur la page **Applications**, sélectionnez les applications et les versions des applications pour lesquelles vous voulez installer les mises à jour. Toutes les applications sont cochées par défaut.

5. Sur la page **Catégorie des mises à jour**, sélectionnez les catégories des mises à jour à installer. Ces catégories sont les mêmes que dans le catalogue Microsoft Update. Toutes les catégories sont cochées par défaut.

6. La page **Nom** permet de renseigner le nom de la règle ajoutée. Vous pouvez changer ce nom plus tard dans la section **Paramètres** de la fenêtre des propriétés de la tâche créée.

Une fois que l'assistant de création de règles a terminé, la nouvelle règle est ajoutée et s'affiche dans la liste des règles de l'assistant de création d'une tâche ou dans les propriétés de la tâche.

Pour ajouter une règle pour les mises à jour des produits tiers, procédez comme suit :

1. Cliquez sur le bouton **Ajouter**.

   L'Assistant de création de règles se lance. Parcourez les étapes de l'assistant à l'aide du bouton **Suivant**.

2. Sur la page **Type de règle**, sélectionnez **Règles pour les mises à jour tierces**.

3. Dans la fenêtre **Conditions générales**, configurez les paramètres suivants :

   - **Définir les mises à jour à installer**

     Sélectionnez les mises à jour qui doivent être installées sur les appareils clients :

     - **Installer uniquement les mises à jour confirmées**. Cette option installe uniquement les mises à jour confirmées.
     - **Installer toutes les mises à jour (sauf les mises à jour rejetées)**. Cette option installe les mises à jour avec l'état *Approuvé* ou *Non défini*.
     - **Installer toutes les mises à jour (y compris les mises à jour rejetées)**. Ceci installe toutes les mises à jour, quel que soit leur état d'approbation. Sélectionnez cette option avec prudence. Par exemple, utilisez cette option si vous souhaitez vérifier l'installation de certaines mises à jour rejetées dans une infrastructure d'essai.

   - **Corriger les vulnérabilités de niveau de gravité égal ou supérieur à**

     Parfois, les mises à jour du logiciel peuvent nuire à l'expérience de l'utilisateur. Dans ce cas, il se peut que vous décidiez d'installer uniquement les mises à jour critiques au fonctionnement du logiciel et d'ignorer les autres.

     Quand cette option est activée, les mises à jour corrigent uniquement les vulnérabilités dont le niveau de gravité tel que défini par Kaspersky est égal ou supérieur à la valeur sélectionnée dans la liste (**Moyenne**, **Élevé** ou **Critique**). Les vulnérabilités dont le niveau de gravité est inférieur à la valeur sélectionnée ne sont pas corrigées.

     Si cette option est désactivée, les mises à jour corrigent toutes les vulnérabilités, quel que soit le niveau de gravité.

     Cette option est Inactif par défaut.

4. Sur la page **Applications**, sélectionnez les applications et les versions des applications pour lesquelles vous voulez installer les mises à jour. Toutes les applications sont cochées par défaut.

5. La page **Nom** permet de renseigner le nom de la règle ajoutée. Vous pouvez changer ce nom plus tard dans la section Paramètres de la fenêtre des propriétés de la tâche créée.

Une fois que l'assistant de création de règles a terminé, la nouvelle règle est ajoutée et s'affiche dans la liste des règles de l'assistant de création d'une tâche ou dans les propriétés de la tâche.

Sélection des correctifs utilisateur pour les vulnérabilités dans le logiciel tiers

Pour utiliser la tâche *Corriger les vulnérabilités*, vous devez spécifier manuellement les mises à jour logicielles visant à corriger les vulnérabilités logicielles tierces répertorié dans les paramètres de la tâche. La tâche *Corriger les vulnérabilités* utilise les correctifs recommandés pour les logiciels Microsoft et les correctifs utilisateur pour d'autres logiciels tiers. Les *correctifs des utilisateurs* sont des mises à jour logicielles corrigeant les vulnérabilités pour lesquelles l'administrateur a précisé manuellement qu'elles sont à installer.

Pour sélectionner les correctifs des vulnérabilités dans les logiciels tiers :

1. Dans le menu principal, accédez à **Opérations → Gestion des correctifs → Vulnérabilités dans les applications**.

   La page affiche la liste des vulnérabilités logicielles détectées sur les appareils client.

2. Cliquez sur le lien portant le nom des vulnérabilités dans les applications pour laquelle vous souhaitez spécifier un correctif utilisateur.

   La fenêtre des propriétés de la vulnérabilité s'ouvre.

3. Dans le volet gauche, sélectionnez la section **Correctifs utilisateurs et autres**.

   La liste des correctifs utilisateur pour la vulnérabilité logicielle sélectionnée s'affiche.

4. Cliquez sur **Ajouter**.

   Une liste des paquets d'installation disponibles s'affiche. La liste des paquets d'installation affichés correspond à la liste **Opérations → Stockages → Paquets d'installation**. Si vous n'avez pas créé de paquet d'installation contenant un correctif utilisateur pour la vulnérabilité sélectionnée, vous pouvez créer le paquet maintenant en démarrant l'Assistant de création du paquet d'installation.

5. Sélectionnez un ou des paquets d'installation contenant un ou des correctifs utilisateurs pour la vulnérabilité du logiciel tiers.

6. Cliquez sur **Enregistrer**.

Les paquets d'installation contenant les correctifs utilisateur pour la vulnérabilité logicielle sont spécifiés. Lorsque la tâche *Corriger les vulnérabilités* est lancée, le paquet d'installation est installé et la vulnérabilité logicielle est corrigée.

Consultation des informations relatives aux vulnérabilités dans les applications sur tous les appareils administrés

Une fois que vous avez analysé les applications des appareils administrés à la recherche de vulnérabilités, vous pouvez consulter la liste des vulnérabilités dans les applications détectées sur tous les appareils administrés. Si vous exécutez la tâche pour la hiérarchie des Serveurs d'administration, vous pouvez consulter la liste des appareils administrés pour lesquels des vulnérabilités ont été détectées uniquement pour le Serveur d'administration sélectionné.

Pour consulter la liste des vulnérabilités dans les applications détectées sur tous les appareils administrés,

Dans le menu principal, accédez à **Opérations → Gestion des correctifs → Vulnérabilités dans les applications**.

La page affiche la liste des vulnérabilités logicielles détectées sur les appareils client.

Vous pouvez également générer et consulter le rapport sur les vulnérabilités.

Vous pouvez indiquer un filtre pour consulter la liste des vulnérabilités dans les applications. Cliquez sur l'icône **Filtrer** () dans le coin supérieur droit de la liste des vulnérabilités dans les applications pour gérer le filtre. Vous pouvez également sélectionner l'un des filtres prédéfinis dans la liste déroulante **Filtres prédéfinis** située au-dessus de la liste des vulnérabilités dans les applications.

Vous pouvez obtenir des informations détaillées sur n'importe quelle vulnérabilité de la liste.

Pour obtenir des informations sur une vulnérabilité dans une application :

Cliquez sur le lien avec le nom de la vulnérabilité dans la liste des vulnérabilités dans les applications.

La fenêtre des propriétés de la vulnérabilité dans l'application s'ouvre.

Consultation des informations relatives aux vulnérabilités dans les applications sur l'appareil administré sélectionné

Vous pouvez consulter les informations relatives aux vulnérabilités dans les applications sur l'appareil administré sélectionné sous Windows.

Pour afficher la liste des vulnérabilités logicielles détectées sur l'appareil administré sélectionné :

1. Dans le menu principal, accédez à **Ressources (Appareils) → Appareils administrés**.

   La liste des appareils administrés s'affiche.

2. Dans la liste des appareils administrés, cliquez sur le lien portant le nom de l'appareil pour lequel vous souhaitez afficher les vulnérabilités dans les applications détectées.

   La fenêtre des propriétés de l'appareil sélectionné s'affiche.

3. Dans la fenêtre des propriétés de l'appareil sélectionné, ouvrez l'onglet **Avancé**.

4. Dans le volet gauche, sélectionnez la section **Vulnérabilités dans les applications**.

   La liste des vulnérabilités dans les applications détectées sur l'appareil administré sélectionné s'affiche.

Pour consulter les propriétés de la vulnérabilité dans l'application sélectionnée,

cliquez sur le lien avec le nom de la vulnérabilité dans l'application dans la liste des vulnérabilités dans les applications.

La fenêtre des propriétés de la vulnérabilité dans l'application sélectionnée s'affiche.

Consultation des statistiques relatives aux vulnérabilités sur les appareils administrés

Vous pouvez consulter les statistiques pour chaque vulnérabilité dans les applications des appareils administrés. Les statistiques sont représentées sous forme de diagramme. Le diagramme affiche le nombre d'appareils ayant les états suivants :

- *Ignorée sur : <nombre d'appareils>*. Cet état est attribué si vous avez réglé manuellement l'option d'ignorer la vulnérabilité dans les propriétés de cette dernière.
- *Corrigée sur : <nombre d'appareils>*. Cet état est attribué si la tâche visant à corriger la vulnérabilité est terminée avec succès.
- *Correctif prévu sur : <nombre d'appareils>*. Cet état est attribué si vous avez créé la tâche visant à corriger la vulnérabilité, mais qu'elle n'a pas encore été effectuée.
- *Correctif appliqué sur : <nombre d'appareils>*. Cet état est attribué si vous avez sélectionné manuellement la mise à jour du logiciel pour corriger la vulnérabilité, mais que cette mise à jour n'a pas corrigé la vulnérabilité.
- *Correctif nécessaire sur : <nombre d'appareils>*. Cet état est attribué si la vulnérabilité a été corrigée uniquement sur certains appareils administrés et si la correction de la vulnérabilité est nécessaire sur d'autres appareils.

Pour consulter les statistiques d'une vulnérabilité sur les appareils administrés :

1. Dans le menu principal, accédez à **Opérations → Gestion des correctifs → Vulnérabilités dans les applications**.

   La page affiche une liste des vulnérabilités dans les applications détectées sur les appareils administrés.

2. Cochez la case à côté de la vulnérabilité requise.

3. Cliquez sur le bouton **Statistiques de vulnérabilité sur les appareils**.

Un diagramme des états de la vulnérabilité s'affiche. Cliquer sur un état ouvre une liste des appareils sur lesquels la vulnérabilité possède l'état sélectionné.

Exportation de la liste des vulnérabilités dans les applications vers un fichier

Vous pouvez exporter la liste des vulnérabilités affichées au format CSV ou TXT. Vous pouvez par exemple utiliser ces fichiers pour les envoyer à votre responsable de la sécurité de l'information ou les stocker à des fins statistiques.

Pour exporter la liste des vulnérabilités dans les applications détectées sur tous les appareils administrés dans un fichier texte :

1. Dans le menu principal, accédez à **Opérations → Gestion des correctifs → Vulnérabilités dans les applications**.

   La page affiche une liste des vulnérabilités dans les applications détectées sur les appareils administrés.

2. Cliquez sur le bouton **Exporter vers un fichier TXT** ou **Exporter vers un fichier CSV** en fonction du format que vous préférez exporter.

Le fichier contenant la liste des vulnérabilités dans les applications est téléchargé sur l'appareil que vous utilisez actuellement.

Pour exporter la liste des vulnérabilités dans les applications détectées sur l'appareil administré sélectionné dans un fichier texte :

1. ouvrez la liste des vulnérabilités dans les applications détectées sur l'appareil administré sélectionné.
2. Sélectionnez les vulnérabilités dans les applications que vous souhaitez exporter.

   Ignorez cette étape si vous souhaitez exporter une liste complète des vulnérabilités dans les applications détectées sur l'appareil administré.

   Si vous souhaitez exporter la liste complète des vulnérabilités dans les applications détectées sur l'appareil administré, seules les vulnérabilités affichées sur la page actuelle seront exportées.
3. Cliquez sur le bouton **Exporter vers un fichier TXT** ou **Exporter vers un fichier CSV** en fonction du format que vous préférez exporter.

Le fichier contenant la liste des vulnérabilités dans les applications détectées sur l'appareil administré sélectionné est téléchargé sur l'appareil que vous utilisez actuellement.

Ignorer les vulnérabilités dans les applications

Vous pouvez ignorer les vulnérabilités dans les applications à corriger. Par exemple, les raisons d'ignorer les vulnérabilités dans les applications peuvent être les suivantes :

- Vous ne considérez pas la vulnérabilité dans l'application comme critique pour votre entreprise.
- Vous savez que la correction de la vulnérabilité dans l'application peut endommager les données relatives au logiciel pour lequel la correction de la vulnérabilité était nécessaire.
- Vous êtes sûr que la vulnérabilité dans l'application n'est pas dangereuse pour le réseau de votre entreprise car vous utilisez d'autres mesures pour protéger vos appareils administrés.

Vous pouvez ignorer une vulnérabilité dans une application sur tous appareils administrés ou seulement sur les appareils administrés sélectionnés.

Pour ignorer une vulnérabilité dans une application sur tous les appareils administrés :

1. Dans le menu principal, accédez à **Opérations → Gestion des correctifs → Vulnérabilités dans les applications**.

   La page affiche la liste des vulnérabilités dans les applications détectées sur les appareils administrés.
2. Cliquez sur le lien portant le nom de la vulnérabilité dans une application que vous souhaitez ignorer dans la liste des vulnérabilités dans les applications.

   La fenêtre des propriétés des vulnérabilités dans les applications s'ouvre.
3. Sous l'onglet **Général**, activez l'option **Ignorer la vulnérabilité**.
4. Cliquez sur le bouton **Enregistrer**.

   La fenêtre des propriétés de la vulnérabilité dans l'application se ferme.

La vulnérabilité dans l'application est ignorée sur les appareils administrés.

Pour ignorer une vulnérabilité dans l'application sur l'appareil administré sélectionné :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Appareils administrés**.

   La liste des appareils administrés s'affiche.

2. Dans la liste des appareils administrés, cliquez sur le lien portant le nom de l'appareil pour lequel vous souhaitez ignorer une vulnérabilité dans une application.

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

3. Dans la fenêtre des propriétés de la Appareil, sélectionnez l'onglet **Avancé**.

4. Dans le volet gauche, sélectionnez la section **Vulnérabilités dans les applications**.

   La liste des vulnérabilités dans les applications détectées sur l'appareil s'affiche.

5. Sélectionnez la vulnérabilité que vous souhaitez ignorer sur l'appareil sélectionné dans la liste des vulnérabilités dans les applications.

   La fenêtre des propriétés des vulnérabilités dans les applications s'ouvre.

6. Dans la fenêtre des propriétés de la vulnérabilité dans l'application de l'onglet **Général**, activez l'option **Ignorer la vulnérabilité**.

7. Cliquez sur le bouton **Enregistrer**.

   La fenêtre des propriétés de la vulnérabilité dans l'application se ferme.

8. Fermez la fenêtre des propriétés de l'appareil.

La vulnérabilité dans l'application est ignorée sur l'appareil sélectionné.

La vulnérabilité dans l'application ignorée ne sera pas corrigée après la fin de la tâche *Corriger les vulnérabilités* ou de la tâche *Installation des mises à jour requises et correction des vulnérabilités*. Vous pouvez exclure les vulnérabilités logicielles ignorées de la liste des vulnérabilités à l'aide d'un filtre.

Administration des applications exécutées sur les appareils client

Cette section décrit les fonctions de Kaspersky Security Center associées à l'administration des applications exécutées sur les appareils clients.

Utilisation du Contrôle des applications pour gérer les fichiers exécutables

Vous pouvez utiliser le module Contrôle des applications pour autoriser ou interdire le lancement de fichiers exécutables sur les appareils des utilisateurs. Le module Contrôle des applications prend en charge les systèmes d'exploitation Windows et Linux.

Pour les systèmes d'exploitation basés sur Linux, le composant Contrôle des applications est disponible à partir de Kaspersky Endpoint Security 11.2 pour Linux. Le composant est également disponible pour Kaspersky Embedded Systems Security pour Windows 3.0 ou version ultérieure.

Prérequis

- Kaspersky Security Center est déployé dans votre entreprise.
- La stratégie de Kaspersky Endpoint Security for Windows ou de Kaspersky Endpoint Security for Linux est créée et activée.
- La stratégie de Kaspersky Embedded Systems Security for Windows ou de Kaspersky Embedded Systems Security for Linux est créée et active.

Étapes

Le scénario d'utilisation Contrôle des applications se déroule par étapes :

1. **Formation et consultation de la liste des fichiers exécutables sur les appareils client**

   Cette étape vous permet de découvrir les fichiers exécutables qui figurent sur les appareils administrés. Consultez la liste des fichiers exécutables et comparez-la avec les listes des fichiers exécutables autorisés et interdits. Les restrictions d'utilisation des fichiers exécutables peuvent être liées aux stratégies de sécurité de l'information dans votre entreprise.

   Instructions pour :

   - Console d'administration : inventaire des fichiers exécutables
   - Kaspersky Security Center Web Console : obtention et consultation d'une liste des fichiers exécutables stockés sur les appareils client

2. **Création de catégories pour les fichiers exécutables utilisés dans votre organisation**

   Analysez les listes des fichiers exécutables stockés sur les appareils administrés. En fonction de l'analyse, créez des catégories pour les fichiers exécutables. Il est recommandé de créer une catégorie "Applications de travail" qui englobe l'ensemble standard des fichiers exécutables utilisés dans votre organisation. Si différents groupes de sécurité utilisent leurs propres ensembles de fichiers exécutables dans leur travail, une catégorie distincte peut être créée pour chaque groupe de sécurité.

   Instructions pour :

   - Console d'administration : Création d'une catégorie d'applications dont le contenu est ajouté manuellement, Création d'une catégorie d'applications qui inclut les fichiers exécutables des appareils sélectionnés, Création d'une catégorie d'applications qui inclut les fichiers exécutables du dossier spécifié.
   - Kaspersky Security Center Web Console : Création d'une catégorie d'applications dont le contenu est ajouté manuellement, Création d'une catégorie d'applications qui inclut les fichiers exécutables des appareils sélectionnés, Création d'une catégorie d'applications qui inclut les fichiers exécutables du dossier spécifié.

3. **Configuration du Contrôle des applications dans la stratégie Kaspersky Endpoint Security**

   Configurez le composant Contrôle des applications dans la stratégie Kaspersky Endpoint Security à l'aide des catégories que vous avez créées à l'étape précédente.

   Instructions pour :

   - Console d'administration : configuration d'administration du lancement des applications sur les appareils client
   - Kaspersky Security Center Web Console : configuration du Contrôle des applications dans la stratégie Kaspersky Endpoint Security for Windows

4. **Configuration du Contrôle des applications dans la stratégie de l'application Kaspersky Embedded Systems Security**

   Configurez le composant Contrôle des applications dans la stratégie de Kaspersky Embedded Systems Security for Windows à l'aide des catégories que vous avez créées. Pour plus d'informations sur le composant Contrôle des applications, consultez l'Aide de Kaspersky Embedded Systems Security for Windows ou l'Aide de Kaspersky Embedded Systems Security for Linux.

   Si vous utilisez un grand nombre de règles, une erreur peut se produire lors du chargement de la stratégie. Vous pouvez augmenter la taille maximale de la demande en octets en utilisant les commandes suivantes :

   - Pour la requête JSON :

     ```
     klscflag -fset -pv ".core/.independent" -s KLLIM -n
     LP_KLOAPI_MaxSizeOfJsonRequestInBytes -v <max_request_size> -t d
     ```

   - Pour la requête HTTP :

     ```
     klscflag -fset -pv ".core/.independent" -s KLLIM -n
     LP_KLOAPI_MaxSizeOfHttpRequestInBytes -v <max_request_size> -t d
     ```

     Où `<max_request_size>` est une taille de requête maximale en octets (par exemple, `200000000`).

5. **Activation du composant Contrôle des applications en mode test**

   Pour vous assurer que les règles de Contrôle des applications ne bloquent pas les fichiers exécutables nécessaires pour le travail, il est recommandé d'activer le test des règles de Contrôle des applications et d'analyser leur fonctionnement après avoir créé de nouvelles règles. Lorsque les tests sont activés, Kaspersky Endpoint Security for Windows ou Kaspersky Embedded Systems Security ne bloquera pas les fichiers exécutables dont le démarrage est interdit par les règles de Contrôle des applications, mais enverra des notifications relatives à leur démarrage dans le Serveur d'administration.

   Lors du test des règles de Contrôle des applications, il est recommandé d'effectuer les actions suivantes :

   - déterminez la période de test. La période de test peut aller de quelques jours à deux mois.
   - Examinez les événements résultant du test de fonctionnement du Contrôle des applications.

   Instructions pratiques pour Kaspersky Security Center Web Console : Configuration du module Contrôle des applications dans la stratégie Kaspersky Endpoint Security for Windows. Suivez ces instructions et activez l'option **Mode de test** dans le processus de configuration.

6. **Modification des paramètres des catégories du composant Contrôle des applications**

   Si nécessaire, modifiez les paramètres du Contrôle des applications. Selon les résultats des tests, vous pouvez ajouter des fichiers exécutables associés aux événements du composant Contrôle des applications à une catégorie enrichie manuellement.

   Instructions pour :

   - Console d'administration : ajout de fichiers exécutables liés par un événement à la catégorie de l'application
   - Kaspersky Security Center Web Console : ajout de fichiers exécutables liés par un événement à la catégorie de l'application

7. **Appliquer les règles du Contrôle des applications en mode de fonctionnement**

   Une fois les règles du Contrôle des applications testées et la configuration des catégories terminée, vous pouvez appliquer les règles du Contrôle des applications en mode de fonctionnement.

   Instructions pratiques pour Kaspersky Security Center Web Console : Configuration du module Contrôle des applications dans la stratégie Kaspersky Endpoint Security for Windows. Suivez ces instructions et désactivez l'option **Mode de test** dans le processus de configuration.

8. **Vérification de la configuration du Contrôle des applications**

   Assurez-vous d'avoir effectué les tâches suivantes :

   - Catégories créées pour les fichiers exécutables.
   - Configuré le Contrôle des applications en utilisant les catégories.
   - Appliquer les règles du Contrôle des applications en mode de fonctionnement.

Résultats

Une fois le scénario terminé, le démarrage des fichiers exécutables est contrôlé sur les appareils administrés. Les utilisateurs peuvent uniquement exécuter les fichiers exécutables autorisés dans votre organisation et ne peuvent pas exécuter les fichiers exécutables qui y sont interdits.

Pour obtenir des informations détaillées sur le Contrôle des applications, consultez les rubriques d'aide suivantes :

- Aide en ligne de Kaspersky Endpoint Security for Windows
- Aide en ligne de Kaspersky Endpoint Security for Linux
- Kaspersky Security for Virtualization Light Agent
- Aide de Kaspersky Embedded Systems Security for Windows
- Aide de Kaspersky Embedded Systems Security for Linux

Modes et catégories du Contrôle des applications

Le module Contrôle des applications surveille les tentatives des utilisateurs de lancer des fichiers exécutables. Vous pouvez utiliser les règles du Contrôle des applications pour contrôler le lancement des fichiers exécutables.

Le module Contrôle des applications est disponible pour Kaspersky Endpoint Security for Windows, Kaspersky Endpoint Security 11.2 for Linux et les versions ultérieures, et pour Kaspersky Security for Virtualization Light Agent. Toutes les instructions de cette section décrivent la configuration du Contrôle des applications pour Kaspersky Endpoint Security for Windows.

Le démarrage des fichiers exécutables dont les paramètres ne correspondent à aucune des règles du Contrôle des applications est régi par le mode de fonctionnement sélectionné pour le module :

- *Liste de refus*. Le mode est utilisé si vous souhaitez autoriser le démarrage de tous les fichiers exécutables, sauf ceux indiqués dans les règles de blocage. Par défaut, ce mode est sélectionné.
- *Liste d'autorisation*. Le mode est utilisé si vous souhaitez bloquer le démarrage de tous les fichiers exécutables, sauf ceux indiqués dans les règles d'autorisation.

Les règles du Contrôle des applications sont mises en œuvre via des catégories de fichiers exécutables. Il existe trois types de catégories dans Kaspersky Security Center :

- Catégorie complétée à la main. vous définissez des conditions, par exemple les métadonnées du fichier, le hashcode du fichier, le certificat du fichier, la catégorie KL, le chemin d'accès au fichier, afin d'inclure des fichiers exécutables dans la catégorie.
- Catégorie incluant des fichiers exécutables depuis les appareils sélectionnés. Vous spécifiez un appareil dont les fichiers exécutables sont automatiquement inclus dans la catégorie.
- Catégorie incluant des fichiers exécutables à partir des appareils sélectionnés. Vous spécifiez un dossier dont les fichiers exécutables sont automatiquement inclus dans la catégorie.

Pour obtenir des informations détaillées sur le Contrôle des applications, consultez les rubriques d'aide suivantes :

- Aide en ligne de Kaspersky Endpoint Security for Windows
- Aide en ligne de Kaspersky Endpoint Security for Linux
- Kaspersky Security for Virtualization Light Agent
- Aide de Kaspersky Embedded Systems Security for Windows
- Aide de Kaspersky Embedded Systems Security for Linux

Obtention et consultation d'une liste des fichiers exécutables stockés sur les appareils client

Vous pouvez obtenir la liste des fichiers exécutables stockés sur les appareils clients de l'une des manières suivantes :

- Activation des notifications sur le démarrage des applications dans la stratégie de Kaspersky Endpoint Security.
- Création d'une tâche d'inventaire.

Activation des notifications sur le démarrage des applications dans la stratégie de Kaspersky Endpoint Security

Pour activer les notifications relatives au démarrage des applications, procédez comme suit :

1. Ouvrez les paramètres de la stratégie de Kaspersky Endpoint Security, puis accédez à **Paramètres généraux** → **Rapports et stockage**.
2. Dans le groupe de paramètres **Transfert de données au Serveur d'administration**, cochez la case **À propos des applications lancées** et enregistrez les modifications.

Lorsqu'un utilisateur tente de lancer des fichiers exécutables, les informations relatives à ces fichiers sont ajoutées à la liste des fichiers exécutables sur un appareil client. Kaspersky Endpoint Security envoie ces informations à l'Agent d'administration, qui les transmet ensuite au Serveur d'administration.

Création d'une tâche d'inventaire

La fonction d'inventaire des fichiers exécutables est disponible pour les applications suivantes :

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Linux version 11.2 et ultérieure
- Kaspersky Security for Virtualization 4.0 Light Agent et versions ultérieures

Vous pouvez réduire la charge sur la base de données tout en obtenant des informations sur les applications installées. Pour gagner de la place dans la base de données, exécutez une tâche d'inventaire sur les appareils de référence sur lesquels un ensemble standard de logiciels est installé. Il est préférable que le nombre d'appareils soit compris entre 1 et 3.

Nous vous déconseillons fortement d'exécuter la tâche d'inventaire lors de l'utilisation des bases de données suivantes : MySQL, PostgreSQL, SQL Server Express Edition et MariaDB (toutes les éditions).

Pour créer une tâche d'inventaire des fichiers exécutables sur les appareils clients, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Tâches**.

   La liste des tâches s'affiche.

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

   Ceci permet de lancer l'assistant de création d'une tâche. Suivez les étapes de l'assistant.

3. Sur la page **Paramètres de nouvelle tâche**, dans la liste déroulante **Application**, sélectionnez Kaspersky Endpoint Security for Windows ou Kaspersky Endpoint Security for Linux, selon le type de système d'exploitation des appareils clients.

4. À partir de la liste déroulante **Type de tâche**, sélectionnez **Inventaire**.

5. Sur la page **Fin de la création de la tâche**, cliquez sur le bouton **Terminer**.

   Une fois que l'Assistant de création d'une tâche a terminé l'opération, la tâche **Inventaire** est créée et configurée. Si vous le souhaitez, vous pouvez modifier les paramètres de la tâche créée. La tâche qui vient d'être créée s'affiche dans la liste des tâches.

Pour obtenir une description détaillée de la tâche d'inventaire, consultez les aides suivantes :

- Aide de Kaspersky Endpoint Security for Windows
- Aide de Kaspersky Endpoint Security for Linux
- Kaspersky Security for Virtualization Light Agent

Une fois la tâche **Inventaire** effectuée, la liste des fichiers exécutables stockés sur les appareils administrés est créée et vous pouvez la consulter.

Lors de l'inventaire, les fichiers exécutables aux formats suivants peuvent être détectés (selon l'option sélectionnée dans les propriétés de la tâche d'inventaire) : MZ, COM, PE, NE, SYS, CMD, BAT, PS1, JS, VBS, REG, MSI, CPL, DLL, JAR et HTML.

Affichage de la liste des fichiers exécutables stockés sur les appareils administrés

Pour consulter la liste de tous les fichiers exécutables stockés sur les appareils client :

Dans le menu principal, accédez à **Opérations → Applications tierces → Fichiers exécutables**.

La page affiche la liste des fichiers exécutables stockés sur les appareils client.

Si nécessaire, vous pouvez envoyer le fichier exécutables de l'appareil administré à l'appareil sur lequel Kaspersky Security Center Web Console est ouvert.

Pour envoyer un fichier exécutable, procédez comme suit :

1. Dans le menu principal, accédez à **Opérations → Applications tierces → Fichiers exécutables**.
2. Cliquez sur le lien du fichier exécutable que vous souhaitez envoyer.
3. Dans la fenêtre qui s'ouvre, accédez à la section **Appareils**, puis cochez la case correspondant à l'appareil administré à partir duquel vous souhaitez envoyer le fichier exécutable.

   Avant d'envoyer le fichier exécutable, assurez-vous que l'appareil administré dispose d'une connexion directe au Serveur d'administration, en cochant la case **Maintenir la connexion au Serveur d'administration**.

4. Cliquez sur le bouton **Envoyer**.

   Le fichier exécutable sélectionné est téléchargé pour être envoyé ultérieurement vers l'appareil sur lequel Kaspersky Security Center Web Console est ouvert.

Création d'une catégorie d'applications enrichie manuellement

Vous pouvez spécifier un ensemble de critères comme modèle pour les fichiers exécutables dont vous souhaitez autoriser ou bloquer le démarrage dans votre entreprise. En vous basant sur les fichiers exécutables correspondant aux critères, vous pouvez créer une catégorie d'applications et l'utiliser dans la configuration du composant Contrôle des applications.

Pour créer une catégorie d'applications enrichie manuellement, procédez comme suit :

1. Dans le menu principal, accédez à **Opérations → Applications tierces → Catégories d'applications**.

   La page comportant une liste des catégories d'applications s'affiche.

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

   L'Assistant de nouvelle catégorie démarre. Parcourez les étapes de l'Assistant à l'aide du bouton **Suivant**.

3. À l'étape **Sélectionner la méthode de création de catégorie**, sélectionnez l'option **Catégorie dont le contenu a été ajouté manuellement. Les données des fichiers exécutables sont ajoutées manuellement à la catégorie**.

4. À l'étape **Conditions**, cliquez sur le bouton **Ajouter** pour ajouter un critère de condition d'inclusion de fichiers à la catégorie créée.

5. À l'étape **Critère de condition**, sélectionnez un type de règle pour la création de la catégorie dans la liste :

- **D'une catégorie KL**

  Si cette option a été sélectionnée, vous pouvez indiquer la catégorie d'applications de Kaspersky en tant que la condition d'ajout des applications dans une catégorie d'utilisateur. Les applications, faisant partie de la catégorie Kaspersky, seront ajoutées dans une catégorie d'applications définie par l'utilisateur.

- **Sélectionner un certificat dans le stockage**

  Si cette option a été sélectionnée, vous pouvez indiquer les certificats du stockage. La condition de catégorie correspond uniquement aux fichiers exécutables signés par le certificat spécifié.

- **Définir le chemin d'accès à l'application (masques pris en charge)**

  Si cette option a été sélectionnée, vous pouvez indiquer le chemin d'accès au fichier ou au dossier sur l'appareil client dont les fichiers exécutables seront ajoutés dans une catégorie d'applications définie par l'utilisateur. Vous pouvez utiliser des expressions régulières, comme *C:\path_to_exe** : *C:\Program Files\Internet Explorer**.

- **Disque amovible**

  Si cette option a été sélectionnée, vous pouvez indiquer le type de support (n'importe lequel ou disque amovible) sur lequel l'application est exécutée. Les applications, lancées sur le moyen de type sélectionné, seront ajoutées dans une catégorie d'applications définie par l'utilisateur.

- **Hash, métadonnées ou certificat** :

  - **Sélectionner dans la liste des fichiers exécutables**

    Si vous avez choisi cette option, vous pouvez sélectionner les applications à ajouter à une catégorie dans la liste des fichiers exécutables de 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, la fenêtre s'ouvre avec les paramètres remplis par les métadonnées de l'application sélectionnée :

- Nom du fichier.
- Version du fichier. Vous pouvez spécifier une valeur précise pour la version ou décrire une condition, par exemple " supérieure à 5.0 ".
- Nom de l'application.
- Version de l'application. Vous pouvez spécifier une valeur précise pour la version ou décrire une condition, par exemple " supérieure à 5.0 ".
- Fournisseur.

Veuillez noter que seul le lancement des fichiers exécutables répondant aux paramètres spécifiés est bloqué, et non le lancement de l'application que vous sélectionnez. Si les métadonnées de l'application sélectionnée correspondent à celles du fichier exécutable qui est lancé lors du lancement de l'application, vous pouvez passer à l'étape suivante. Sinon, vous devez modifier les valeurs manuellement pour qu'elles correspondent aux métadonnées du fichier exécutable.

- **Définir manuellement**

Si cette option est sélectionnée, vous devez indiquer le hash du fichier, ou les métadonnées ou le certificat en guise de condition d'ajout des applications à la catégorie utilisateur.

Hash du fichier

En fonction de la version de l'application de sécurité installée sur les appareils de votre réseau, il faut choisir un algorithme de calcul de la fonction hash par l'application Kaspersky Security Center pour les fichiers de la catégorie. Les informations relatives aux 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 du calcul ne contient pas de vulnérabilités et il est considéré actuellement comme la fonction de chiffrement la plus sûre. Kaspersky Endpoint Security 10 Service Pack 2 for Windows et suivants prennent en charge le calcul de la fonction hash SHA256. Le calcul de la fonction de hach MD5 est pris en charge pour les versions inférieures à Kaspersky Endpoint Security 10 Service Pack 2 for Windows.

Choisissez une des options du calcul de la fonction hash par l'application Kaspersky Security Center pour les fichiers de la catégorie :

- Si toutes les instances des applications de sécurité installées sur votre réseau sont Kaspersky Endpoint Security 10 Service Pack 2 for Windows ou des versions ultérieures, cochez la case **SHA256**. Il est déconseillé d'ajouter une catégorie créée selon le critère du hachage SHA256 du fichier exécutable pour les versions de l'application antérieures à Kaspersky Endpoint Security 10 Service Pack 2 for Windows. Cela pourrait entraîner un échec de l'application de sécurité. 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 Service Pack 2 for Windows sont installées sur votre réseau, sélectionnez **Hash MD5**. Il est interdit d'ajouter une catégorie créée selon le critère de la somme de contrôle MD5 du fichier exécutable pour les versions Kaspersky Endpoint Security 10 Service Pack 2 for Windows et suivantes. Dans ce cas vous pouvez utiliser la fonction de hachage cryptographique SHA256 pour les fichiers de la catégorie.

- Si différents appareils de votre réseau utilisent à la fois des versions antérieures et ultérieures de Kaspersky Endpoint Security 10, cochez à la fois la case **SHA256** et la case **Hash MD5**.

Données méta

Si cette option est sélectionnée, vous pouvez spécifier les métadonnées du fichier, telles que le nom du fichier, la version du fichier, le fournisseur. La condition de catégorie ne concerne que les fichiers exécutables ayant les mêmes métadonnées.

Certificat

Si cette option a été sélectionnée, vous pouvez indiquer les certificats du stockage. La condition de catégorie correspond uniquement aux fichiers exécutables signés par le certificat spécifié.

- Depuis un fichier ou un paquet MSI / un fichier archivé

Si cette option a été sélectionnée, vous pouvez indiquer le fichier de l'installateur MSI en tant que la condition d'ajout des applications dans une catégorie d'utilisateur. Les données méta de l'installateur de l'application seront transmises sur le Serveur d'administration. Les applications, dont les données méta de l'installateur coïncident avec l'installateur MSI indiqué, seront ajoutées dans une catégorie d'applications définie par l'utilisateur.

Le critère sélectionné est ajouté à la liste des conditions.

Vous pouvez ajouter autant de critères que nécessaire à la création de la catégorie d'applications.

6. À l'étape **Exclusions**, cliquez sur le bouton **Ajouter** pour ajouter un critère de condition d'exclusion de fichiers de la catégorie en cours de création.

7. À l'étape **Critère de condition**, sélectionnez un type de règle dans la liste, comme vous avez sélectionné une règle pour la création de la catégorie.

Lorsque l'Assistant a terminé l'opération, la catégorie d'applications est créée. Elle s'affiche dans la liste des catégories d'applications. Vous pouvez utiliser la catégorie d'application créée lorsque vous configurez le Contrôle des applications.

Pour obtenir des informations détaillées sur le Contrôle des applications, consultez les rubriques d'aide suivantes :

- Aide en ligne de Kaspersky Endpoint Security for Windows
- Aide en ligne de Kaspersky Endpoint Security for Linux
- Kaspersky Security for Virtualization Light Agent
- Aide de Kaspersky Embedded Systems Security for Windows
- Aide de Kaspersky Embedded Systems Security for Linux

Création d'une catégorie d'applications incluant des fichiers exécutables provenant des appareils sélectionnés

Vous pouvez utiliser des fichiers exécutables des appareils sélectionnés comme modèle des fichiers exécutables que vous souhaitez autoriser ou bloquer. En vous basant sur les fichiers exécutables des appareils sélectionnés, vous pouvez créer une catégorie et l'utiliser dans la configuration du composant Contrôle des applications.

Pour récupérer la liste des fichiers exécutables depuis les appareils, procédez comme suit :

1. Assurez-vous que la stratégie de Kaspersky Endpoint Security for Windows ou de Kaspersky Endpoint Security for Linux est créée et active. Activez le module Contrôle des applications dans la stratégie.

2. Obtenez une liste des fichiers exécutables stockés sur les appareils client.

Pour créer une catégorie incluant des fichiers exécutables provenant des appareils sélectionnés :

1. Dans le menu principal, accédez à **Opérations → Applications tierces → Catégories d'applications**.

   La page comportant une liste des catégories s'affiche.

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

   L'Assistant de nouvelle catégorie démarre. Parcourez les étapes de l'assistant à l'aide du bouton **Suivant**.

3. À l'étape **Sélectionner la méthode de création de catégorie**, spécifiez le nom de la catégorie et sélectionnez l'option **Catégorie qui reprend les fichiers exécutables issus d'appareils sélectionnés. Ces fichiers exécutables sont traités automatiquement et leurs métriques sont ajoutées à la catégorie**.

4. Cliquez sur le bouton **Ajouter**.

5. Dans la fenêtre qui s'ouvre, sélectionnez l'appareil (les appareils) dont les fichiers exécutables seront utilisés pour créer la catégorie.

6. Définissez les paramètres suivants :

- **Algorithme de calcul de la fonction hash**

  En fonction de la version de l'application de sécurité installée sur les appareils de votre réseau, il faut choisir un algorithme de calcul de la fonction hash par l'application Kaspersky Security Center pour les fichiers de la catégorie. Les informations relatives aux 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 du calcul ne contient pas de vulnérabilités et il est considéré actuellement comme la fonction de chiffrement la plus sûre. Kaspersky Endpoint Security 10 Service Pack 2 for Windows et suivants prennent en charge le calcul de la fonction hash SHA256. Le calcul de la fonction de hach MD5 est pris en charge pour les versions inférieures à Kaspersky Endpoint Security 10 Service Pack 2 for Windows.

  Choisissez une des options du calcul de la fonction hash par l'application Kaspersky Security Center pour les fichiers de la catégorie :

  - Si toutes les instances des applications de sécurité installées sur votre réseau sont Kaspersky Endpoint Security 10 Service Pack 2 for Windows ou des versions ultérieures, cochez la case **SHA256**. Il est déconseillé d'ajouter une catégorie créée selon le critère du hachage SHA256 du fichier exécutable pour les versions de l'application antérieures à Kaspersky Endpoint Security 10 Service Pack 2 for Windows. Cela pourrait entraîner un échec de l'application de sécurité. 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 Service Pack 2 for Windows sont installées sur votre réseau, sélectionnez **Hash MD5**. Il est interdit d'ajouter une catégorie créée selon le critère de la somme de contrôle MD5 du fichier exécutable pour les versions Kaspersky Endpoint Security 10 Service Pack 2 for Windows et suivantes. Dans ce cas vous pouvez utiliser la fonction de hachage cryptographique SHA256 pour les fichiers de la catégorie.

  Si différents appareils de votre réseau utilisent à la fois des versions antérieures et ultérieures de Kaspersky Endpoint Security 10, cochez à la fois la case **SHA256** et la case **Hash MD5**.

  La case **Calculer SHA256 pour les fichiers en la catégorie (pris en charge pour Kaspersky Endpoint Security 10 Service Pack 2 for Windows et versions supérieures)** est cochée par défaut.

  La case **Calculer MD5 pour les fichiers en la catégorie (pris en charge pour les versions inférieures à Kaspersky Endpoint Security 10 Service Pack 2 for Windows)** est décochée.

- **Synchroniser les données avec le stockage du Serveur d'administration**

  Sélectionnez cette option si vous souhaitez que le Serveur d'administration vérifie régulièrement les modifications dans le ou les dossiers spécifiés.

  Cette option est Inactif par défaut.

  Si vous activez cette option, indiquez la période (en heures) pour vérifier les modifications dans le ou les dossiers spécifiés. L'intervalle de l'analyse est de 24 heures par défaut.

- **Type de fichier**

Dans cette section, vous pouvez spécifier le type de fichier utilisé pour créer la catégorie d'applications.

Tous les fichiers. Tous les fichiers sont pris en compte lors de la création de la catégorie. Cette option est sélectionnée par défaut.

Uniquement les fichiers hors des catégories d'applications. Seuls les fichiers hors catégories d'applications sont pris en compte lors de la création de la catégorie.

- **Dossiers**

  Dans cette section, vous pouvez spécifier les dossiers de l'appareil (des appareils) sélectionné(s) contenant les fichiers utilisés pour créer la catégorie d'applications.

  Tous les dossiers. Tous les dossiers sont pris en compte pour la catégorie en cours de création. Cette option est sélectionnée par défaut.

  Dossier indiqué. Seul le dossier spécifié est pris en compte pour la catégorie en cours de création. Si vous sélectionnez cette option, vous devez indiquer le chemin d'accès au dossier.

À la fin de l'Assistant, la catégorie des fichiers exécutables est créée. Elle s'affiche dans la liste des catégories. Vous pouvez utiliser la catégorie créée lorsque vous configurez le Contrôle des applications.

Création d'une catégorie d'applications incluant des fichiers exécutables provenant du dossier sélectionné

Vous pouvez utiliser des fichiers exécutables provenant d'un dossier sélectionné comme norme de fichiers exécutables que vous souhaitez autoriser ou bloquer dans votre organisation. En vous basant sur les fichiers exécutables provenant du dossier sélectionné, vous pouvez créer une catégorie d'applications et l'utiliser dans la configuration du module Contrôle des applications.

Pour créer une catégorie incluant des fichiers exécutables provenant du dossier sélectionné :

1. Dans le menu principal, accédez à **Opérations → Applications tierces → Catégories d'applications**.

   La page comportant une liste des catégories s'affiche.

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

   L'Assistant de nouvelle catégorie démarre. Parcourez les étapes de l'assistant à l'aide du bouton **Suivant**.

3. À l'étape **Sélectionner la méthode de création de catégorie**, spécifiez le nom de la catégorie et sélectionnez l'option **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**.

4. Indiquez le dossier dont les fichiers exécutables seront utilisés pour créer la catégorie.

5. Configurez les paramètres suivants :

- Inclure dans la catégorie des bibliothèques connectées de manière dynamique (DLL)

  Sont intégrées dans la catégorie d'applications les bibliothèques de liens dynamiques (fichiers au format DLL) et le module Contrôle des applications enregistre les actions de ces bibliothèques lancées dans le système. Lors de l'inclusion de fichiers au format DLL dans une catégorie, les performances de Kaspersky Security Center peuvent diminuer.

  Celle-ci est décochée par défaut.

- Inclure les données relatives aux scripts dans la catégorie

  Sont intégrées dans la catégorie d'applications les données sur les scripts et les scripts ne sont pas bloqués pas par le module Protection contre les menaces Internet. Lors de l'inclusion des données sur les scripts dans une catégorie, Kaspersky Security Center peut perdre en performance.

  Celle-ci est décochée par défaut.

- Algorithme de calcul de la fonction hash : **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) / 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)**

En fonction de la version de l'application de sécurité installée sur les appareils de votre réseau, il faut choisir un algorithme de calcul de la fonction hash par l'application Kaspersky Security Center pour les fichiers de la catégorie. Les informations relatives aux 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 du calcul ne contient pas de vulnérabilités et il est considéré actuellement comme la fonction de chiffrement la plus sûre. Kaspersky Endpoint Security 10 Service Pack 2 for Windows et suivants prennent en charge le calcul de la fonction hash SHA256. Le calcul de la fonction de hach MD5 est pris en charge pour les versions inférieures à Kaspersky Endpoint Security 10 Service Pack 2 for Windows.

Choisissez une des options du calcul de la fonction hash par l'application Kaspersky Security Center pour les fichiers de la catégorie :

- Si toutes les instances des applications de sécurité installées sur votre réseau sont Kaspersky Endpoint Security 10 Service Pack 2 for Windows ou des versions ultérieures, cochez la case **SHA256**. Il est déconseillé d'ajouter une catégorie créée selon le critère du hachage SHA256 du fichier exécutable pour les versions de l'application antérieures à Kaspersky Endpoint Security 10 Service Pack 2 for Windows. Cela pourrait entraîner un échec de l'application de sécurité. 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 Service Pack 2 for Windows sont installées sur votre réseau, sélectionnez **Hash MD5**. Il est interdit d'ajouter une catégorie créée selon le critère de la somme de contrôle MD5 du fichier exécutable pour les versions Kaspersky Endpoint Security 10 Service Pack 2 for Windows et suivantes. Dans ce cas vous pouvez utiliser la fonction de hachage cryptographique SHA256 pour les fichiers de la catégorie.

Si différents appareils de votre réseau utilisent à la fois des versions antérieures et ultérieures de Kaspersky Endpoint Security 10, cochez à la fois la case **SHA256** et la case **Hash MD5**.

La case **Calculer SHA256 pour les fichiers en la catégorie (pris en charge pour Kaspersky Endpoint Security 10 Service Pack 2 for Windows et versions supérieures)** est cochée par défaut.

La case **Calculer MD5 pour les fichiers en la catégorie (pris en charge pour les versions inférieures à Kaspersky Endpoint Security 10 Service Pack 2 for Windows)** est décochée.

- Forcer l'analyse du dossier à la recherche de modifications

Si cette option est activée, l'application effectue régulièrement une analyse forcée du dossier d'ajout de la catégorie pour vérifier la présence de modifications. La fréquence de l'analyse peut être définie en heures dans le champ de saisie situé près de la case. Par défaut, la fréquence des vérifications forcées est de 24 heures.

Si l'option est désactivée, l'application n'imposera pas de vérification du dossier. Le serveur appelle les fichiers du dossier en cas de modification, d'ajout ou de suppression.

Cette option est Inactif par défaut.

À la fin de l'Assistant, la catégorie des fichiers exécutables est créée. Elle s'affiche dans la liste des catégories. Vous pouvez utiliser la catégorie dans la configuration du Contrôle des applications.

Pour obtenir des informations détaillées sur le Contrôle des applications, consultez les rubriques d'aide suivantes :

- Aide en ligne de Kaspersky Endpoint Security for Windows
- Aide en ligne de Kaspersky Endpoint Security for Linux
- Kaspersky Security for Virtualization Light Agent

- Aide de Kaspersky Embedded Systems Security for Windows
- Aide de Kaspersky Embedded Systems Security for Linux

Affichage de la liste des catégories d'applications

Vous pouvez consulter la liste des catégories de fichiers exécutables configurés et les paramètres de chaque catégorie.

Pour consulter la liste des catégories d'applications,

Dans le menu principal, accédez à **Opérations → Applications tierces → Catégories d'applications**.

La page comportant une liste des catégories s'affiche.

Pour consulter les propriétés d'une catégorie d'applications,

Cliquez sur le nom de la catégorie.

La fenêtre des propriétés de la catégorie s'affiche. Les propriétés sont regroupées sur plusieurs onglets.

Ajout de fichiers exécutables liés par un événement à la catégorie d'applications

Une fois que le Contrôle des applications est configuré dans les stratégies Kaspersky Endpoint Security for Windows, les événements suivants s'affichent dans la liste des événements :

- **Lancement de l'application interdit** (événement *Critique*). Cet événement s'affiche si vous avez configuré le Contrôle des applications pour appliquer des règles.
- **Lancement de l'application interdit en mode de test** (événement d'*Information*). Cet événement s'affiche si vous avez configuré le Contrôle des applications pour tester des règles.
- **Message à l'administrateur concernant l'interdiction de lancement de l'application** (l'événement *Avertissement*). Cet événement s'affiche si vous avez configuré le Contrôle des applications pour appliquer des règles et si un utilisateur a demandé à accéder à l'application dont le démarrage est bloqué.

Il est recommandé de créer des sélections d'événements pour consulter les événements associés au fonctionnement du Contrôle des applications.

Vous pouvez ajouter des fichiers exécutables associés aux événements du Contrôle des applications à une catégorie d'applications existante ou à une nouvelle catégorie d'applications. Vous pouvez ajouter des fichiers exécutables uniquement à une catégorie d'applications enrichie manuellement.

Pour ajouter des fichiers exécutables liés aux événements du Contrôle des applications à une catégorie d'applications :

1. Dans le menu principal, accédez à **Surveillance et rapports → Sélections d'événements**.

   La liste des sélections d'événements s'affiche.

2. Sélectionnez la sélection d'événements pour consulter les événements associés au Contrôle des applications et démarrer cette sélection d'événements.

   Si vous n'avez pas créé de sélection d'événements associée au Contrôle des applications, vous pouvez sélectionner et démarrer une sélection prédéfinie, par exemple, les **Événements récents**.

   La liste des événements s'affiche.

3. Sélectionnez les événements dont vous souhaitez ajouter les fichiers exécutables associés à la catégorie d'applications, puis cliquez sur le bouton **Affecter à une catégorie**.

   L'Assistant de nouvelle catégorie démarre. Parcourez les étapes de l'assistant à l'aide du bouton **Suivant**.

4. Indiquez les paramètres appropriés sur la page de l'assistant :

- Dans la section **Action sur le fichier exécutable lié à l'événement**, sélectionnez une des options suivantes :
  - Ajoute une nouvelle catégorie d'applications

    Sélectionnez cette option si vous souhaitez créer une nouvelle catégorie d'applications basée sur des fichiers exécutables liés par un événement.

    Cette option est sélectionnée par défaut.

    Si vous avez sélectionné cette option, indiquez un nouveau nom de catégorie.

  - Ajouter à une catégorie d'application existante

    Sélectionnez cette option s'il est nécessaire d'ajouter des fichiers exécutables liés par un événement à une catégorie d'applications existante.

    Par défaut, cette option n'est pas sélectionnée.

    Si vous avez sélectionné cette option, sélectionnez la catégorie d'applications enrichie manuellement à laquelle vous souhaitez ajouter les fichiers exécutables.

- Dans la section **Type de règle**, sélectionnez une des options suivantes :
  - **Règles pour l'ajout aux inclusions**
  - **Règles pour l'ajout aux exclusions**
- Dans la section **Paramètre utilisé comme condition**, sélectionnez une des options suivantes :
  - Détails du certificat (ou hash SHA256 pour les fichiers sans certificat)

    Les fichiers peuvent être signés par un certificat. De plus un certificat peut signer plusieurs fichiers. Par exemple, différentes versions d'une application peuvent être signées par un certificat ou plusieurs applications différentes d'un même éditeur peuvent être signées par un même certificat. En cas de sélection du certificat, la catégorie peut reprendre plusieurs versions de l'application ou plusieurs applications d'un même éditeur.

    Chaque fichier possède sa propre fonction de hachage SHA256 unique. En cas de sélection de la fonction hash SHA256, la catégorie reprend uniquement un seul fichier correspondant, par exemple, la version définie de l'application.

    Sélectionnez cette option si vous souhaitez ajouter les données du certificat du fichier exécutable (ou la fonction hash SHA256 pour les fichiers sans certificat) aux règles de la catégorie.

    Cette option est sélectionnée par défaut.

  - Détails du certificat (les fichiers sans certificat sont ignorés)

Les fichiers peuvent être signés par un certificat. De plus un certificat peut signer plusieurs fichiers. Par exemple, différentes versions d'une application peuvent être signées par un certificat ou plusieurs applications différentes d'un même éditeur peuvent être signées par un même certificat. En cas de sélection du certificat, la catégorie peut reprendre plusieurs versions de l'application ou plusieurs applications d'un même éditeur.

Sélectionnez cette option si vous souhaitez ajouter les données du certificat du fichier exécutable aux règles de la catégorie. Si le fichier exécutable n'a pas de certificat, ce fichier sera ignoré. Les informations le concernant ne seront pas ajoutées dans la catégorie.

- **SHA256 uniquement (les fichiers sans hash sont ignorés)**

  Chaque fichier possède sa propre fonction de hachage SHA256 unique. En cas de sélection de la fonction hash SHA256, la catégorie reprend uniquement un seul fichier correspondant, par exemple, la version définie de l'application.

  Sélectionnez cette option si vous souhaitez ajouter uniquement les données de la fonction hash SHA256 du fichier exécutable.

- **MD5 uniquement (mode supprimé, uniquement pour Kaspersky Endpoint Security 10 Service Pack 1)**

  Chaque fichier possède sa propre fonction de hachage MD5 unique. En cas de sélection de la fonction hash MD5, la catégorie reprend uniquement un seul fichier correspondant, par exemple, la version définie de l'application.

  Sélectionnez cette option si vous souhaitez ajouter uniquement les données de la fonction hash MD5 du fichier exécutable. Le calcul de la fonction de hachage MD5 est pris en charge pour les versions inférieures à Kaspersky Endpoint Security 10 Service Pack 1 for Windows.

5. Cliquez sur le bouton **OK**.

   Lorsque l'assistant a terminé, les fichiers exécutables associés aux événements du Contrôle des applications sont ajoutés à une catégorie d'applications existante ou à une nouvelle catégorie d'applications. Vous pouvez consulter les paramètres de la catégorie d'applications que vous avez modifiée ou créée.

Pour obtenir des informations détaillées sur le Contrôle des applications, consultez les rubriques d'aide suivantes :

- Aide en ligne de Kaspersky Endpoint Security for Windows
- Aide en ligne de Kaspersky Endpoint Security for Linux
- Kaspersky Security for Virtualization Light Agent
- Aide de Kaspersky Embedded Systems Security for Windows
- Aide de Kaspersky Embedded Systems Security for Linux

Configuration du Contrôle des applications dans la stratégie Kaspersky Endpoint Security for Windows

Après avoir créé les catégories du Contrôle des applications, vous pouvez les utiliser pour la configuration du Contrôle des applications dans les stratégies Kaspersky Endpoint Security for Windows.

Pour configurer le Contrôle des applications dans la stratégie Kaspersky Endpoint Security for Windows :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Stratégies et profils**.

   Une page comportant une liste des stratégies s'affiche.

2. Cliquez sur la stratégie **Kaspersky Endpoint Security for Windows**.

   La fenêtre des paramètres de la stratégie s'ouvre.

3. Accédez à **Paramètres de l'application** → **Contrôles de sécurité** → **Contrôle des applications**.

   La fenêtre **Contrôle des applications** comportant les paramètres du Contrôle des applications s'affiche.

4. L'option **Contrôle des applications** est activée par défaut. Assurez-vous que l'option **Contrôle des applications DÉSACTIVÉ** est en position désactivée.

5. Dans le groupe de paramètres **Paramètres du Contrôle des applications**, activez le mode de fonctionnement en vue d'appliquer les règles du Contrôle des applications et autorisez Kaspersky Endpoint Security for Windows à bloquer le lancement des applications.

   Si vous souhaitez tester les règles de Contrôle des applications, activez le mode test dans la section **Paramètres du Contrôle des applications**. En mode test, Kaspersky Endpoint Security for Windows ne bloque pas le lancement des applications, mais consigne dans le rapport les informations relatives aux règles déclenchées. Cliquez sur le lien **Consulter le rapport** pour afficher ces informations.

6. Activez l'option **Contrôler le chargement des modules DLL** si vous souhaitez que Kaspersky Endpoint Security for Windows surveille le chargement des modules DLL lorsque des applications sont démarrées par les utilisateurs.

   Les informations concernant le module et l'application ayant chargé le module seront enregistrées dans un rapport.

   Kaspersky Endpoint Security for Windows surveille uniquement les modules DLL et les pilotes chargés après que l'option **Contrôler le chargement des modules DLL** a été sélectionnée. Redémarrez l'appareil après avoir sélectionné l'option **Contrôler le chargement des modules DLL** si vous souhaitez que Kaspersky Endpoint Security for Windows surveille tous les modules DLL et les pilotes, y compris ceux qui ont été chargés avant le démarrage de Kaspersky Endpoint Security for Windows.

7. (Facultatif) Dans le bloc **Modèles de message**, vous pouvez modifier le modèle du message qui s'affiche lorsque le démarrage d'une application est bloqué et lorsque le modèle d'email vous est envoyé.

8. Dans les paramètres du groupe **Mode de contrôle des applications**, sélectionnez le mode **Liste de refus** ou **Liste d'autorisation**.

   Le mode **Liste de refus** est sélectionné par défaut.

9. Cliquez sur le lien **Paramètres des listes de règles**.

   La fenêtre **Listes de refus et d'autorisation** s'ouvre pour vous permettre d'ajouter une catégorie d'applications. Par défaut, l'onglet **Liste de refus** est sélectionné si le mode **Liste de refus** est sélectionné ou l'onglet **Liste d'autorisation** est sélectionné si le mode **Liste d'autorisation** est sélectionné.

10. Dans la fenêtre **Listes de refus et listes d'autorisation**, cliquez sur le bouton **Ajouter**.

    La fenêtre **Règle de contrôle des applications** s'ouvre.

11. Cliquez sur le lien **Veuillez choisir une catégorie**.

    La fenêtre **Catégorie d'applications** s'ouvre.

12. Ajoutez la ou les catégories d'applications que vous avez créées précédemment.

    Vous pouvez modifier les paramètres d'une catégorie créée en cliquant sur le bouton **Modifier**.

    Vous pouvez créer une nouvelle catégorie en cliquant sur le bouton **Ajouter**.

    Vous pouvez supprimer une catégorie dans la liste en cliquant sur le bouton **Supprimer**.

13. Une fois que la liste des catégories d'applications est complète, cliquez sur le bouton **OK**.

    La fenêtre **Catégorie d'applications** se ferme.

14. Dans la fenêtre de la règle de **Contrôle des applications**, créez la liste des utilisateurs et des groupes d'utilisateurs auxquels s'applique la règle de Contrôle des applications dans la section **Sujets et leurs droits**.

15. Cliquez sur le bouton **OK** pour enregistrer les paramètres et fermer la fenêtre **Règle du contrôle des applications**.

16. Cliquez sur le bouton **OK** pour enregistrer les paramètres et fermer la fenêtre **Listes de refus et listes d'autorisation**.

17. Cliquez sur le bouton **OK** pour enregistrer les paramètres et fermer la fenêtre **Contrôle des applications**.

18. Fermez la fenêtre avec les paramètres de la stratégie de Kaspersky Endpoint Security for Windows.

Le Contrôle des applications est configuré. Une fois la stratégie propagée aux appareils client, le démarrage des fichiers exécutables est administré.

Pour obtenir des informations détaillées sur le Contrôle des applications, consultez les rubriques d'aide suivantes :

- Aide en ligne de Kaspersky Endpoint Security for Windows
- Aide en ligne de Kaspersky Endpoint Security for Linux
- Kaspersky Security for Virtualization Light Agent
- Aide de Kaspersky Embedded Systems Security for Windows
- Aide de Kaspersky Embedded Systems Security for Linux

Obtention et consultation d'une liste des applications installées sur les appareils client

Kaspersky Security Center procède à l'inventaire de l'ensemble des logiciels installés sur les appareils clients administrés exploitation Linux et Windows.

L'Agent d'administration constitue une liste des applications installées sur l'appareil et la transmet au Serveur d'administration. Il faut environ 10 à 15 minutes à l'Agent d'administration pour mettre à jour la liste des applications.

Pour les appareils clients Windows, l'Agent d'administration reçoit la plupart des informations sur les applications installées à partir du registre Windows. Pour les appareils clients Linux, les gestionnaires de paquets fournissent à l'Agent d'administration des informations sur les applications installées.

Si une application de la section **Registre des applications** a été détectée sur un appareil Linux, les propriétés de l'application ne contiennent pas les informations sur les fichiers exécutables associés.

Pour consulter la liste des applications installées sur les appareils administrés :

1. Dans le menu principal, accédez à **Opérations → Applications tierces → Registre des applications**.

   La page affiche un tableau avec les applications installées sur les appareils administrés. Sélectionnez l'application pour afficher ses propriétés, par exemple, le nom du fournisseur, le numéro de version, la liste des fichiers exécutables, la liste des appareils sur lesquels l'application est installée, la liste des mises à jour du logiciel disponibles et la liste des vulnérabilités dans les applications détectées.

2. Vous pouvez regrouper et filtrer les données du tableau avec les applications installées comme suit :

   - Cliquez sur l'icône des paramètres ( ) dans le coin supérieur droit du tableau.

     Dans le menu **Paramètres des colonnes** affiché, sélectionnez les colonnes à afficher dans le tableau. Pour consulter le type de système d'exploitation des appareils clients sur lesquels l'application est installée, sélectionnez la colonne **Type de système d'exploitation**.

   - Cliquez sur l'icône du filtre ( ) dans le coin supérieur droit du tableau, puis indiquez et appliquez le critère de filtre dans le menu appelé.

     Le tableau filtré des applications installées s'affiche.

Pour afficher la liste des applications installées sur un appareil administré spécifique,

Dans le menu principal, accédez à **Appareils → Appareils administrés → <nom de l'appareil> → Avancé → Registre des applications**. Dans ce menu, vous pouvez exporter la liste des applications vers un fichier CSV ou un fichier TXT.

Pour obtenir des informations détaillées sur le Contrôle des applications, consultez les rubriques d'aide suivantes :

- Aide en ligne de Kaspersky Endpoint Security for Windows
- Aide en ligne de Kaspersky Endpoint Security for Linux
- Kaspersky Security for Virtualization Light Agent
- Aide de Kaspersky Embedded Systems Security for Windows
- Aide de Kaspersky Embedded Systems Security for Linux

Création d'un paquet d'installation d'une application tierce à partir de la base de données Kaspersky

Kaspersky Security Center Web Console vous permet d'effectuer une installation à distance d'applications tierces à l'aide de paquets d'installation. Ces applications tierces sont incluses dans une base de données Kaspersky dédiée. Cette base de données est créée automatiquement lorsque vous exécutez la tâche *Télécharger les mises à jour dans le stockage du Serveur d'administration* pour la première fois.

Pour créer un paquet d'installation d'une application tierce à partir de la base de données Kaspersky, procédez comme suit :

1. Dans le menu principal, accédez à **Découverte et déploiement → Déploiement et attribution → Paquets d'installation**.

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

3. Sur la page Assistant de création du paquet d'installation qui s'ouvre, sélectionnez l'option **Sélectionner l'application de la base de Kaspersky pour créer un paquet d'installation**, puis cliquez sur **Suivant**.

4. Dans la liste des applications qui s'ouvre, sélectionnez l'application appropriée, puis cliquez sur **Suivant**.

5. Sélectionnez la version linguistique appropriée dans la liste déroulante, puis cliquez sur **Suivant**.

   Cette étape ne s'affiche que si l'application propose un choix de plusieurs options de langue.

6. Si vous êtes invité à accepter un Contrat de licence dans le cadre de l'installation, sur la page **Contrat de licence utilisateur final** qui s'ouvre, cliquez sur le lien pour lire le Contrat de licence sur le site Web du fournisseur, puis cochez la case **Je confirme avoir entièrement lu, compris et accepté les conditions de ce Contrat de Licence Utilisateur Final**.

7. Sur la page **Nom du nouveau paquet d'installation** qui s'ouvre, dans le champ **Nom de l'archive**, entrez le nom du paquet d'installation, puis cliquez sur **Suivant**.

Attendez que le paquet d'installation nouvellement créé soit chargé sur le Serveur d'administration. Lorsque l'Assistant de création du paquet d'installation affiche le message vous informant que le processus de création de paquet a réussi, cliquez sur **Terminer**.

Le paquet d'installation nouvellement créé s'affiche dans la liste des paquets d'installation. Vous pouvez sélectionner ce paquet lors de la création ou de la reconfiguration de la tâche *Installation à distance d'une application*.

Affichage et modification des paramètres d'un paquet d'installation d'une application tierce à partir de la base de données de Kaspersky

Si vous avez précédemment créé des paquets d'installation d'applications tierces mentionnées dans la base de données de Kaspersky, vous pouvez afficher et modifier les paramètres de ces paquets.

La modification des paramètres d'un paquet d'installation d'une application tierce à partir de la base de données de Kaspersky n'est proposée que sous la licence de Gestion des vulnérabilités et des correctifs.

Pour afficher et modifier les paramètres d'un paquet d'installation d'une application tierce à partir de la base de données de Kaspersky :

1. Dans le menu principal, accédez à **Découverte et déploiement** → **Déploiement et attribution** → **Paquets d'installation**.

2. Dans la liste des paquets d'installation qui s'ouvre, cliquez sur le nom du paquet concerné.

3. Sur la page de propriétés qui s'ouvre, modifiez les paramètres, si nécessaire.

4. Cliquez sur le bouton **Enregistrer**.

Les paramètres que vous avez modifiés sont enregistrés.

Paramètres d'un paquet d'installation d'une application tierce à partir de la base de données de Kaspersky

Les paramètres d'un paquet d'installation d'une application tierce sont regroupés dans les onglets suivants :

Seule une partie des paramètres listés ci-dessous est affichée par défaut, vous pouvez donc ajouter les colonnes correspondantes en cliquant sur le bouton **Filtrer** et en sélectionnant les noms de colonnes appropriées dans la liste.

- Onglet **Général** :
  - Champ de saisie contenant le nom du paquet d'installation qui peut être modifié manuellement
  - Application

    Le nom de l'application tierce pour laquelle le paquet d'installation est créé.
  - Version

    Le numéro de version de l'application tierce pour laquelle le paquet d'installation est créé.
  - Taille

    La taille du paquet d'installation tiers (en kilo-octets).
  - Date de création

    La date et l'heure de création du paquet d'installation tiers.
  - Chemin

    Le chemin d'accès au dossier réseau où est stocké le paquet d'installation tiers.
- Onglet **Séquence de l'installation** :
  - Installer les modules système général requis

    Si cette option est activée, l'application, avant d'installer une mise à jour, installe automatiquement tous les composants généraux système (prérequis) requis pour l'installation de la mise à jour. Par exemple, il peut s'agir des mises à jour du système d'exploitation.

    Si cette option est désactivée, vous devrez peut-être installer les prérequis manuellement.

    Cette option est Inactif par défaut.
  - Tableau affichant les propriétés de mise à jour et contenant les colonnes suivantes :
    - Nom

Le nom de la mise à jour.

- **Description**

  La description de la mise à jour.

- **Source**

  La source de la mise à jour, c'est-à-dire si elle a été publiée par Microsoft ou par un autre développeur tiers.

- **Type**

  Le type de mise à jour, c'est-à-dire si elle est destinée à un pilote ou à une application.

- **Catégorie**

  La catégorie Windows Server Update Services (WSUS) affichée pour les mises à jour Microsoft (mises à jour critiques, mises à jour des définitions, pilotes, paquets des modules complémentaires, mises à jour de la protection, Service Packs, outils, paquets cumulatifs de mise à jour, mises à jour, mise à niveau).

- **Niveau d'importance selon MSRC**

  Le niveau d'importance de la mise à jour défini par Microsoft Security Response Center (MSRC).

- **Niveau d'importance**

  Le niveau d'importance de la mise à jour défini par Kaspersky.

- **Niveau d'importance du correctif**

  Le niveau d'importance du correctif s'il est destiné à une application Kaspersky.

- **Article**

  L'identifiant (ID) de l'article dans la Base de connaissances décrivant la mise à jour.

- **Bulletin**

  L'identifiant du bulletin de sécurité décrivant la mise à jour.

- **Non désigné pour l'installation (nouvelle version)**

  Indique si la mise à jour présente l'état Non désigné pour l'installation.

- **A installer**

Indique si la mise à jour présente l'état À installer.

- **Installation en cours**

  Indique si la mise à jour présente l'état Installation.

- **Installé**

  Indique si la mise à jour présente l'état Installée.

- **Échec**

  Indique si la mise à jour présente l'état Échec.

- **Redémarrage requis**

  Indique si la mise à jour présente l'état Redémarrage requis.

- **Enregistré**

  Affiche la date et l'heure d'enregistrement de la mise à jour.

- **Installation en mode interactif**

  Indique si la mise à jour nécessite une action de l'utilisateur pendant de l'installation.

- **Révoquées**

  Affiche la date et l'heure de révocation de la mise à jour.

- **État d'approbation de la mise à jour**

  Indique si la mise à jour est approuvée pour l'installation.

- **Révision**

  Affiche le numéro de révision actuel de la mise à jour.

- **Identificateur de mise à jour**

  Affiche l'identifiant de la mise à jour.

- **Version de l'application**

  Affiche le numéro de version vers lequel l'application doit être mise à jour.

- **Remplacé**

Affiche la ou les autres mises à jour qui peuvent remplacer la mise à jour.

- **Remplaçable**

  Affiche la ou les autres mises à jour qui peuvent être remplacées par la mise à jour.

- **Il faut accepter les conditions du Contrat de licence**

  Indique si la mise à jour nécessite l'acceptation des conditions d'un Contrat de licence utilisateur final (CLUF).

- **Descriptions URL**

  Affiche le nom du fournisseur de la mise à jour.

- **Famille d'application**

  Affiche le nom de la famille d'applications à laquelle appartient la mise à jour.

- **Application**

  Affiche le nom de l'application à laquelle appartient la mise à jour.

- **Langue de la localisation**

  Affiche la langue de la localisation de la mise à jour.

- **Non désigné pour l'installation (nouvelle version)**

  Indique si la mise à jour présente l'état Non désignée pour l'installation (nouvelle version).

- **L'installation des préaccessoires est requise**

  Indique si la mise à jour présente l'état L'installation des préaccessoires est requise.

- **Mode de téléchargement**

  Affiche le mode de téléchargement de la mise à jour.

- **Est un correctif**

  Indique si la mise à jour est un correctif.

- **Non installé(e)**

  Indique si la mise à jour présente l'état Non installée.

- L'ongle **Paramètres** affichant les paramètres des paquets d'installation (avec leurs noms, leurs descriptions et leurs valeurs) utilisés comme paramètres de ligne de commande lors de l'installation. Si le paquet ne fournit pas de tels paramètres, le message correspondant s'affiche. Vous pouvez modifier les valeurs de ces paramètres.

- L'onglet **Historique des révisions** qui affiche les révisions du paquet d'installation et qui contient les colonnes suivantes :

  - **Révision** – le numéro de la révision des paquets d'installation.

  - **Heure** – la date et l'heure de modification des paramètres du paquet d'installation.

  - **Utilisateur** – le nom de l'utilisateur ayant modifié les paramètres du paquet d'installation.

  - **Action** – les actions effectuées sur le paquet d'installation dans la révision.

  - **Description** – la description de la révision de modification des paramètres du paquet d'installation.

    Par défaut, la description de la révision n'est pas remplie. Pour ajouter une description de la révision, choisissez la révision requise, puis cliquez sur le bouton **Modifier la description**. Dans la fenêtre qui s'ouvre, saisissez un texte correspondant à la description de la révision.

Tags de l'application

Kaspersky Security Center permet de tagger les applications depuis le registre des applications. Un tag est l'identificateur d'une application qui peut être utilisé pour regrouper ou rechercher des applications. Un tag attribué à des applications peut servir de condition dans les sélections d'appareils.

Par exemple, vous pouvez créer le tag `[Browsers]` et l'affecter à tous les navigateurs (Microsoft Internet Explorer, Google Chrome, Mozilla Firefox, etc.).

Création d'un tag de l'application

Pour créer un tag de l'application, procédez comme suit :

1. Dans le menu principal, accédez à **Opérations → Applications tierces → Tags de l'application**.

2. Cliquez sur **Ajouter**.

   Une fenêtre de nouveau tag s'ouvre.

3. Saisissez le nom du tag.

4. Cliquez sur le bouton **OK** afin d'enregistrer les modifications.

Le nouveau tag apparaît dans la liste des tags de l'application.

Renommage d'un tag de l'application

Pour renommer un tag de l'application, procédez comme suit :

1. Dans le menu principal, accédez à **Opérations** → **Applications tierces** → **Tags de l'application**.
2. Cochez la case en regard du tag que vous voulez renommer, puis cliquez sur **Modifier**.

   Une fenêtre de propriété du tag s'ouvre.
3. Modifiez le nom du tag.
4. Cliquez sur le bouton **OK** afin d'enregistrer les modifications.

Le tag mis à jour apparaît dans la liste des tags de l'application.

Attribution de tags à une application

Pour attribuer un ou plusieurs tags à une application, procédez comme suit :

1. Dans le menu principal, accédez à **Opérations** → **Applications tierces** → **Registre des applications**.
2. Cliquez sur le nom de l'application à laquelle vous souhaitez attribuer les tags.
3. Sélectionnez l'onglet **Tags**.

   L'onglet affiche tous les tags de l'application qui existent sur le Serveur d'administration. Pour les tags attribués à l'application sélectionnée, la case dans la colonne **Tag défini** est cochée.
4. Pour les tags que vous souhaitez attribuer, cochez les cases dans la colonne **Tag défini**.
5. Cliquez sur le bouton **Enregistrer** afin d'enregistrer les modifications.

Les tags sont attribués à l'application.

Suppression de tags attribués à un appareil

Pour supprimer un ou plusieurs tags d'une application, procédez comme suit :

1. Dans le menu principal, accédez à **Opérations** → **Applications tierces** → **Registre des applications**.
2. Cliquez sur le nom de l'application de laquelle vous souhaitez supprimer les tags.
3. Sélectionnez l'onglet **Tags**.

   L'onglet affiche tous les tags de l'application qui existent sur le Serveur d'administration. Pour les tags attribués à l'application sélectionnée, la case dans la colonne **Tag défini** est cochée.

4. Pour les tags que vous souhaitez supprimer, cochez les cases dans la colonne **Tag défini**.
5. Cliquez sur le bouton **Enregistrer** afin d'enregistrer les modifications.

Les tags sont supprimés de l'application.

Les tags de l'application supprimés ne sont pas supprimés. Si vous le voulez, vous pouvez les supprimer manuellement.

Suppression d'un tag de l'application

Pour supprimer un tag de l'application, procédez comme suit :

1. Dans le menu principal, accédez à **Opérations → Applications tierces → Tags de l'application**.
2. Dans la liste, sélectionnez le tag de l'application que vous souhaitez supprimer.
3. Cliquez sur le bouton **Supprimer**.
4. Dans la fenêtre qui s'ouvre, cliquez sur **OK**.

Le tag de l'application est supprimé. Le tag supprimé est automatiquement retiré de toutes les applications auxquelles il était attribué.

Surveillance et rapports

Cette section décrit les capacités de surveillance et d'élaboration de rapports de Kaspersky Security Center. Ces capacités offrent un aperçu de votre infrastructure, des états de la protection et des statistiques.

Une fois Kaspersky Security Center déployé, ou pendant l'opération de déploiement, vous pouvez configurer les fonctions de surveillance et de création de rapports répondant le mieux à vos besoins.

Scénario : Surveillance et rapports

Cette section fournit un scénario pou configurer la fonction de surveillance et de création de rapports dans Kaspersky Security Center.

Prérequis

Une fois que vous avez déployé Kaspersky Security Center sur le réseau d'une entreprise, vous pouvez commencer à le surveiller et obtenir des rapports opérationnels.

La surveillance et la création de rapports dans le réseau d'une organisation se déroulent par étapes :

1. **Configuration de la permutation des états des appareils**

   Familiarisez-vous avec les paramètres d'état des appareils qui dépendent de conditions spécifiques. En changeant ces paramètres, vous pouvez changer le nombre d'événements de niveau *Critique* ou *Avertissement*. Lorsque vous configurez le changement de statut de l'appareil, assurez-vous que :

   - Les nouveaux paramètres ne contreviennent pas aux stratégies de sécurité de l'information de votre organisation.
   - Vous pouvez réagir rapidement aux événements de sécurité importants sur le réseau de votre organisation.

2. **Configuration des notifications sur les événements survenus sur les appareils clients :**

   Instructions pour :

   Configurer la notification (par email, par SMS ou en exécutant un fichier exécutable) d'événements sur les appareils clients

3. **Modification de la réaction de votre réseau de sécurité à l'événement Attaque de virus**

   Vous pouvez configurer les seuils spécifiques dans les propriétés du Serveur d'administration. Vous pouvez également créer une stratégie plus stricte qui sera activée ou créer une tâche qui sera exécutée quand l'événement se produira.

4. **Exécution des actions recommandées pour les notifications critiques et d'avertissement**

   Instructions pour :

   Effectuer les actions recommandées pour le réseau de votre organisation

5. **Vérification de l'état de la sécurité du réseau de votre organisation**

   Instructions pour :

   - Examiner le widget État de la protection
   - Générer et examiner le Rapport sur l'état de la protection
   - Générez et contrôlez le Rapport sur les erreurs

6. **Localisation des appareils clients non protégés**

   Instructions pour :

   - Contrôlez le widget Nouveaux appareils
   - Générez et contrôlez le Rapport sur le déploiement de la protection

7. **Vérification de la protection des appareils clients**

   Instructions pour :

   - Générer et examiner les rapports des catégories État de la protection et Statistiques des menaces
   - Démarrer et examiner la sélection d'événements Critique

8. **Évaluation et limitation de la charge d'événements sur la base de données**

   Les informations sur les événements qui se produisent pendant le fonctionnement des applications administrées sont transmises de l'appareil client et enregistrées dans la base de données du Serveur d'administration. Pour réduire la charge sur le Serveur d'administration, évaluez et limitez le nombre maximal d'événements stockables dans la base de données.

Instructions pour :

- Calcul de l'espace dans la base de données
- Limiter le nombre maximum d'événements

9. **Contrôle des informations de licence**

   Instructions pour :

   - Ajouter le widget Utilisation de la clé de licence au tableau de bord et l'examiner
   - Générez et contrôlez le Rapport sur les clés de licence utilisées

Résultats

Une fois le scénario terminé, vous êtes informé de la protection du réseau de votre organisation et pouvez donc planifier des actions pour renforcer la protection.

À propos des types de surveillance et de rapport

Les informations relatives aux événements de sécurité dans un réseau d'organisation sont conservées dans la base de données du Serveur d'administration. Sur la base des événements, Kaspersky Security Center Web Console offre les types suivants de surveillance et de création des rapports sur le réseau de votre entreprise :

- Tableau de bord
- Rapports
- Sélections d'événements
- Notifications

Tableau de bord

Le tableau de bord vous permet de contrôler visuellement les données graphiques des tendances de la sécurité du réseau de votre organisation.

Rapports

Les rapports permettent d'obtenir des informations numériques détaillées sur la sécurité du réseau de votre organisation, d'enregistrer ces informations dans un fichier, de les envoyer par email et les imprimer.

Sélections d'événements

Sélections d'événements fournissent une vue à l'écran d'ensembles d'événements nommés stockés dans la base de données du Serveur d'administration. Ces ensembles d'événements sont regroupés selon les catégories suivantes :

- Par niveau d'importance — **Événements critiques**, **Erreurs de fonctionnement**, **Avertissements** et **Événements d'information**
- Chronologiquement — **Derniers événements**
- Par type — **Requêtes des utilisateurs** et **Événements de l'audit**

Vous pouvez créer et voir les sélections d'événements définies par l'utilisateur sur la base des paramètres disponibles, dans l'interface de Kaspersky Security Center Web Console pour configuration.

Notifications

Les notifications servent à vous alerter des événements et vous permettent d'accélérer la réaction à ces événements en effectuant rapidement les actions recommandées ou que vous estimez appropriées.

Tableau de bord et widgets

Cette section contient des informations sur le tableau de bord et les widgets qu'il propose. La section comprend des instructions sur la gestion des widgets et la configuration des paramètres des widgets.

À propos du tableau de bord

Le tableau de bord vous permet de contrôler visuellement les données graphiques des tendances de la sécurité du réseau de votre organisation.

Le tableau de bord est disponible dans Kaspersky Security Center Web Console, dans la section **Surveillance et rapports**, en cliquant sur **Tableau de bord**.

Le tableau de bord fournit des widgets qui peuvent être personnalisés. Vous pouvez choisir parmi une grande quantité de widgets différents, sous la forme de diagrammes circulaires, tableaux, graphiques, diagrammes en barre et listes. Les informations affichées dans les widgets sont automatiquement mises à jour, la période de mise à jour est d'une à deux minutes. L'intervalle entre les mises à jour varie selon les différents widgets. Vous pouvez actualiser les données sur un widget manuellement à tout moment à l'aide du menu de paramètres.

Par défaut, les widgets incluent des informations sur tous les événements stockés dans la base de données du Serveur d'administration.

Kaspersky Security Center Web Console contient un groupe de widgets par défaut dans les catégories suivantes :

- **État de la protection**
- **Déploiement**
- **Mise à jour**
- **Statistiques des menaces**
- **Autre**

Certains widgets contiennent des informations au format texte avec des liens. Vous pouvez visualiser le détail des informations en cliquant sur un lien.

Lors de la configuration du tableau de bord, vous pouvez ajouter les widgets dont vous avez besoin, masquer les widgets dont vous n'avez pas besoin, changer la taille ou l'apparence des widgets, déplacer des widgets, et modifier leurs paramètres.

Ajout de widgets au tableau de bord

Pour ajouter des widgets au tableau de bord :

1. Dans le menu principal, accédez à **Surveillance et rapports** → **Tableau de bord**.
2. Cliquez sur le bouton **Ajouter ou restaurer un widget web**.
3. Sélectionnez dans la liste des widgets disponibles ceux que vous souhaitez ajouter au tableau de bord.

   Les widgets sont organisés en catégories. Pour voir la liste des widgets inclus dans une catégorie, cliquez sur l'icône en chevron (›) en regard du nom de la catégorie.
4. Cliquez sur le bouton **Ajouter**.

Les widgets sélectionnés sont ajoutés à la fin du tableau de bord.

Vous pouvez alors modifier la représentation et les paramètres des widgets ajoutés.

Dissimulation d'un widget dans le tableau de bord

Pour masquer un widget affiché sur le tableau de bord :

1. Dans le menu principal, accédez à **Surveillance et rapports** → **Tableau de bord**.
2. Cliquez sur l'icône des paramètres (⚙) en regard du widget que vous souhaitez masquer.
3. Sélectionnez **Masquer le widget web**.
4. Dans la fenêtre **Avertissement** qui s'ouvre, cliquez sur **OK**.

Le widget sélectionné est masqué. Plus tard, vous pourrez à nouveau ajouter ce widget au tableau de bord.

Déplacement d'un widget sur le tableau de bord

Pour déplacer un widget sur le tableau de bord, procédez comme suit :

1. Dans le menu principal, accédez à **Surveillance et rapports** → **Tableau de bord**.
2. Cliquez sur l'icône des paramètres (⚙) en regard du widget que vous souhaitez déplacer.

3. Sélectionnez **Déplacer**.

4. Cliquez sur l'endroit vers lequel vous souhaitez déplacer le widget. Vous pouvez sélectionner uniquement un autre widget.

Les widgets sélectionnés permutent de position.

Modification de la taille et de l'apparence du widget

S'agissant des widgets qui affichent un diagramme, vous pouvez modifier la représentation : barres ou lignes. Certains widgets acceptent une modification de la taille : compact, moyen ou maximal.

Pour modifier la représentation d'un widget, procédez comme suit :

1. Dans le menu principal, accédez à **Surveillance et rapports → Tableau de bord**.

2. Cliquez sur l'icône des paramètres (⚙) en regard du widget que vous souhaitez modifier.

3. Exécutez une des actions suivantes :

   - Pour afficher le widget en tant que graphique à barres, sélectionnez **Type de graphique : barres**.
   - Pour afficher le widget en tant que graphique à lignes, sélectionnez **Type de graphique : courbes**.
   - Pour modifier la zone occupée par le widget, sélectionnez l'une des valeurs suivantes :
     - **Compact**
     - **Compact (barre seulement)**
     - **Moyen (graphique en anneau)**
     - **Moyen (graphique à barres)**
     - **Maximal**

La représentation du widget sélectionné change.

Modification des réglages d'un widget

Pour modifier les réglages d'un widget :

1. Dans le menu principal, accédez à **Surveillance et rapports → Tableau de bord**.

2. Cliquez sur l'icône des paramètres (⚙) en regard du widget que vous souhaitez modifier.

3. Sélectionnez **Afficher les paramètres**.

4. Dans la fenêtre des paramètres du widget qui s'ouvre, modifiez les paramètres du widget selon vos besoins.

5. Cliquez sur le bouton **Enregistrer** afin d'enregistrer les modifications.

Les paramètres du widget sélectionnés sont modifiés.

L'ensemble de paramètres dépend de chaque widget. Ci-dessous figurent quelques paramètres habituels :

- **Portée du widget web** (l'ensemble d'objets pour lesquels le widget affiche des informations) : par exemple, un groupe d'administration ou une sélection d'appareils.
- **Sélectionnez une tâche** (la tâche pour laquelle le widget affiche des informations).
- **Période** (la période pendant laquelle les informations sont affichées dans le widget) : entre deux dates définies ; depuis une date définie jusqu'au jour actuel ; jusqu'à un nombre de jours défini avant le jour actuel.
- **Définir l'état comme "Critique" si** et **Définir l'état comme "Avertissement" si** (les règles qui déterminent la couleur d'un indicateur de couleur).

Après avoir modifié les paramètres du widget, vous pouvez mettre à jour manuellement les données sur le widget.

Pour mettre à jour les données d'un widget, procédez comme suit :

1. Dans le menu principal, accédez à **Surveillance et rapports → Tableau de bord**.
2. Cliquez sur l'icône des paramètres (⚙) en regard du widget que vous souhaitez déplacer.
3. Sélectionnez **Actualiser**.

Les données du widget sont à jour.

À propos le mode Tableau de bord uniquement

Vous pouvez configurer le mode Tableau de bord uniquement pour les employés qui ne gèrent pas le réseau mais qui souhaitent consulter les statistiques de protection du réseau dans Kaspersky Security Center (par exemple, un cadre supérieur). Lorsqu'un utilisateur a activé ce mode, seul un tableau de bord avec un ensemble prédéfini de widgets s'affiche pour l'utilisateur. Ainsi, il peut suivre les statistiques indiquées dans les widgets, par exemple, l'état de la protection de tous les appareils administrés, le nombre de menaces récemment détectées ou la liste des menaces les plus fréquentes sur le réseau.

Lorsqu'un utilisateur travaille en mode Tableau de bord uniquement, les restrictions suivantes s'appliquent :

- Le menu principal ne s'affiche pas pour l'utilisateur, il ne peut donc pas modifier les paramètres de protection du réseau.
- L'utilisateur ne peut effectuer aucune action avec les widgets, par exemple les ajouter ou les masquer. Par conséquent, vous devez placer tous les widgets requis pour l'utilisateur sur le tableau de bord et les configurer, par exemple, définir la règle de comptage des objets ou spécifier l'intervalle de temps.

Vous ne pouvez pas vous attribuer le mode Tableau de bord uniquement. Si vous souhaitez travailler dans ce mode, contactez un administrateur système, un prestataire de services administrés (MSP) ou un utilisateur doté du droit **Modifier les ACL d'objets** dans la zone fonctionnelle **Fonctionnalités générales : Autorisations utilisateur**.

Configuration du mode Tableau de bord uniquement

Avant de commencer à configurer le mode Tableau de bord uniquement, assurez-vous que les conditions préalables suivantes sont réunies :

- Vous disposez du droit **Modifier les ACL d'objets** dans la zone fonctionnelle **Fonctionnalités générales : Autorisations utilisateur**. Si vous n'avez pas ce droit, l'onglet de configuration du mode sera manquant.
- Accorde les droits de **lecture** dans la zone fonctionnelle **Fonctionnalités générales : Fonctionnalité de base**.

Si une hiérarchie de Serveurs d'administration est organisée dans votre réseau, pour configurer le mode Tableau de bord seul, rendez-vous sur le Serveur où le compte utilisateur est disponible sous l'onglet **Utilisateurs** de la section **Utilisateurs et rôles → Utilisateurs et groupes**. Il peut s'agir d'un serveur principal ou d'un serveur secondaire physique. Il n'est pas possible de régler le mode sur un serveur virtuel.

Pour configurer le mode Tableau de bord uniquement :

1. Dans le menu principal, accédez à **Utilisateurs et rôles → Utilisateurs et groupes**, puis sélectionnez l'onglet **Utilisateurs**.
2. Cliquez sur le nom du compte utilisateur dont vous souhaitez ajuster le tableau de bord avec des widgets.
3. Dans la fenêtre des paramètres du compte qui s'ouvre, cliquez sur l'onglet **Tableau de bord**.

   Sur l'onglet qui s'ouvre, le même tableau de bord s'affiche pour vous et pour l'utilisateur.
4. Si l'option **Afficher la console en mode Tableau de bord uniquement** est activée, basculez le bouton bascule pour la désactiver.

   Lorsque cette option est activée, vous ne pouvez pas non plus modifier le tableau de bord. Après avoir désactivé l'option, vous pouvez gérer les widgets.
5. Configurez l'apparence du tableau de bord. L'ensemble des widgets préparés sur l'onglet **Tableau de bord** est disponible pour l'utilisateur avec le compte personnalisable. Il ou elle ne peut pas modifier les paramètres ou la taille des widgets, ajouter ou supprimer des widgets du tableau de bord. Par conséquent, ajustez-les pour l'utilisateur afin qu'il puisse consulter les statistiques de protection du réseau. Pour cela, dans l'onglet **Tableau de bord**, vous pouvez réaliser les mêmes actions avec les widgets que dans la section **Surveillance et rapports → Tableau de bord** :

   - Ajoutez des nouveaux widgets au tableau de bord.
   - Cachez les widgets dont l'utilisateur n'a pas besoin.
   - Déplacez les widgets dans un ordre spécifique.
   - Modifiez la taille ou l'apparence des widgets.
   - Modifiez les paramètres du widget.

6. Basculez le bouton à bascule pour activer l'option **Afficher la console en mode Tableau de bord uniquement**.

   Après cela, seul le tableau de bord est disponible pour l'utilisateur. Il peut surveiller les statistiques mais ne peut pas modifier les paramètres de protection du réseau ni l'apparence du tableau de bord. Comme le même tableau de bord s'affiche pour vous et pour l'utilisateur, vous ne pouvez pas non plus modifier le tableau de bord.

   Si vous laissez l'option désactivée, le menu principal s'affiche pour l'utilisateur afin qu'il puisse effectuer diverses actions dans Kaspersky Security Center, y compris la modification des paramètres de sécurité et des widgets.

7. Cliquez sur le bouton **Enregistrer** lorsque vous avez terminé de configurer le mode Tableau de bord uniquement. Ce n'est qu'après cela que le tableau de bord préparé sera affiché pour l'utilisateur.

8. Si l'utilisateur souhaite consulter les statistiques des applications Kaspersky prises en charge et a besoin de droits d'accès pour ce faire, configurez les droits de l'utilisateur. Après cela, les données des applications Kaspersky s'affichent pour l'utilisateur dans les widgets de ces applications.

L'utilisateur peut désormais se connecter à Kaspersky Security Center sous le compte personnalisé et suivre les statistiques de protection du réseau en mode Tableau de bord uniquement.

Rapports

Cette section décrit comment utiliser les rapports, gérer les modèles de rapport personnalisés, utiliser les modèles de rapport pour générer de nouveaux rapports et créer des tâches de remise de rapports.

Utilisation des rapports

Les rapports permettent d'obtenir des informations numériques détaillées sur la sécurité du réseau de votre organisation, d'enregistrer ces informations dans un fichier, de les envoyer par email et les imprimer.

Les rapports sont disponibles dans Kaspersky Security Center Web Console, dans la section **Surveillance et rapports**, en cliquant sur **Rapports**.

Par défaut, les rapports incluent des informations sur les 30 derniers jours.

Kaspersky Security Center contient un groupe de rapports par défaut dans les catégories suivantes :

- **État de la protection**
- **Déploiement**
- **Mise à jour**
- **Statistiques des menaces**
- **Autre**

Vous pouvez créer des modèles de rapports personnalisés, modifier des modèles de rapport, et les supprimer.

Vous pouvez créer des rapports qui sont basés sur des modèles existants, exporter des rapports vers des fichiers et créer des tâches pour la remise des rapports.

Créer le nouveau rapport

Pour créer un modèle de rapport, procédez comme suit :

1. Dans le menu principal, accédez à **Surveillance et rapports** → **Rapports**.
2. Cliquez sur **Ajouter**.

   Finalement, l'assistant de création du modèle du rapport se lancera. Parcourez les étapes de l'assistant à l'aide du bouton **Suivant**.
3. Saisissez le nom du rapport, puis sélectionnez le type de rapport.
4. À l'étape **Zone d'action** de l'assistant, sélectionnez l'ensemble d'appareils clients (groupe d'administration, sélection d'appareil, appareils sélectionnés, ou tous les appareils du réseau) dont les données seront reprises dans les rapports créés au départ de ce modèle de rapport.
5. À l'étape **Période du rapport** de l'assistant, définissez la période du rapport. Les valeurs disponibles sont les suivantes :

   - Entre deux dates définies
   - Depuis la date définie jusqu'à la date de création du rapport
   - Depuis la date de création du rapport moins le nombre de jours indiqué avant la date de création du rapport

   Cette page peut ne pas apparaître avec certains rapports.
6. Cliquez sur le bouton **OK** pour quitter l'Assistant.
7. Exécutez une des actions suivantes :

   - Cliquez sur le bouton **Enregistrer et exécuter** pour enregistrer le nouveau modèle de rapport et pour exécuter un rapport créé sur la base de ce modèle.

     Le modèle de rapport est enregistré. Le rapport est créé.
   - Cliquez sur le bouton **Enregistrer** pour enregistrer le nouveau modèle de rapport.

     Le modèle de rapport est enregistré.

Ce nouveau modèle peut être utilisé pour créer et afficher des rapports.

Consultation et modification des propriétés du modèle de rapport

Vous pouvez consulter et modifier les propriétés de base d'un modèle de rapport par exemple, le nom du modèle de rapport ou les champs affichés dans le rapport.

Pour consulter et modifier les propriétés d'un modèle de rapport :

1. Dans le menu principal, accédez à **Surveillance et rapports → Rapports**.
2. Cochez la case en regard du modèle de rapport dont vous souhaitez consulter et modifier les propriétés.
   Vous pouvez également d'abord créé le rapport, puis cliquer sur le bouton **Modifier**.
3. Cliquez sur le bouton **Ouvrir les propriétés du modèle de rapport**.
   La fenêtre **Édition du rapport <nom du rapport>** s'ouvre à l'onglet **Général**.

4. Modifiez les propriétés du modèle de rapport.

- Onglet **Général** :
  - Nom du modèle de rapport
  - **Nombre maximal d'entrées affichées**

    Quand cette option est activée, le nombre d'entrées affichées dans le tableau contenant les données détaillées du rapport ne peut être supérieur à la valeur indiquée.

    Les entrées du rapport sont tout d'abord classées en fonction des règles définies dans la section **Champs** → **Champs d'informations** des propriétés des modèles de rapport, puis seule la première des entrées obtenues est conservée. L'en-tête du tableau contenant les données détaillées du rapport reprend le nombre d'entrées affichées et le nombre total d'entrées disponible qui correspondent aux autres paramètres du modèle de rapport.

    Quand cette option est désactivée, le tableau contenant les données détaillées du rapport affiche toutes les entrées disponibles. Nous déconseillons de désactiver cette option. La restriction du nombre d'entrées affichées dans le rapport réduit la charge sur le système de gestion de base de données (SGBD) et réduit le temps requis pour la création et l'exportation du rapport. Certains rapports contiennent trop d'entrées. Dans ce cas, il peut être difficile de les lire et de les analyser tous. Aussi, votre appareil pourrait épuiser sa mémoire lors de la création de ces rapports et vous empêcher de les visualiser.

    Cette option est activée par défaut. La valeur par défaut est égale à 1000.

  - **Groupe**

    Cliquez sur le bouton **Paramètres** pour changer l'ensemble d'appareils clients pour lequel le rapport est créé. Pour certains types de rapports, le bouton est parfois indisponible. Les paramètres réels varient en fonction des paramètres définis lors de la création du modèle de rapport.

  - **Période**

    Cliquez sur le bouton **Paramètres** pour modifier la période du rapport. Pour certains types de rapports, le bouton est parfois indisponible. Les valeurs disponibles sont les suivantes :

    - Entre deux dates définies
    - Depuis la date définie jusqu'à la date de création du rapport
    - Depuis la date de création du rapport moins le nombre de jours indiqué avant la date de création du rapport

  - **Inclure les données à partir des Serveurs d'administration secondaires et virtuels**

    Quand cette option est activée, le rapport reprend les informations des Serveurs d'administration secondaires et virtuels placés sous le Serveur d'administration pour lequel le modèle de rapport est créé.

    Désactivez cette option si vous souhaitez voir les données uniquement pour le Serveur d'administration actuel.

    Cette option est activée par défaut.

  - **Jusqu'au niveau d'imbrication**

Le rapport contient les données des Serveurs d'administration secondaires et virtuels placés sous le Serveur d'administration actuel à un niveau d'imbrication inférieur ou égal à la valeur indiquée.

La valeur par défaut est de 1. Vous pouvez modifier cette valeur si vous devez obtenir des informations des Serveurs d'administration secondaires situés à des niveaux inférieurs dans l'arborescence.

- **Intervalle d'attente des données (min.)**

  Avant de créer le rapport, le Serveur d'administration pour lequel le modèle de rapport est créé attend les données des Serveurs d'administration secondaires pendant le nombre de minutes indiqué. Si le Serveur d'administration secondaire n'a envoyé aucune donnée à l'issue de cette période, le rapport est créé malgré tout. Au lieu des données réelles, le rapport affiche des données tirées du cache (si l'option **Mettre en cache les données des Serveurs d'administration secondaires** est activée) ou **N/A** (non disponible) dans le cas contraire.

  La valeur par défaut est de 5 (minutes).

- **Mettre en cache les données des Serveurs d'administration secondaires**

  Les Serveurs d'administration secondaires transmettent régulièrement des données au Serveur d'administration pour lequel le rapport est créé. Là, les données transmises sont placées dans le cache.

  Quand le Serveur d'administration actuel ne peut recevoir les données d'un Serveur d'administration secondaire lors de la création du rapport, le rapport affiche les données tirées du cache. La date de placement des données dans le cache est également affichée.

  L'activation de cette option permet de consulter les informations de Serveurs d'administration secondaires même lorsqu'il est impossible de récupérer les données à jour. Les données affichées peuvent toutefois être obsolètes.

  Cette option est Inactif par défaut.

- **Fréquence de mise à jour des données en cache (h.)**

  Les Serveurs d'administration secondaires transmettent à intervalles réguliers des données au Serveur d'administration pour lequel le rapport est créé. Vous pouvez spécifier cette période en heures. Une valeur égale à 0 signifie que les données sont transférées uniquement lorsque le rapport est créé.

  La valeur par défaut est égale à 0.

- **Transmettre des informations détaillées à partir des Serveurs d'administration secondaires**

  Dans le rapport généré, le tableau contenant les données détaillées du rapport reprend les données des Serveurs d'administration secondaires du Serveur d'administration pour lequel le modèle de rapport est créé.

  L'activation de cette option ralentit la création du rapport et augment le trafic entre les Serveurs d'administration. Toutefois, elle permet de consulter toutes les données dans un rapport.

  Au lieu d'activer cette option, vous pouvez analyser les données détaillées de rapport afin de détecter un Serveur d'administration secondaire défectueux, puis générer le même rapport uniquement pour celui-ci.

  Cette option est Inactif par défaut.

- Onglet **Champs**

  Sélectionnez les champs qui seront affichés dans le rapport, et utilisez les boutons **Haut** et **Bas** pour changer l'ordre des champs. Cliquez sur le bouton **Ajouter** ou **Modifier** pour indiquer si les informations du rapport doivent être triées et filtrées selon chaque filtre.

  Dans la section **Filtres des champs Détails**, vous pouvez également cliquer sur le bouton **Convertir les filtres** pour commencer à utiliser le format de filtrage étendu. Ce format vous permet de combiner les conditions de filtrage précisées dans divers champs à l'aide de l'opération logique OU. Après avoir cliqué sur le bouton, le panneau **Convertir les filtres** s'ouvre sur la droite. Cliquez sur le bouton **Convertir les filtres** pour confirmer la conversion. Vous pouvez maintenant définir un filtre converti avec les conditions de la section **Champs d'informations** appliquées à l'aide de l'opération logique OU.

  > La conversion d'un rapport au format prenant en charge des conditions de filtrage complexes le rendra incompatible avec les versions précédentes de Kaspersky Security Center (11 et antérieures). De plus, le rapport converti ne contiendra aucune donnée des Serveurs d'administration secondaires exécutant ces versions incompatibles.

5. Cliquez sur le bouton **Enregistrer** afin d'enregistrer les modifications.
6. Fermez la fenêtre **Modification du rapport <Nom du rapport>**.

Le modèle de rapport mis à jour apparaît dans la liste des modèles de rapport.

Exportation d'un rapport dans un fichier

Vous pouvez exporter un rapport dans un fichier XML, HTML ou PDF.

Pour exporter un rapport dans un fichier, procédez comme suit :

1. Dans le menu principal, accédez à **Surveillance et rapports** → **Rapports**.
2. Cochez la case en regard du rapport que vous souhaitez exporter dans un fichier.
3. Cliquez sur le bouton **Rapport d'exportation**.
4. Dans la fenêtre qui s'ouvre, modifiez le nom du fichier du rapport dans le champ **Nom**. Par défaut, le nom du fichier correspond au nom du modèle de rapport sélectionné.
5. Sélectionnez le type de fichier du rapport : XML, HTML ou PDF.
6. Cliquez sur le bouton **Rapport d'exportation**.

   Le rapport au format sélectionné est téléchargé dans le dossier par défaut de votre appareil ou une fenêtre **Enregistrer sous** standard s'ouvre dans votre navigateur pour vous permettre d'enregistrer le fichier à l'emplacement de votre choix.

Le rapport est enregistré dans le fichier.

Génération et affichage d'un rapport

Pour former et consulter le rapport, procédez comme suit :

1. Dans le menu principal, accédez à **Surveillance et rapports → Rapports**.
2. Cliquez sur le nom du modèle de rapport que vous souhaitez utiliser pour créer un rapport.

   Un rapport utilisant le modèle sélectionné s'affiche.

Les données du rapport sont affichées conformément à la localisation définie pour le Serveur d'administration.

Le rapport affiche les données suivantes :

- Sous l'onglet **Récapitulatif** :
  - Le type et le nom du rapport, une brève description et la période couverte, ainsi que les informations sur la création d'un rapport créée pour un groupe d'appareils.
  - Graphique présentant les données les plus représentatives du rapport.
  - Tableau récapitulatif avec les indices énumérés du rapport.
- Dans l'onglet **En savoir plus**, un tableau contenant les données de rapport détaillées.

Création d'une tâche d'envoi du rapport

Vous pouvez créer une tâche qui enverra les rapports sélectionnés.

Pour créer une tâche de diffusion des rapports, procédez comme suit :

1. Dans le menu principal, accédez à **Surveillance et rapports → Rapports**.
2. Cochez les cases en regard des modèles de rapport pour lequel vous souhaitez créer une tâche de diffusion des rapports.
3. Cliquez sur le bouton **Créer une tâche d'envoi**.

   Ceci permet de lancer l'assistant de création d'une tâche. Parcourez les étapes de l'assistant à l'aide du bouton **Suivant**.
4. À l'étape **Paramètres de nouvelle tâche** de l'Assistant, saisissez le nom de la tâche.

   Le nom par défaut est **Envoi de rapports**. Si une tâche portant ce nom existe déjà, un numéro d'ordre (<N>) est ajouté au nom de la tâche.

5. À l'étape de **Configuration du rapport** de l'Assistant, configurez les paramètres suivants :

   a. Modèles de rapports que la tâche doit diffuser.

   b. Le format du rapport est HTML, XLS ou PDF.

      L'outil wkhtmltopdf est requis pour convertir un rapport au format PDF. Lorsque vous sélectionnez l'option PDF, le Serveur d'administration vérifie si l'outil wkhtmltopdf est installé sur l'appareil. Si l'outil n'est pas installé, l'application affiche un message indiquant la nécessité d'installer l'outil sur l'appareil du Serveur d'administration. Installez l'outil manuellement, puis passez à l'étape suivante.

   c. Si les rapports doivent être envoyés par email avec les paramètres d'envoi par email.

      Vous pouvez définir jusqu'à 20 adresses email. Pour séparer les adresses email, appuyez sur la touche **Entrée**. Vous pouvez également coller une liste d'adresses email séparées par une virgule, puis appuyer sur la touche **Entrée**.

   d. Si les rapports doivent être enregistrés dans un dossier, si les rapports précédemment enregistrés dans ce dossier doivent être remplacés, et si un compte utilisateur spécifique doit être utilisé pour accéder au dossier (pour un dossier partagé).

6. À l'étape **Planifier la tâche** de l'Assistant, sélectionnez la planification du lancement de la tâche.

   Voici les options disponibles de planification de la tâche :

- **Manuel**

  La tâche ne s'exécute pas automatiquement. Vous pouvez uniquement la lancer manuellement.

  Cette option est sélectionnée par défaut.

- **Toutes les N minutes**

  La tâche s'exécute régulièrement, à l'intervalle défini en minutes, à partir de l'heure indiquée le jour de la création de la tâche.

  La tâche s'exécute par défaut toutes les 30 minutes, à partir de l'heure actuelle du système.

- **Toutes les N heures**

  La tâche s'exécute régulièrement, selon l'intervalle défini en heures, à partir de la date et heure définis.

  La tâche s'exécute par défaut toutes les six heures à partir de la date et de l'heure actuelles du système.

- **Tous les N jours**

  La tâche s'exécute régulièrement, selon l'intervalle défini en jours. En outre, vous pouvez spécifier la date et l'heure de la première exécution de la tâche. Ces options supplémentaires deviennent disponibles si elles sont prises en charge par l'application pour laquelle vous créez la tâche.

  La tâche s'exécute par défaut chaque jour, à partir de la date et de l'heure actuelle du système.

- **Toutes les N semaines**

  La tâche s'exécute régulièrement, selon l'intervalle défini en semaines, le jour indiqué de la semaine et à l'heure indiquée.

  La tâche s'exécute par défaut chaque lundi à l'heure système actuelle.

- **Chaque mois**

  La tâche s'exécute régulièrement le jour du mois défini, à l'heure indiquée.

  Si le jour en question ne figure pas dans le mois, la tâche s'exécute le dernier jour.

  La tâche s'exécute par défaut le premier jour de chaque mois, à l'heure système actuelle.

- **Les jours indiqués**

  La tâche s'exécute régulièrement les jours du mois définis, à l'heure indiquée.

  Par défaut, aucun jour du mois n'est sélectionné. L'heure de début par défaut est 18:00.

- **Lors de la détection d'une attaque de virus**

La tâche s'exécute après un événement *Attaque de virus* de virus. Sélectionnez les types d'application qui vont surveiller les propagations de virus. Les types suivants de Application sont présent :

- Antivirus pour postes de travail et serveurs de fichiers
- Antivirus de protection du périmètre
- Antivirus pour systèmes de messagerie

Tous les types d'application sont cochés par défaut.

Il se peut que vous souhaitiez exécuter différentes tâches en fonction du type d'application de sécurité qui signale une propagation de virus. Dans ce cas, supprimez la sélection des types d'application dont vous n'avez pas besoin.

- Après l'exécution d'une autre tâche

La tâche actuelle démarre à la fin d'une autre tâche. Cette option ne fonctionne que si les deux tâches sont affectées aux mêmes appareils. Par exemple, vous pouvez exécuter la tâche *Administration des appareils* avec l'option **&Activer l'appareil** et, une fois celle-ci terminée, exécuter la tâche de *recherche de virus* comme tâche de déclenchement.

Il faut sélectionner la tâche de déclenchement dans le tableau et l'état avec lequel cette tâche doit se terminer (**Terminée avec succès** ou **Échec**).

Si nécessaire, vous pouvez rechercher, trier et filtrer les tâches dans le tableau comme suit :

- Saisissez le nom de la tâche dans le champ de recherche pour rechercher une tâche par son nom.
- Cliquez sur l'icône de tri pour trier les tâches par nom.

  Par défaut, les tâches sont triées par ordre alphabétique croissant.
- Cliquez sur l'icône du filtre, et dans la fenêtre qui s'ouvre, filtrez les tâches par groupe, puis cliquez sur le bouton **Appliquer**.

7. À cette étape de l'Assistant, configurez d'autres paramètres de planification de tâches :

- Dans la section **Calendrier de la tâche**, vérifiez ou reconfigurez la planification précédemment sélectionnée, puis définissez l'intervalle de temps, les jours du mois ou de la semaine, la condition de propagation de virus ou la fin d'une autre tâche comme déclencheur du lancement de celle-ci. Une heure de début peut également être définie dans cette section si la planification applicable est sélectionnée.

- Dans la section **Paramètres supplémentaires**, définissez les paramètres suivants :

  - **Lancer les tâches non exécutées**

    Cette option détermine le comportement d'une tâche si un appareil client n'est pas visible sur le réseau quand la tâche est sur le point de démarrer.

    Si la case est Activé, lors du lancement suivant de l'application de Kaspersky sur cet appareil client, une tentative de lancement de la tâche sera faite. Si la programmation de la tâche est **Manuel**, **Une fois** ou **Immédiatement**, la tâche est immédiatement lancée dès que l'appareil apparaît sur le réseau ou immédiatement après l'inclusion de l'appareil dans la zone d'action de la tâche.

    Si cette option est désactivée, seules les tâches planifiées s'exécutent sur les appareils clients. Pour les planifications **Manuel**, **Une fois** et **Immédiatement**, les tâches s'exécutent uniquement sur les appareils clients qui sont visibles sur le réseau. Par exemple, vous pouvez désactiver cette option pour une tâche qui consomme des ressources que vous voulez exécuter uniquement en dehors des heures de bureau.

    Cette option est Inactif par défaut.

  - **Adopter un décalage aléatoire automatique pour les lancements de tâche**

    Si cette option est activée, la tâche est lancée sur les appareils clients de manière aléatoire au cours d'un intervalle défini. C'est ce qu'on appelle un *lancement échelonné d'une tâche*. Un lancement échelonné de tâche permet d'éviter la communication simultanée d'un nombre important d'appareils clients avec le Serveur d'administration lors du lancement de la tâche programmée.

    Le temps du lancement aléatoire est automatiquement calculée lors de la création d'une tâche selon le nombre d'appareils clients sur lesquels la tâche est diffusée. Par la suite, la tâche démarre toujours à l'heure de lancement calculée. Toutefois, quand les paramètres de la tâche sont modifiés ou si la tâche est lancée manuellement, la valeur calculée de l'heure de lancement de la tâche est modifiée.

    Si la case n'est pas cochée, le lancement de la tâche sur les appareils clients s'opère selon la planification.

  - **Décaler aléatoirement et automatiquement le lancement de la tâche dans un intervalle de**

    Si cette option est activée, la tâche est lancée sur les appareils clients de manière aléatoire au cours de l'intervalle défini. Un lancement échelonné de tâche permet d'éviter la communication simultanée d'un nombre important d'appareils clients avec le Serveur d'administration lors du lancement de la tâche programmée.

    Si la case n'est pas cochée, le lancement de la tâche sur les appareils clients s'opère selon la planification.

    Cette option est Inactif par défaut. Par défaut, la valeur de cet intervalle est de une minute.

  - **Arrêter la tâche si elle prend plus de**

A l'issue du délai défini, la tâche s'arrête automatiquement, qu'elle soit finie ou non.

Activez cette option si vous souhaitez interrompre (ou arrêter) les tâches dont l'exécution dure trop longtemps.

Cette option est Inactif par défaut. La durée d'exécution de la tâche par défaut est de 120 minutes.

8. À l'étape **Sélection du compte utilisateur pour exécuter la tâche** de l'Assistant, indiquez les identifiants du compte utilisateur qui sera utilisé pour exécuter la tâche.

9. Si vous souhaitez modifier un autre paramètre de la tâche une fois que la tâche est créée, à l'étape **Fin de la création de la tâche** de l'Assistant, activez l'option **Ouvrir les détails de la tâche à la fin de la création** (cette option est activée par défaut).

10. Cliquez sur le bouton **Terminer** pour créer la tâche et fermer l'Assistant.

    La tâche de remise de rapports est créée. Si l'option **Ouvrir les détails de la tâche à la fin de la création** est activée, la fenêtre des paramètres de la tâche s'ouvre.

Suppression des modèles de rapport

Pour supprimer un ou plusieurs modèles de rapport, procédez comme suit :

1. Dans le menu principal, accédez à **Surveillance et rapports** → **Rapports**.

2. Cochez les cases en regard des modèles de rapport que vous souhaitez supprimer.

3. Cliquez sur le bouton **Supprimer**.

4. Dans la fenêtre qui s'ouvre, cliquez **OK** pour confirmer votre choix.

Les modèles de rapport sélectionnés sont supprimés. Si ces modèles de rapport ont été inclus dans les tâches de diffusion des rapports, ils sont également retirés des tâches.

Événements et sélections d'événements

Cette section fournit des informations sur les événements et les sélections d'événements, sur les types d'événements qui se produisent dans les modules de Kaspersky Security Center et sur la gestion du blocage d'événements fréquents.

À propos des événements de Kaspersky Security Center

Kaspersky Security Center vous permet d'obtenir des informations sur les événements survenus pendant le fonctionnement du Serveur d'administration et des applications Kaspersky installées sur les appareils administrés. Les informations relatives aux événements sont conservées dans la base de données du Serveur d'administration.

Types d'événement

Dans Kaspersky Security Center, il existe les types d'événements suivants :

- Événements généraux. Ces événements se produisent dans toutes les applications Kaspersky administrées. Voici un exemple d'événement général : Attaque de virus. Les événements généraux ont une syntaxe et une sémantique strictement définies. Les événements généraux sont utilisés, par exemple, dans les rapports et les tableaux de bord.

- Événements spécifiques aux applications Kaspersky administrées. Chaque application de Kaspersky administrée possède son propre ensemble d'événements.

Sources de l'événement

Les événements peuvent être générés par les applications suivantes :

- Modules de Kaspersky Security Center :
  - Serveur d'administration
  - Agent d'administration
  - Serveur MDM iOS
  - Serveur des appareils mobiles Exchange ActiveSync
- Applications Kaspersky administrées

  Pour en savoir plus sur les événements générés par les applications administrées par Kaspersky, veuillez consulter la documentation de l'application correspondante.

Vous pouvez consulter la liste complète des événements qui peuvent être générés par une application sous l'onglet **Configuration des événements** dans la stratégie de l'application. Pour le Serveur d'administration, vous pouvez également consulter la liste des événements dans les propriétés du Serveur d'administration.

Niveau d'importance des événements

Chaque événement possède le niveau d'importance personnel. En fonction des conditions dans lesquelles l'événement s'est produit, il peut recevoir un niveau d'importance différent. Il existe quatre niveaux d'importance pour les événements :

- *Événement critique* : événement qui indique l'apparition d'un problème critique qui peut entraîner une perte de données, un échec ou une erreur critique.

- *Erreur de fonctionnement* : événement qui indique l'apparition d'un problème sérieux, d'une erreur ou d'un échec survenu pendant le fonctionnement de l'application ou l'exécution de la procédure.

- *Avertissement* événement qui n'est pas forcément sérieux, mais qui pourrait entraîner des problèmes à l'avenir. Le plus souvent les événements appartiennent à la catégorie Avertissement, si vous pouvez rétablir le fonctionnement de l'application par la suite, sans perte de données ou de fonctions.

- *Information* : événement qui vise à informer sur la réussite d'une opération, le fonction adéquat de l'application ou la fin d'une procédure.

On définit pour chaque événement la durée de conservation pendant laquelle l'événement peut être consulté ou modifié dans Kaspersky Security Center. Certains événements ne sont pas conservés par défaut dans la base de données du Serveur d'administration car la durée de conservation définie pour ceux-ci est égale à zéro. L'exportation vers des systèmes externes est uniquement possible pour les événements conservés dans la base de données du Serveur d'administration depuis moins d'un jour.

Utilisation des sélections d'événements

Sélections d'événements fournissent une vue à l'écran d'ensembles d'événements nommés stockés dans la base de données du Serveur d'administration. Ces ensembles d'événements sont regroupés selon les catégories suivantes :

- Par niveau d'importance — **Événements critiques**, **Erreurs de fonctionnement**, **Avertissements** et **Événements d'information**
- Chronologiquement — **Derniers événements**
- Par type — **Requêtes des utilisateurs** et **Événements de l'audit**

Vous pouvez créer et voir les sélections d'événements définies par l'utilisateur sur la base des paramètres disponibles, dans l'interface de Kaspersky Security Center Web Console pour configuration.

Les sélections d'événements sont disponibles dans Kaspersky Security Center Web Console, dans la section **Surveillance et rapports**, en cliquant sur **Sélections d'événements**.

Par défaut, les sélections d'événements incluent des informations sur les 7 derniers jours.

Kaspersky Security Center offre un groupe par défaut de sélections (prédéfinies) d'événements :

- Événements de différents niveaux d'importance :
  - **Événements critique**
  - **Erreur de fonctionnement**
  - **Avertissements**
  - **Informations sur les événements**
- **Requêtes des utilisateurs** (événements d'applications administrées)
- **Derniers événements** (de la dernière semaine)
- **Événements d'audit**.

Vous pouvez également créer et configurer des sélections personnalisées. Dans les sélections personnalisées, vous pouvez filtrer les événements selon les propriétés des appareils d'où ils proviennent (nom des appareils, plages IP et groupes d'administration), par types d'événements et niveaux de gravité, par application et nom du composant et par période. Il est possible également d'inclure les résultats de la tâche dans la zone d'action de la recherche. Vous pouvez également utiliser un champ de recherche simple dans lequel vous saisirez un ou plusieurs mots. Dans ce cas, tous les événements qui contiennent n'importe lequel des mots saisis n'importe où dans les attributs (comme le nom de l'événement, la description ou le nom du composant) sont affichés.

Aussi bien pour les sélections prédéfinies que pour les sélections personnalisées, il est possible de réduire le nombre d'événements affichés ou le nombre d'enregistrements à chercher. Ces deux options ont un impact sur le temps qu'il faut à Kaspersky Security Center pour afficher ces événements. Plus la base de données est volumineuse, plus le processus peut prendre de temps.

Vous pouvez réaliser les opérations suivantes :

- Modifier les propriétés des sélections d'événements
- Générer des sélections d'événements
- Afficher les détails des sélections d'événements
- Supprimer des sélections d'événements
- Supprimer des événements de la base de données du Serveur d'administration

Création d'une sélection d'événements

Pour créer une sélection d'événements, procédez comme suit :

1. Dans le menu principal, accédez à **Surveillance et rapports** → **Sélections d'événements**.
2. Cliquez sur **Ajouter**.
3. Dans la fenêtre **Nouvelle sélection d'événements** qui s'ouvre, définissez les paramètres de la nouvelle sélection d'événements. Réalisez ceci dans une ou plusieurs sections de la fenêtre.
4. Cliquez sur le bouton **Enregistrer** afin d'enregistrer les modifications.

   La fenêtre de confirmation s'ouvre.
5. Pour voir les résultats de la sélection d'événements, ne décochez pas la case **Accéder au résultat de la sélection**.
6. Cliquez sur **Enregistrer** pour confirmer la création de la sélection d'événements.

Si vous n'avez pas décoché la case **Accéder au résultat de la sélection**, les résultats de la sélection d'événements sont affichés. Dans le cas contraire, la nouvelle sélection d'événements apparaît dans a liste des sélection d'événements.

Édition d'une sélection d'événements

Pour modifier une sélection d'événements, procédez comme suit :

1. Dans le menu principal, accédez à **Surveillance et rapports** → **Sélections d'événements**.
2. Cochez la case en regard de la sélection d'événements que vous souhaitez modifier.
3. Cliquez sur le bouton **Propriétés**.

   Une fenêtre avec les paramètres de la sélection d'événements s'ouvre.

4. Modifiez les propriétés de la sélection d'événements.

> Pour les sélections d'événements prédéfinies, vous pouvez modifier uniquement les propriétés sous les onglets suivants : **Général** (sauf pour le nom de la sélection), **Heure** et **Privilèges d'accès**.

Pour les sélections définies par l'utilisateur, vous pouvez modifier toutes les propriétés.

5. Cliquez sur le bouton **Enregistrer** afin d'enregistrer les modifications.

La sélection d'événements modifiée apparaît dans la liste.

Affichage d'une liste d'une sélection d'événements

Pour afficher une sélection d'événements, procédez comme suit :

1. Dans le menu principal, accédez à **Surveillance et rapports** → **Sélections d'événements**.
2. Cochez la case en regard de la sélection d'événements que vous souhaitez lancer.
3. Exécutez une des actions suivantes :
   - Si vous souhaitez configurer le tri dans le résultat de la sélection d'événements, procédez comme suit :
     a. Cliquez sur le bouton **Reconfigurer le tri et démarrer**.
     b. Dans la fenêtre ouverte **Reconfigurer le tri pour la sélection d'événements**, définissez les paramètres de tri.
     c. Cliquez sur le nom de la sélection.
   - Sinon, si vous souhaitez afficher la liste des événements tels qu'ils sont triés sur le Serveur d'administration, cliquez sur le nom de la sélection.

Le résultat de la sélection d'événements s'affiche.

Exportation d'une sélection d'événements

Kaspersky Security Center vous permet d'enregistrer une sélection d'événements et ses paramètres dans un fichier KLO. Vous pouvez utiliser ce fichier KLO pour importer la sélection d'événements enregistrés dans Kaspersky Security Center Windows et Kaspersky Security Center Linux.

> Notez que vous pouvez exporter uniquement les sélections d'événements définis par l'utilisateur. Les sélections d'événements de l'ensemble par défaut de Kaspersky Security Center (sélections prédéfinies) ne peuvent pas être enregistrées dans un fichier.

Pour exporter une sélection d'événements, procédez comme suit :

1. Dans le menu principal, accédez à **Surveillance et rapports → Sélections d'événements**.
2. Cochez la case en regard de la sélection d'événements que vous souhaitez exporter.

   Vous ne pouvez pas exporter plusieurs sélections d'événements à la fois. Si vous sélectionnez plusieurs sélections, le bouton **Exporter** sera désactivé.
3. Cliquez sur le bouton **Exporter**.
4. Dans la fenêtre **Enregistrer sous** qui s'ouvre, indiquez le nom et le chemin du fichier de sélection d'événements, puis cliquez sur le bouton **Enregistrer**.

   La fenêtre **Enregistrer sous** s'affiche uniquement si vous utilisez Google Chrome, Microsoft Edge ou Opera. Si vous utilisez un autre navigateur, le fichier de sélection d'événements est automatiquement enregistré dans le dossier **Téléchargements**.

Importation d'une sélection d'événements

Kaspersky Security Center vous permet d'importer une sélection d'événements à partir d'un fichier KLO. Le fichier KLO contient la sélection d'événements exportée et ses paramètres.

Pour importer une sélection d'événements, procédez comme suit :

1. Dans le menu principal, accédez à **Surveillance et rapports → Sélections d'événements**.
2. Cliquez sur le bouton **Importer**, puis choisissez un fichier de sélection d'événements à importer.
3. Dans la fenêtre ouverte, spécifiez le chemin d'accès au fichier KLO, puis cliquez sur le bouton **Ouvrir**. Notez que vous ne pouvez sélectionner qu'un seul fichier de sélection d'événements.

   Le traitement de la sélection d'événements démarre.

La notification avec les résultats de l'importation s'affiche. Si l'importation de la sélection d'événements a réussi, vous pouvez cliquer sur le lien **Afficher les détails de l'importation** pour afficher les propriétés de la sélection d'événements.

Après une importation réussie, la sélection d'événements s'affiche dans la liste de sélection. Les paramètres de la sélection d'événements sont également importés.

Si la sélection d'événements nouvellement importée a un nom identique à celui d'une sélection d'événements existante, le nom de la sélection importée est suivi de l'index **(<numéro de séquence suivant>)**, par exemple : **(1)**, **(2)**.

Affichage des détails d'un événement

Pour afficher les détails d'un événement :

1. Démarrage d'une sélection d'événements.
2. Cliquez sur l'heure de l'événement requis.
   La fenêtre des **Propriétés de l'événement** s'affiche.
3. Dans la fenêtre qui s'affiche, vous pouvez effectuer l'une des opérations suivantes :
   - Affichez les informations sur l'événement sélectionné
   - Accédez à l'événement suivant et précédent dans la résultat de la sélection d'événements
   - Accédez à l'appareil où l'événement s'est produit
   - Accédez au groupe d'administration qui inclut l'appareil sur lequel l'événement s'est produit
   - Pour un événement lié à une tâche, accédez aux propriétés de la tâche

Exportation des événements dans un fichier

Kaspersky Security Center permet d'enregistrer les événements de la sélection d'événements dans un fichier TXT.

Pour exporter des événements vers un fichier :

1. Démarrage d'une sélection d'événements.
2. Cochez la case à côté de l'événement requis.
   Vous pouvez également sélectionner plusieurs événements ou toute la sélection d'événements.
3. Cliquez sur le bouton **Exporter dans un fichier**.

L'événement sélectionné est exporté dans un fichier TXT.

Voir un historique d'objet à partir d'un événement

Pour un événement de création ou de modification d'un objet qui prend en charge la gestion des révisions, vous pouvez passer à l'historique des révisions de l'objet.

Pour voir un historique d'objet à partir d'un événement :

1. Démarrage d'une sélection d'événements.
2. Cochez la case à côté de l'événement requis.
3. Cliquez sur le bouton **Historique des révisions**.

L'Historique des révisions de l'objet est ouvert.

Supprimer des événements

Pour supprimer un ou plusieurs événements :

1. Démarrage d'une sélection d'événements.
2. Cochez la case à côté des événements requis.
3. Cliquez sur le bouton **Supprimer**.

Les événements sélectionnés sont supprimés et ne peuvent pas être restaurés.

Suppression de sélections d'événements

Vous ne pouvez supprimer que les sélection d'événements définies par les utilisateurs. Les sélections d'événement prédéfinies ne peuvent pas être supprimées.

Pour supprimer une ou plusieurs sélections d'événements, procédez comme suit :

1. Dans le menu principal, accédez à **Surveillance et rapports → Sélections d'événements**.
2. Cochez les cases en regard des sélections d'événements que vous souhaitez supprimer.
3. Cliquez sur **Supprimer**.
4. Dans la fenêtre qui s'ouvre, cliquez sur **OK**.

La sélection d'événements est supprimée.

Définition de la condition de stockage pour un événement

Kaspersky Security Center vous permet d'obtenir des informations sur les événements survenus pendant le fonctionnement du Serveur d'administration et des applications Kaspersky installées sur les appareils administrés. Les informations relatives aux événements sont conservées dans la base de données du Serveur d'administration. Vous pouvez avoir besoin de stocker certains événements pendant une période plus longue ou plus courte que celle indiquée par les valeurs par défaut. Vous pouvez modifier les paramètres par défaut de la condition de stockage pour un événement.

Si vous n'êtes pas intéressé par le stockage de certains événements dans la base de données du Serveur d'administration, vous pouvez désactiver le paramètre approprié dans la stratégie du Serveur d'administration et dans la stratégie de l'application Kaspersky, ou dans les propriétés du Serveur d'administration (uniquement pour les événements du Serveur d'administration). Cela réduit le nombre de types d'événements dans la base de données.

Plus la condition de stockage d'un événement est de longue durée, plus la base de données atteint rapidement sa capacité maximale. Toutefois, une condition de stockage de plus longue durée pour un événement vous permet d'effectuer des tâches de surveillance et rapports pendant une période plus longue.

Pour définir la condition de stockage d'un événement dans la base de données du Serveur d'administration :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Stratégies et profils**.
2. Cliquez sur le nom de la stratégie concernée.

   Vous pouvez sélectionner une stratégie d'une application Kaspersky gérée, d'un Agent d'administration du réseau ou d'un Serveur d'administration. Pour le Serveur d'administration, vous pouvez également configurer la durée de stockage des événements en cliquant sur l'icône des paramètres ( ) à côté du nom du Serveur d'administration requis.
3. Sélectionnez l'onglet **Configuration des événements**.

   La liste des types d'événements liés à la section **Critique** s'affiche. Le cas échéant, passez à la section **Erreur de fonctionnement**, **Avertissement** ou **Information**.
4. Dans la liste des types d'événements du volet droit, cliquez sur le lien de l'événement dont vous souhaitez modifier la condition de stockage.

   Dans la section **Enregistrement des événements** de la fenêtre qui s'ouvre, le commutateur **Conserver dans la base de données du Serveur pendant (jours)** est activé.
5. Dans la zone de modification au-dessous de ce bouton bascule, entrez le nombre de jours de stockage de l'événement.
6. Si vous ne souhaitez pas stocker un événement dans la base de données du Serveur d'administration, désactivez l'option **Conserver dans la base de données du Serveur pendant (jours)**.

   > Si vous configurez les événements du Serveur d'administration dans la fenêtre des propriétés du Serveur d'administration et si les paramètres des événements sont verrouillés dans la stratégie du Serveur d'administration de Kaspersky Security Center, vous ne pouvez pas redéfinir la valeur de la durée de stockage d'un événement.
7. Cliquez sur **OK**, puis après avoir fermé le volet droit, cliquez sur le bouton **Enregistrer**.

   La fenêtre des propriétés de la stratégie est fermée.

Désormais, lorsque le Serveur d'administration reçoit et mémorise les événements du type sélectionné, leur durée de conservation sera modifiée. Le Serveur d'administration ne modifie pas la durée de stockage des événements reçus précédemment.

Événements des modules de Kaspersky Security Center

Chaque module de Kaspersky Security Center possède son propre ensemble de types d'événements. Cette section reprend les types d'événements qui se produisent dans le Serveur d'administration de Kaspersky Security Center, l'Agent d'administration et le Serveur MDM iOS. Les types d'événements qui surviennent dans les applications de Kaspersky ne sont pas répertoriés dans cette section.

Pour chaque événement pouvant être généré par une application, vous pouvez spécifier les paramètres de notification et les paramètres de stockage sous l'onglet **Configuration des événements** dans la stratégie de l'application. Pour le Serveur d'administration, vous pouvez également consulter et configurer la liste des événements dans les propriétés du Serveur d'administration. Si vous souhaitez configurer les paramètres de notification pour tous les événements à la fois, configurez les paramètres de notification généraux dans les propriétés du Serveur d'administration.

Structure des données de la description du type d'événement

Pour chaque type d'événement, le nom affiché, l'identifiant (ID), le code alphabétique, la description et la durée de stockage par défaut sont fournis.

- **Nom affiché du type d'événement**. Ce texte est affiché dans Kaspersky Security Center lorsque vous configurez les événements et lorsqu'ils se produisent.
- **ID de type d'événement**. Ce code numérique est utilisé lorsque vous traitez des événements à l'aide d'outils tiers en vue d'une analyse.
- **Type d'événement** (code alphabétique). Ce code est utilisé lorsque vous naviguez parmi les événements et les traitez à l'aide des représentations publiques fournies dans la base de données de Kaspersky Security Center et lorsque les événements sont exportés dans un système SIEM.
- **Description**. Ce texte décrit les situations où l'événement se produit et ce qu'il faut faire dans ce cas.
- **Durée de stockage par défaut**. Il s'agit du nombre de jours pendant lesquels l'événement est conservé dans la base de données du Serveur d'administration et affiché dans la liste des événements sur le Serveur d'administration. A l'issue de cette période, l'événement est supprimé. Si la valeur du paramètre de conservation des événements est de 0, les événements sont détectés, mais ils ne sont pas affichés dans la liste des événements du Serveur d'administration. Si votre configuration prévoit l'enregistrement de ces événements dans le journal des événements du système d'exploitation, c'est là qu'il faudra les chercher.

  Vous pouvez modifier la durée de conservation pour les événements :

  - Console d'administration : définition de la condition de stockage pour un événement
  - Kaspersky Security Center Web Console : définition de la condition de stockage pour un événement

Les autres données peuvent inclure les champs suivants :

- **event_id** : numéro unique de l'événement dans la base de données, généré et attribué automatiquement ; à ne pas confondre avec l'**identifiant de type d'événement**.
- **task_id** : l'identifiant de la tâche qui a provoqué l'événement (le cas échéant)
- **severity** : l'un des niveaux de gravité suivants (dans l'ordre croissant de gravité) :

  0) Niveau de gravité incorrect

  1) Informations

  2) Avertissement

  3) Erreur

  4) Critique

Événements du Serveur d'administration

Cette section contient des informations sur les événements liés au serveur d'administration.

Événements critiques du Serveur d'administration

Le tableau ci-dessous indique les types d'événements du Serveur d'administration de Kaspersky Security Center, regroupés par niveau de gravité **Critique**.

Pour chaque événement pouvant être généré par une application, vous pouvez spécifier les paramètres de notification et les paramètres de stockage sous l'onglet **Configuration des événements** dans la stratégie de l'application. Pour le Serveur d'administration, vous pouvez également consulter et configurer la liste des événements dans les propriétés du Serveur d'administration. Si vous souhaitez configurer les paramètres de notification pour tous les événements à la fois, configurez les paramètres de notification généraux dans les propriétés du Serveur d'administration.

Si vous avez indiqué le port dans la fenêtre des propriétés du Serveur d'administration de la Console d'administration, **Kaspersky Security Center publie ses métriques** et ses événements critiques afin que le système de surveillance et d'alerte puisse les obtenir par Prometheus. Prometheus obtient les métriques et les événements critiques, puis génère des alertes pour chaque événement.

// KL.KSC.Common—Kaspersky Security Center common counters

"xdr_klserver_errors", "counter", "klserver errors"

"xdr_klserver_api_calls_time", "counter", "klserver api calls time"

// KL.KSC.Transport—Transport counters set

"ksc_Transport__Number_of_all_connections", "counter", "number of all connections"

"ksc_Transport__Number_of_all_nagent_connection", "counter", "number of all Network Agent connection"

"ksc_Transport__Number_of_controlled_nagent_connections", "counter", "number of controlled Network Agent connections"

"ksc_Transport__Total_active_hosts_count", "gauge", "total active devices count"

"ksc_Transport__Number_of_pings_processed", "counter", "number of pings processed"

"ksc_Transport__Number_of_pings_rejected", "counter", "number of pings rejected"

"ksc_Transport__Number_of_ping_processing_errors", "counter", "number of ping processing errors"

"ksc_Transport__Number_of_TCP_connections_accepted", "counter", "number of TCP connections accepted"

"ksc_Transport__Number_of_failed_TCP_connections", "counter", "number of failed TCP connections"

"ksc_Transport__Bytes_sent_by_TCP", "counter", "bytes sent by TCP"

"ksc_Transport__Bytes_received_by_TCP", "counter", "bytes received by TCP"

"ksc_Transport__Number_of_GetNextFileChunk_requests", "counter", "number of GetNextFileChunk requests"

"ksc_Transport__Number_of_GetNextFileChunk_rejected", "counter", "number of GetNextFileChunk rejected"

"ksc_Transport__Bytes_transmitted_through_GetNextFileChunk", "counter", "bytes transmitted through GetNextFileChunk"

// KL.KSC.Events—Events delivery counters set

"ksc_Events__Number_of_event_bulks_processed", "counter", "number of event bulks processed"

"ksc_Events__Number_of_event_bulks_rejected", "counter", "number of event bulks rejected"

"ksc_Events__Number_of_event_bulks_processing_errors", "counter", "number of event bulks processing errors"

"ksc_Events__Number_of_event_bulks_processing_just_now", "gauge", "number of event bulks processing just now"

"ksc_Events__Number_of_events_processed", "counter", "number of events processed"

"ksc_Events__Number_of_events_rejected", "counter", "number of events rejected"

"ksc_Events__Number_of_events_processing_errors", "counter", "number of events processing errors"

"ksc_Events__Number_of_events_processing_just_now", "gauge", "number of events processing just now"

// KL.KSC.Resources—Kaspersky Security Center resources usage

"ksc_Resources__CPU_time_in_user_mode", "counter", "CPU time in user mode"

"ksc_Resources__CPU_time_in_kernel_mode", "counter", "CPU time in kernel mode"

"ksc_Resources__PID_of_klserver_process", "gauge", "process ID of klserver"

"ksc_Resources__PID_of_klnagent_process", "gauge", "process ID of klnagent"

"ksc_Resources__Available_disk_user_quota_for_server_data", "gauge", "available disk user quota for server data"

"ksc_Resources__Available_disk_user_quota_for_packages", "gauge", "available disk user quota for packages"

"ksc_Resources__Current_OpenAPI_threads_count", "counter", "current OpenAPI threads count

"ksc_Resources__Maximum_OpenAPI_threads_count", "counter", "maximum OpenAPI threads count"

// KL.KSC.NLST

// KL.KSC.NLST.Trans.Common—List of server transactions

"ksc_NLST__Common__Current_transactions_count", "gauge", "current transactions count

"ksc_NLST__Common__Transactions_queue_ful", "gauge", "transactions queue full"

"ksc_NLST__Common__Transactions_queue_near_to_ful", "gauge", "transactions queue near to full"

// KL.KSC.NLST.InvAppCtrlLink—Application Control link

"ksc_NLST__Application_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Application_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Application_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Application_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Application_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Application_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Application_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Application_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Application_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.InvSoft—Software Inventory

"ksc_NLST__Software_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Software_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Software_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Software_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Software_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Software_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Software_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Software_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Software_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.InvHard—Hardware Inventory

"ksc_NLST__Hardware_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Hardware_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Hardware_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Hardware_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Hardware_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Hardware_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Hardware_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Hardware_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Hardware_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.DevCtrl—Device Control

"ksc_NLST__Device_control__items_changed", "gauge", "items changed"

"ksc_NLST__Device_control__items_deleted", "gauge", "items deleted"

"ksc_NLST__Device_control__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Device_control__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Device_control__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Device_control__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Device_control__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Device_control__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Device_control__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.MDM—Mobile Device Management

"ksc_NLST__Mobile_device_management__items_changed", "gauge", "items changed"

"ksc_NLST__Mobile_device_management__items_deleted", "gauge", "items deleted"

"ksc_NLST__Mobile_device_management__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Mobile_device_management__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Mobile_device_management__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Mobile_device_management__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Mobile_device_management__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Mobile_device_management__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Mobile_device_management__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.MDMmails—Device management emails

"ksc_NLST__Device_management_emails__items_changed", "gauge", "items changed"

"ksc_NLST__Device_management_emails__items_deleted", "gauge", "items deleted"

"ksc_NLST__Device_management_emails__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Device_management_emails__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Device_management_emails__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Device_management_emails__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Device_management_emails__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Device_management_emails__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Device_management_emails__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.AppCtrl—Application Control

"ksc_NLST__Application_control__items_changed", "gauge", "items changed"

"ksc_NLST__Application_control__items_deleted", "gauge", "items deleted"

"ksc_NLST__Application_control__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Application_control__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Application_control__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Application_control__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Application_control__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Application_control__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Application_control__transactions_in_queue", "gauge", "transactions in queue"

"ksc_NLST__Application_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Application_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Application_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Application_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Application_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Application_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Application_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Application_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Application_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.DPEErrors—Data protection errors

"ksc_NLST__Data_protection_errors__items_changed", "gauge", "items changed"

"ksc_NLST__Data_protection_errors__items_deleted", "gauge", "items deleted"

"ksc_NLST__Data_protection_errors__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Data_protection_errors__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Data_protection_errors__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Data_protection_errors__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Data_protection_errors__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Data_protection_errors__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Data_protection_errors__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.iOsMDM—iOS Mobile Device Management

"ksc_NLST__iOS_mobile_device_management__items_changed", "gauge", "items changed"

"ksc_NLST__iOS_mobile_device_management__items_deleted", "gauge", "items deleted"

"ksc_NLST__iOS_mobile_device_management__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__iOS_mobile_device_management__change_item_operations", "gauge", "change item operations"

"ksc_NLST__iOS_mobile_device_management__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__iOS_mobile_device_management__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__iOS_mobile_device_management__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__iOS_mobile_device_management__list_is_pending", "gauge", "list is pending"

"ksc_NLST__iOS_mobile_device_management__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.Vapm—Vulnerability assessment and patch management

"ksc_NLST__Vulnerability_assesment_and_patch_management__items_changed", "gauge", "items changed"

"ksc_NLST__Vulnerability_assesment_and_patch_management__items_deleted", "gauge", "items deleted"

"ksc_NLST__Vulnerability_assesment_and_patch_management__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Vulnerability_assesment_and_patch_management__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Vulnerability_assesment_and_patch_management__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Vulnerability_assesment_and_patch_management__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Vulnerability_assesment_and_patch_management__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Vulnerability_assesment_and_patch_management__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Vulnerability_assesment_and_patch_management__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.Va—Vulnerability assessment

"ksc_NLST__Vulnerability_assesment__items_changed", "gauge", "items changed"

"ksc_NLST__Vulnerability_assesment__items_deleted", "gauge", "items deleted"

"ksc_NLST__Vulnerability_assesment__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Vulnerability_assesment__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Vulnerability_assesment__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Vulnerability_assesment__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Vulnerability_assesment__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Vulnerability_assesment__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Vulnerability_assesment__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.VM—Virtual machines

"ksc_NLST__Virtual_machines__items_changed", "gauge", "items changed"

"ksc_NLST__Virtual_machines__items_deleted", "gauge", "items deleted"

"ksc_NLST__Virtual_machines__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Virtual_machines__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Virtual_machines__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Virtual_machines__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Virtual_machines__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Virtual_machines__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Virtual_machines__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.WUS—Windows Update

"ksc_NLST__Windows_update__items_changed", "gauge", "items changed"

"ksc_NLST__Windows_update__items_deleted", "gauge", "items deleted"

"ksc_NLST__Windows_update__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Windows_update__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Windows_update__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Windows_update__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Windows_update__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Windows_update__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Windows_update__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.CIP_PLC—CIP PLC

"ksc_NLST__CIP_PLC__items_changed", "gauge", "items changed"

"ksc_NLST__CIP_PLC__items_deleted", "gauge", "items deleted"

"ksc_NLST__CIP_PLC__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__CIP_PLC__change_item_operations", "gauge", "change item operations"

"ksc_NLST__CIP_PLC__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__CIP_PLC__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__CIP_PLC__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__CIP_PLC__list_is_pending", "gauge", "list is pending"

"ksc_NLST__CIP_PLC__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.NagentNetScan—Network Agent Network Scan

"ksc_NLST__Network_scan__items_changed", "gauge", "items changed"

"ksc_NLST__Network_scan__items_deleted", "gauge", "items deleted"

"ksc_NLST__Network_scan__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Network_scan__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Network_scan__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Network_scan__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Network_scan__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Network_scan__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Network_scan__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.AS—Adaptive Security

"ksc_NLST__Adaptive_security__items_changed", "gauge", "items changed"

"ksc_NLST__Adaptive_security__items_deleted", "gauge", "items deleted"

"ksc_NLST__Adaptive_security__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Adaptive_security__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Adaptive_security__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Adaptive_security__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Adaptive_security__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Adaptive_security__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Adaptive_security__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.ASS—Adaptive Security State

"ksc_NLST__Adaptive_security_state__items_changed", "gauge", "items changed"

"ksc_NLST__Adaptive_security_state__items_deleted", "gauge", "items deleted"

"ksc_NLST__Adaptive_security_state__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Adaptive_security_state__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Adaptive_security_state__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Adaptive_security_state__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Adaptive_security_state__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Adaptive_security_state__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Adaptive_security_state__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.KillChain—Kill Chain

"ksc_NLST__Kill_chain__items_changed", "gauge", "items changed"

"ksc_NLST__Kill_chain__items_deleted", "gauge", "items deleted"

"ksc_NLST__Kill_chain__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Kill_chain__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Kill_chain__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Kill_chain__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Kill_chain__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Kill_chain__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Kill_chain__transactions_in_queue", "gauge", "transactions in queue"

Nom affiché du type d'événement	ID de type d'événement	Type d'événement	Description	Durée de stockage par défaut
La restriction de la licence a été dépassée	4099	KLSRV_EV_LICENSE_CHECK_MORE_110	Une fois par jour, Kaspersky Security Center vérifie si une limite de licence est dépassée. Ce type d'événements se produit si le serveur d'administration détecte que certaines limites de licence sont dépassées par les applications Kaspersky installées sur les appareils clients et si le nombre d'unités de licence actuellement utilisé sous licence unique est supérieur à 110 % du nombre total d'unités sous licence. Même lorsque cet événement se produit, les appareils clients sont protégés. Vous pouvez répondre à l'événement des manières suivantes : • Parcourez la liste des appareils administrés. Supprimez les appareils inutilisés. • Fournissez une licence pour plusieurs appareils (ajoutez un code d'activation valide ou un fichier clé au serveur d'administration). Kaspersky Security Center définit les règles de génération d'événements lorsqu'une limite de la licence est dépassée.	180 jours
Attaque de virus	26 (pour la Protection contre les fichiers malicieux)	GNRL_EV_VIRUS_OUTBREAK	Ce type d'événements se produit lorsque le nombre d'objets malveillants détectés sur plusieurs appareils administrés dépasse le seuil sur une courte durée. Vous pouvez répondre à l'événement des manières suivantes : • Vous pouvez configurer le seuil dans les propriétés du Serveur d'administration. • Vous pouvez aussi créer une stratégie plus stricte qui sera activée ou créer une tâche qui sera exécutée quand l'événement se produit.	180 jours
Attaque de virus	27 (pour la Protection contre les menaces par emails)	GNRL_EV_VIRUS_OUTBREAK	Ce type d'événements se produit lorsque le nombre d'objets malveillants détectés sur plusieurs appareils administrés dépasse le seuil sur une courte durée. Vous pouvez répondre à l'événement des manières suivantes : • Vous pouvez configurer le seuil dans les propriétés du Serveur d'administration. • Vous pouvez aussi créer une stratégie plus stricte qui sera activée ou créer une tâche qui sera exécutée quand l'événement se produit.	180 jours
Attaque de virus	28 (pour le pare-feu)	GNRL_EV_VIRUS_OUTBREAK	Ce type d'événements se produit lorsque le nombre d'objets malveillants détectés sur plusieurs appareils administrés dépasse le seuil sur une courte durée. Vous pouvez répondre à l'événement des manières suivantes : • Vous pouvez configurer le seuil dans les propriétés du Serveur d'administration. • Vous pouvez aussi créer une stratégie plus stricte qui sera activée ou créer une tâche qui sera exécutée quand l'événement se produit.	180 jours

Nom affiché du type d'événement	ID de type d'événement	Type d'événement	Description	Durée de stockage par défaut
L'appareil n'est plus administré	4111	KLSRV_HOST_OUT_CONTROL	Des événements de ce type se produisent si un appareil administré est visible sur le réseau mais n'est pas connecté au Serveur d'administration pendant une certaine durée. Trouvez ce qui empêche le fonctionnement normal de l'Agent d'administration sur l'appareil. Les causes possibles sont des problèmes de réseau et la suppression de l'agent d'administration de l'appareil.	180 jours
L'appareil est en état Critique	4113	KLSRV_HOST_STATUS_CRITICAL	Ce type d'événements se produit lorsqu'un appareil administré a reçu l'état *Critique*. Vous pouvez configurer les conditions dans lesquelles l'état de l'appareil devient *Critique*.	180 jours
Le fichier clé a été ajouté à la liste de refus	4124	KLSRV_LICENSE_BLACKLISTED	Des événements de ce type se produisent lorsque Kaspersky a ajouté le code d'activation ou le fichier clé que vous utilisez à la liste de refus. Pour en savoir plus, contactez le Support technique.	180 jours
Mode limité	4130	KLSRV_EV_LICENSE_SRV_LIMITED_MODE	Ce type d'événements se produit lorsque Kaspersky Security Center commence à fonctionner avec les fonctionnalités de base, sans les fonctionnalités de Gestion des vulnérabilités et des correctifs et d'administration des appareils mobiles. Les causes de l'événement et les réponses appropriées sont indiquées ci-après : • La durée de validité de la licence a expiré. Fournissez une licence pour utiliser le mode de fonctionnalité complète de Kaspersky Security Center (ajoutez un code d'activation valide ou un fichier clé au Serveur d'administration). • Le serveur d'administration gère plus d'appareils que spécifié par la limite de licence. Déplacez les appareils des groupes d'administration d'un serveur d'administration vers les groupes d'un autre serveur d'administration (si permis pas la limite de licence de l'autre serveur d'administration).	180 jours

Nom affiché du type d'événement	ID de type d'événement	Type d'événement	Description	Durée de stockage par défaut
La licence expire bientôt	4129	KLSRV_EV_LICENSE_SRV_EXPIRE_SOON	Des événements de ce type se produisent lorsque la date de fin de la durée de validité de la licence commerciale approche. Une fois par jour, Kaspersky Security Center vérifie si la date de fin de la durée de validité de la licence approche. Les événements de ce type sont publiés 30 jours, 15 jours, 5 jours et 1 jour avant la date de fin de la durée de validité de la licence. Vous ne pouvez pas modifier le nombre de jours. Si le Serveur d'administration est désactivé le jour défini avant la date de fin de la durée de validité de la licence, l'événement ne sera pas publié avant le jour suivant. À l'expiration de la licence commerciale, Kaspersky Security Center ne fournit que les fonctionnalités de base. Vous pouvez répondre à l'événement des manières suivantes : • Assurez-vous qu'une clé de licence de réserve est ajoutée au Serveur d'administration. • Si vous utilisez un abonnement, assurez-vous de le renouveler. Un abonnement illimité est renouvelé automatiquement s'il a été prépayé auprès du prestataire de services à la date d'échéance.	180 jours
Le certificat a expiré	4132	KLSRV_CERTIFICATE_EXPIRED	Des événements de ce type se produisent lorsque le certificat client sur les appareils mobiles expire.	180 jours
Le certificat du Serveur d'administration a expiré.	6129	Certificat de serveur expiré	Des événements de ce type se produisent lorsque les certificats du Serveur d'administration pour les appareils mobiles et les appareils UEFI expirent. Vous devez mettre à jour le certificat expiré.	180 jours
Les mises à jour des modules des applications Kaspersky ont été rappelées	4142	KLSRV_SEAMLESS_UPDATE_REVOKED	Ce type d'événements se produit si des mises à jour continues ont été révoquées (l'état *Révoqué* est affiché pour ces mises à jour) par des spécialistes techniques de Kaspersky ; par exemple, ils doivent être mis à jour vers une version plus récente. L'événement concerne les correctifs de Kaspersky Security Center et non les modules d'applications administrés par Kaspersky. L'événement indique que les mises à jour continues ne sont pas installées.	180 jours
Audit : l'exportation vers le SIEM a échoué	5130	KLAUD_EV_SIEM_EXPORT_ERROR	Les événements de ce type se produisent lorsque l'exportation d'événements vers le système SIEM a échoué en raison d'une erreur de connexion avec le système SIEM.	180 jours

Événements liés à des erreurs de fonctionnement du Serveur d'administration

Le tableau ci-dessous indique les types d'événements du Serveur d'administration de Kaspersky Security Center au niveau de gravité **Erreur de fonctionnement**.

Pour chaque événement pouvant être généré par une application, vous pouvez spécifier les paramètres de notification et les paramètres de stockage sous l'onglet **Configuration des événements** dans la stratégie de l'application. Pour le Serveur d'administration, vous pouvez également consulter et configurer la liste des événements dans les propriétés du Serveur d'administration. Si vous souhaitez configurer les paramètres de notification pour tous les événements à la fois, configurez les paramètres de notification généraux dans les propriétés du Serveur d'administration.

Événements liés à des erreurs de fonctionnement du Serveur d'administration

Nom affiché du type d'événement	ID de type d'événement	Type d'événement	Description	Durée de stockage par défaut
Erreur du temps d'exécution	4125	KLSRV_RUNTIME_ERROR	Ce type d'événements se produit à cause de problèmes inconnus. Ce sont le plus souvent des problèmes de SGBD, de réseau et d'autres problèmes logiciels et matériels. Les détails de l'événement peuvent se trouver dans la description de l'événement.	180 jours
Pour un des groupes des applications sous licence, la limite des installations a été dépassée	4126	KLSRV_INVLICPROD_EXCEDED	Le serveur d'administration génère ce type d'événements périodiquement (toutes les heures). Ce type d'événements se produit si dans Kaspersky Security Center, vous administrez les clés d'applications tierces et si le nombre d'installations a dépassé la limite définie par la clé de licence de l'application tierce. Vous pouvez répondre à l'événement des manières suivantes : • Parcourez la liste des appareils administrés. Supprimez l'application tierce des appareils où l'application n'est pas utilisée. • Utiliser une licence tierce pour plusieurs appareils. Vous pouvez gérer les clés de licence d'applications tierces à l'aide des fonctionnalités des groupes des applications sous licence. Un groupe des applications sous licence inclut les applications tierces qui répondent aux critères que vous avez définis.	180 jours
Échec du sondage du segment dans le cloud	4143	KLSRV_KLCLOUD_SCAN_ERROR	Des événements de ce type se produisent lorsque le Serveur d'administration ne parvient pas à interroger un segment de réseau dans un environnement cloud. Lisez les détails dans la description de l'événement et répondez en conséquence.	Non stocké
Échec de la copie des mises à jour vers le dossier indiqué	4123	KLSRV_UPD_REPL_FAIL	Ce type d'événements se produit lorsque les mises à jour logicielles sont copiées dans un ou plusieurs dossier(s) partagés. Vous pouvez répondre à l'événement des manières suivantes : • Vérifiez si le compte d'utilisateur utilisé pour accéder au(x) dossier(s) est autorisé en écriture. • Vérifiez si un nom d'utilisateur et / ou un mot de passe du ou des dossiers a changé. • Vérifiez la connexion Internet, car elle peut être à l'origine de l'événement. Suivez les instructions pour mettre à jour les bases de données et es modules logiciels.	180 jours
Plus d'espace disponible sur le disque	4107	KLSRV_DISK_FULL	Des événements de ce type se produisent lorsque le disque dur de l'appareil sur lequel le Serveur d'administration est installé ne dispose plus d'espace libre. Libérez de l'espace disque sur l'appareil.	180 jours

Nom affiché du type d'événement	ID de type d'événement	Type d'événement	Description	Durée de stockage par défaut
Le dossier en accès public n'est pas disponible	4108	KLSRV_SHARED_FOLDER_UNAVAILABLE	Ce type d'événements se produit si le dossier partagé du Serveur d'administration n'est pas disponible. Vous pouvez répondre à l'événement des manières suivantes : • Vérifiez si le Serveur d'administration (où se trouve le dossier partagé) est sous tension et disponible. • Vérifiez si un nom d'utilisateur et / ou un mot de passe du dossier a changé. • Vérifiez la connexion réseau.	180 jours

Nom affiché du type d'événement	ID de type d'événement	Type d'événement	Description	Durée de stockage par défaut
La base de données du Serveur d'administration n'est pas disponible	4109	KLSRV_DATABASE_UNAVAILABLE	Ce type d'événements se produit si le Serveur d'administration n'est pas disponible. Vous pouvez répondre à l'événement des manières suivantes : • Vérifiez si le serveur distant sur lequel est installé SQL Server est disponible. • Affichez les journaux du SGBD pour trouver la raison de l'indisponibilité de la base de données du Serveur d'administration. Par exemple, un serveur distant sur lequel est installé SQL Server peut ne pas être disponible à cause de la maintenance préventive.	180 jours
Espace insuffisant dans la base de données du Serveur d'administration	4110	KLSRV_DATABASE_FULL	Ce type d'événements se produit lorsque la base de données du Serveur d'administration n'a plus d'espace libre. Le Serveur d'administration ne fonctionne pas lorsque sa base de données a atteint sa capacité maximale et que la base de données ne peut plus recevoir d'enregistrement. Les causes de cet événement, en fonction du SGBD utilisé, et les réponses appropriées à l'événement sont indiquées ci-après : • Vous utilisez le SGBD de SQL Server édition Express : Dans la documentation SQL Server Express, contrôlez la taille limite de la base de données pour la version que vous utilisez. La base de données de votre Serveur d'administration a probablement dépassé la taille limite. Limiter le nombre d'événements à stocker dans la base de données du Serveur d'administration. La base de données du Serveur d'administration contient trop d'événements envoyés par le module Contrôle des applications. Vous pouvez modifier les paramètres de la stratégie Kaspersky Endpoint Security for Windows concernant le stockage des événements du Contrôle des applications dans la base de données du Serveur d'administration. • Vous utilisez un SGBD autre que SQL Server Express Edition : Ne pas limiter le nombre d'événements à stocker dans la base de données du Serveur d'administration. Réduire la liste d'événements à stocker dans la base de données du Serveur d'administration. Consulter les informations sur la sélection du SGBD.	180 jours

Événements d'avertissement du Serveur d'administration

Le tableau ci-dessous montre les événements du Serveur d'administration de Kaspersky Security Center au niveau de gravité **Avertissement**.

Pour chaque événement pouvant être généré par une application, vous pouvez spécifier les paramètres de notification et les paramètres de stockage sous l'onglet **Configuration des événements** dans la stratégie de l'application. Pour le Serveur d'administration, vous pouvez également consulter et configurer la liste des événements dans les propriétés du Serveur d'administration. Si vous souhaitez configurer les paramètres de notification pour tous les événements à la fois, configurez les paramètres de notification généraux dans les propriétés du Serveur d'administration.

Événements d'avertissement du Serveur d'administration

Nom affiché du type d'événement	ID de type d'événement	Type d'événement	Description	Durée de stockage par défaut
Un événement fréquent a été détecté		KLSRV_EVENT_SPAM_EVENTS_DETECTED	Des événements de ce type se produisent lorsque le Serveur d'administration détecte un événement fréquent sur l'appareil administré. Pour en savoir plus sur la section suivante : Blocage des événements fréquents.	90 jours
La restriction de la licence a été dépassée	4098	KLSRV_EV_LICENSE_CHECK_100_110	Une fois par jour, Kaspersky Security Center vérifie si une limite de licence est dépassée. Ce type d'événements se produit si le serveur d'administration détecte que certaines limites de licence sont dépassées par les applications Kaspersky installées sur les appareils clients et si le nombre d'unités de licence actuellement utilisé sous licence unique représente 100 % à 110 % du nombre total d'unités sous licence. Même lorsque cet événement se produit, les appareils clients sont protégés. Vous pouvez répondre à l'événement des manières suivantes : • Parcourez la liste des appareils administrés. Supprimez les appareils inutilisés. • Fournissez une licence pour plusieurs appareils (ajoutez un code d'activation valide ou un fichier clé au serveur d'administration). Kaspersky Security Center définit les règles de génération d'événements lorsqu'une limite de la licence est dépassée.	90 jours
L'appareil est resté inactif sur le réseau depuis longtemps	4103	KLSRV_EVENT_HOSTS_NOT_VISIBLE	Des événements de ce type se produisent lorsqu'un appareil administré est inactif pendant un certain temps. Le plus souvent, cela se produit lorsqu'un appareil administré est mis hors service. Vous pouvez répondre à l'événement des manières suivantes : • Supprimez manuellement l'appareil de la liste des appareils administrés. • Spécifiez l'intervalle de temps après lequel l'événement **L'appareil est resté inactif sur le réseau depuis longtemps** est créé à l'aide de la Console d'administration ou de Kaspersky Security Center Web Console. • Spécifiez l'intervalle de temps après lequel l'appareil est automatiquement supprimé du groupe à l'aide de la Console d'administration ou de Kaspersky Security Center Web Console.	90 jours

Nom affiché du type d'événement	ID de type d'événement	Type d'événement	Description	Durée de stockage par défaut
Noms d'appareil en conflit	4102	KLSRV_EVENT_HOSTS_CONFLICT	Des événements de ce type se produisent lorsque le Serveur d'administration considère deux ou plusieurs appareils administrés comme un seul appareil. La plupart du temps, cela se produit lorsqu'un disque dur cloné a été utilisé pour déployer des logiciels sur des appareils administrés et sans que l'Agent d'administration ne passe en mode de clonage de disque dédié sur un appareil de référence. Pour éviter ce problème, passez l'Agent d'administration en mode de clonage de disque sur un appareil de référence avant de cloner le disque dur de cet appareil.	90 jours
L'appareil est en état Avertissement	4114	KLSRV_HOST_STATUS_WARNING	Ce type d'événements se produit lorsqu'un appareil administré a reçu l'état *Avertissement*. Vous pouvez configurer les conditions dans lesquelles l'état de l'appareil devient *Avertissement*.	90 jours
La limite des installations sera bientôt dépassée pour l'un des groupes d'applications sous licence	4127	KLSRV_INVLICPROD_FILLED	Des événements de ce type se produisent lorsque le nombre d'installations pour des applications tierces incluses dans un groupe des applications sous licence atteint 90 % de la valeur maximale autorisée indiquée dans les propriétés de la clé de licence. Vous pouvez répondre à l'événement des manières suivantes : • Si l'application tierce n'est pas utilisée sur certains des appareils administrés, supprimez l'application de ces appareils. • Si vous prévoyez que le nombre d'installations pour l'application tierce dépassera le nombre maximum autorisé prochainement, envisagez d'obtenir à l'avance une licence tierce pour un plus grand nombre d'appareils. Vous pouvez gérer les clés de licence d'applications tierces à l'aide des fonctionnalités des groupes des applications sous licence.	90 jours
Le certificat a été demandé	4133	KLSRV_CERTIFICATE_REQUESTED	Des événements de ce type se produisent lorsqu'un certificat pour l'administration des appareils mobiles ne parvient pas à être réémis automatiquement. Les causes et les réponses appropriées à cet événement peuvent être les suivantes : • La réémission automatique a été lancée pour un certificat pour lequel l'option **Réémettre automatiquement le certificat si possible** est désactivée. Cela peut être dû à une erreur qui s'est produite lors de la création du certificat. Il peut être nécessaire d'émettre à nouveau le certificat manuellement. • Si vous utilisez une intégration avec une infrastructure à clé publique, la cause peut être l'absence d'un attribut SAM-Account-Name du compte utilisé pour l'intégration avec PKI et pour l'émission du certificat. Vérifiez les propriétés du compte.	90 jours

Nom affiché du type d'événement	ID de type d'événement	Type d'événement	Description	Durée de stockage par défaut
Le certificat a été supprimé	4134	KLSRV_CERTIFICATE_REMOVED	Des événements de ce type se produisent lorsqu'un administrateur supprime tout type de certificat (général, email, VPN) pour l'Administration des appareils mobiles. Une fois qu'un certificat aura été supprimé, les appareils mobiles connectés via ce certificat ne parviendront pas à se connecter au Serveur d'administration. Cet événement pourrait être utile lors d'une enquête sur les dysfonctionnements liés à l'administration des appareils mobiles.	90 jours
Le certificat expire	6128	Le certificat du serveur expire bientôt	Des événements de ce type se produisent lorsque les certificats du Serveur d'administration pour les appareils mobiles et les appareils UEFI expirent. Vous devez mettre à jour le certificat expiré.	90 jours
La durée de validité du certificat APNs a expiré	4135	KLSRV_APN_CERTIFICATE_EXPIRED	Des événements de ce type se produisent lorsqu'un certificat APNs expire. Vous devez renouveler manuellement le certificat APNs et l'installer sur un serveur MDM iOS.	Non stocké
La durée de validité du certificat APNs expire bientôt	4136	KLSRV_APN_CERTIFICATE_EXPIRES_SOON	Les événements de ce type se produisent lorsqu'il reste moins de 14 jours avant l'expiration du certificat APNs. Lorsque le certificat APNs expire, vous devez renouveler manuellement le certificat APNs et l'installer sur un serveur MDM iOS. Nous vous recommandons de planifier le renouvellement du certificat APNs avant la date d'expiration.	Non stocké
Échec de l'envoi d'un message FCM sur l'appareil mobile	4138	KLSRV_GCM_DEVICE_ERROR	Des événements de ce type se produisent lorsque l'Administration des appareils mobiles est configurée de façon à utiliser Firebase Cloud Messaging (FCM) pour se connecter aux appareils mobiles administrés avec un système d'exploitation Android et que le serveur FCM ne parvient pas à traiter certaines des requêtes reçues de la part du Serveur d'administration. Cela signifie que certains des appareils mobiles administrés ne recevront aucune notification push. Lisez le code HTTP dans les détails de la description de l'événement et répondez en conséquence. Pour en savoir plus sur les codes HTTP reçus de la part du serveur FCM et sur les erreurs qui y sont liées, veuillez consulter la documentation du service Firebase (voir le chapitre « Codes de réponse d'erreur aux messages en aval »).	90 jours

Nom affiché du type d'événement	ID de type d'événement	Type d'événement	Description	Durée de stockage par défaut
Erreur HTTP lors de l'envoi d'un message FCM sur le serveur FCM	4139	KLSRV_GCM_HTTP_ERROR	Des événements de ce type se produisent lorsque l'Administration des appareils mobiles est configurée de façon à utiliser Firebase Cloud Messaging (FCM) pour connecter les appareils mobiles administrés avec le système d'exploitation Android et que le serveur FCM revient à la requête du Serveur d'administration avec un code HTTP différent de 200 (OK). Les causes et les réponses appropriées à cet événement peuvent être les suivantes : • Problèmes du côté du serveur FCM. Lisez le code HTTP dans les détails de la description de l'événement et répondez en conséquence. Pour en savoir plus sur les codes HTTP reçus de la part du serveur FCM et sur les erreurs qui y sont liées, veuillez consulter la documentation du service Firebase (voir le chapitre « Codes de réponse d'erreur aux messages en aval »). • Problèmes du côté du serveur proxy (si vous utilisez un serveur proxy). Lisez le code HTTP dans les détails de la description de l'événement et répondez en conséquence.	90 jours
Échec de l'envoi d'un message FCM sur le serveur FCM	4140	KLSRV_GCM_GENERAL_ERROR	Des événements de ce type se produisent en raison d'erreurs inattendues du côté du Serveur d'administration lors de l'utilisation du protocole HTTP de Firebase Cloud Messaging. Lisez les détails dans la description de l'événement et répondez en conséquence. Si vous ne pouvez pas trouver la solution à un problème par vous-même, nous vous recommandons de contacter le Support Technique de Kaspersky.	90 jours
Espace libre insuffisant sur le disque dur	4105	KLSRV_NO_SPACE_ON_VOLUMES	Des événements de ce type se produisent lorsque le disque dur de l'appareil sur lequel le Serveur d'administration est installé ne dispose presque plus d'espace libre. Libérez de l'espace disque sur l'appareil.	90 jours

Nom affiché du type d'événement	ID de type d'événement	Type d'événement	Description	Durée de stockage par défaut
Trop peu d'espace disponible dans la base de données du Serveur d'administration	4106	KLSRV_NO_SPACE_IN_DATABASE	Ce type d'événements se produit si l'espace de la base de données du Serveur d'administration est trop limité. Si vous ne corrigez pas la situation, quand la base de données du Serveur d'administration atteindra sa pleine capacité, le Serveur d'administration ne fonctionnera plus. Les causes de cet événement, en fonction du SGBD utilisé, et les réponses appropriées à l'événement sont indiquées ci-après. Vous utilisez le SGBD de SQL Server édition Express : • Dans la documentation SQL Server Express, contrôlez la taille limite de la base de données pour la version que vous utilisez. La base de données de votre Serveur d'administration est probablement tout près d'atteindre la taille limite. • Limiter le nombre d'événements à stocker dans la base de données du Serveur d'administration. • La base de données du Serveur d'administration contient trop d'événements envoyés par le module Contrôle des applications. Vous pouvez modifier les paramètres de la stratégie Kaspersky Endpoint Security for Windows concernant le stockage des événements du Contrôle des applications dans la base de données du Serveur d'administration. Vous utilisez un SGBD autre que SQL Server Express Edition : • Ne pas limiter le nombre d'événements à stocker dans la base de données du Serveur d'administration • Réduire la liste d'événements à stocker dans la base de données du Serveur d'administration Consulter les informations sur la sélection du SGBD.	90 jours
La connexion au Serveur d'administration secondaire a été perdue	4116	KLSRV_EV_SLAVE_SRV_DISCONNECTED	Des événements de ce type se produisent lorsqu'une connexion au Serveur d'administration secondaire est interrompue. Lisez le journal des événements Kaspersky sur l'appareil où le Serveur d'administration secondaire est installé et répondez en conséquence.	90 jours
La connexion au Serveur d'administration principal a été interrompue	4118	KLSRV_EV_MASTER_SRV_DISCONNECTED	Des événements de ce type se produisent lorsqu'une connexion au Serveur d'administration principal est interrompue. Lisez le journal des événements Kaspersky sur l'appareil où le Serveur d'administration principal est installé et répondez en conséquence.	90 jours

Nom affiché du type d'événement	ID de type d'événement	Type d'événement	Description	Durée de stockage par défaut
Les nouvelles mises à jour des modules des applications Kaspersky ont été enregistrées	4141	KLSRV_SEAMLESS_UPDATE_REGISTERED	Des événements de ce type se produisent lorsque le Serveur d'administration enregistre de nouvelles mises à jour pour le logiciel Kaspersky installé sur des appareils administrés dont l'installation nécessite une autorisation. Approuvez ou refusez les mises à jour à l'aide de la Console d'administration ou de Kaspersky Security Center Web Console.	90 jours
La limite du nombre d'événements dans la base de données est dépassée, la suppression des événements a commencé	4145	KLSRV_EVP_DB_TRUNCATING	Ce type d'événements se produit lorsque la suppression des anciens événements de la base de données du Serveur d'administration commence une fois que la base de données du Serveur d'administration a atteint sa capacité. Vous pouvez répondre à l'événement des manières suivantes : • Modifiez le nombre maximal d'événements stockés dans la base de données du Serveur d'administration • Réduire la liste d'événements à stocker dans la base de données du Serveur d'administration	Non stocké
La limite du nombre d'événements dans la base de données est dépassée, les événements ont été supprimés	4146	KLSRV_EVP_DB_TRUNCATED	Ce type d'événements se produit lorsque d'anciens événements ont été supprimés de la base de données du Serveur d'administration une fois que la base de données du Serveur d'administration a atteint sa capacité. Vous pouvez répondre à l'événement des manières suivantes : • Modifiez le nombre maximal autorisé d'événements stockés dans la base de données du Serveur d'administration • Réduire la liste d'événements à stocker dans la base de données du Serveur d'administration	Non stocké
Audit (échec du test de connexion au serveur SIEM)	5120	KLAUD_EV_SIEM_TEST_FAILED	Les événements de ce type se produisent lorsqu'un test de connexion au serveur SIEM a échoué.	30 jours
Échec de l'émission automatique du certificat		KLSRV_CERTIFICATE_AUTO_ISSUE_ERROR	Cet événement se produit en cas d'erreur lors de la création d'un certificat client pour un appareil mobile (un appareil fonctionnant sous un protocole mobile).	90 jours

Événements d'information du Serveur d'administration

Le tableau ci-dessous montre les événements du Serveur d'administration de Kaspersky Security Center au niveau de gravité **Information**.

Pour chaque événement pouvant être généré par une application, vous pouvez spécifier les paramètres de notification et les paramètres de stockage sous l'onglet **Configuration des événements** dans la stratégie de l'application. Pour le Serveur d'administration, vous pouvez également consulter et configurer la liste des événements dans les propriétés du Serveur d'administration. Si vous souhaitez configurer les paramètres de notification pour tous les événements à la fois, configurez les paramètres de notification généraux dans les propriétés du Serveur d'administration.

Nom affiché du type d'événement	ID de type d'événement	Type d'événement	Durée de stockage par défaut	Remarques
Clé de licence utilisée à plus de 90 %	4097	KLSRV_EV_LICENSE_CHECK_90	30 jours	
Un nouvel appareil a été détecté	4100	KLSRV_EVENT_HOSTS_NEW_DETECTED	30 jours	
L'appareil a été ajouté automatiquement au groupe	4101	KLSRV_EVENT_HOSTS_NEW_REDIRECTED	30 jours	
L'appareil a été déplacé automatiquement selon la règle	1074	KLSRV_HOST_MOVED_WITH_RULE_EX	30 jours	
L'appareil a été supprimé du groupe : longue absence d'activité sur le réseau	4104	KLSRV_INVISIBLE_HOSTS_REMOVED	30 jours	
Pour un des groupes des applications sous licence, le nombre d'installations autorisées est épuisé à plus de 95 %	4128	KLSRV_INVLICPROD_EXPIRED_SOON	30 jours	
Des fichiers à envoyer à Kaspersky pour analyse ont été détectés	4131	KLSRV_APS_FILE_APPEARED	30 jours	
L'ID d'instance FCM de l'appareil mobile a modifié	4137	KLSRV_GCM_DEVICE_REGID_CHANGED	30 jours	
Les mises à jour ont bien été copiées dans le dossier indiqué	4122	KLSRV_UPD_REPL_OK	30 jours	
La connexion au Serveur d'administration secondaire a été établie	4115	KLSRV_EV_SLAVE_SRV_CONNECTED	30 jours	
La connexion au Serveur d'administration principal a été établie	4117	KLSRV_EV_MASTER_SRV_CONNECTED	30 jours	
Les bases de données ont été mises à jour	4144	KLSRV_UPD_BASES_UPDATED	30 jours	
Audit : une connexion au Serveur d'administration a été établie	4147	KLAUD_EV_SERVERCONNECT	30 jours	Les événements de ce type se produisent lorsqu'un utilisateur se connecte au Serveur d'administration à l'aide de la Console d'administration ou de Kaspersky Security Center Web Console. Ces événements incluent l'adresse IP de l'appareil sur lequel la Console d'administration basée sur MMC ou le serveur Kaspersky Security Center Web Console est installé.

Nom affiché du type d'événement	ID de type d'événement	Type d'événement	Durée de stockage par défaut	Remarques
Audit : un objet a été modifié	4148	KLAUD_EV_OBJECTMODIFY	30 jours	Cet événement permet de suivre les modifications apportées aux objets suivants : • Groupe d'administration • Groupe de sécurité • Utilisateur • Paquet • Tâche • Stratégie • Serveur • Serveur virtuel
Audit : l'état de l'objet a été modifié	4150	KLAUD_EV_TASK_STATE_CHANGED	30 jours	Par exemple, cet événement se produit lorsqu'une tâche a échoué avec une erreur.
Audit : les paramètres de groupe ont été modifiés	4149	KLAUD_EV_ADMGROUP_CHANGED	30 jours	
Audit : la connexion au Serveur d'administration a été interrompue	4151	KLAUD_EV_SERVERDISCONNECT	30 jours	
Audit : les propriétés de l'objet ont été modifiées	4152	KLAUD_EV_OBJECTPROPMODIFIED	30 jours	Cet événement suit les modifications apportées aux propriétés suivantes : • Utilisateur • Licence • Serveur • Serveur virtuel
Audit : les autorisations de l'utilisateur ont été modifiées	4153	KLAUD_EV_OBJECTACLMODIFIED	30 jours	
Audit : les clés de chiffrement ont été importées ou exportées à partir du Serveur d'administration	5100	KLAUD_EV_DPEKEYSEXPORT	30 jours	
Audit : le test de connexion au serveur SIEM a réussi	5110	KLAUD_EV_SIEM_TEST_SUCCESS	30 jours	Les événements de ce type se produisent lorsqu'un test de connexion au serveur SIEM a réussi.
Certificat de réserve créé		Certificat de réserve de serveur créé	30 jours	Cet événement se produit lorsqu'un certificat de Serveur d'administration a été créé.
Renouvellement du certificat		Certificat de serveur renouvelé	30 jours	Cet événement se produit lorsque le certificat du Serveur d'administration a été renouvelé.

Les événements **Certificat de réserve créé** et **Renouvellement du certificat** sont publiés automatiquement par le Serveur d'administration et affichés dans la Console d'administration uniquement lorsque les opérations

correspondant à ces événements sont exécutées pour les certificats de Serveur d'administration pour les appareils mobiles et les appareils UEFI.

Événements de l'Agent d'administration

Cette section contient des informations sur les événements liés à l'agent d'administration.

Événements liés aux erreurs de fonctionnement de l'Agent d'administration

Le tableau ci-dessous indique les types d'événements de l'Agent d'administration de Kaspersky Security Center, regroupés par niveau de sécurité **Erreur de fonctionnement**.

Pour chaque événement pouvant être généré par une application, vous pouvez spécifier les paramètres de notification et les paramètres de stockage sous l'onglet **Configuration des événements** dans la stratégie de l'application. Si vous souhaitez configurer les paramètres de notification pour tous les événements à la fois, configurez les paramètres de notification généraux dans les propriétés du Serveur d'administration.

Événements liés aux erreurs de fonctionnement de l'Agent d'administration

Nom affiché du type d'événement	ID de type d'événement	Type d'événement	Description	Durée de stockage par défaut
Erreur d'installation de la mise à jour	7702	KLNAG_EV_PATCH_INSTALL_ERROR	Des événements de ce type se produisent si l'Installation automatique des mises à jour et des correctifs pour les modules de Kaspersky Security Center ne réussit pas. L'événement ne concerne pas les mises à jour des applications Kaspersky administrées. Lisez la description de l'événement. Cet événement peut être dû à un problème Windows sur le serveur d'administration. Si la description mentionne un problème de configuration Windows, résolvez le problème.	30 jours
Échec de l'installation de la mise à jour du logiciel tiers	7697	KLNAG_EV_3P_PATCH_INSTALL_ERROR	Des événements de ce type se produisent si les fonctionnalités de la gestion des vulnérabilités et des correctifs et d'Administration des appareils mobiles sont en cours d'utilisation, et si la mise à jour des logiciels tiers n'a pas réussi. Vérifiez si le lien vers le logiciel tiers est valide. Lisez la description de l'événement.	30 jours
Échec de l'installation des mises à jour Windows Update	7717	KLNAG_EV_WUA_INSTALL_ERROR	Ce type d'événements se produit si les mises à jour Windows échouent. Configurez les mises à jour Windows dans une stratégie d'Agent d'administration. Lisez la description de l'événement. Recherchez l'erreur dans la base de connaissance Microsoft. Contactez le Support Technique de Microsoft si vous ne parvenez pas à résoudre le problème vous-même.	30 jours
Gestion des utilisateurs : erreurs	7723	KLNAG_EV_USR_MNG_ERR	Événement d'avertissement général.	30 jours
Impossible de restaurer le fichier sudoers à la valeur de référence	7726	KLNAG_EV_SUDOER_RESTORED_ERR	L'événement contient la description de l'erreur de remplacement du fichier sudoers.	30 jours

Nom affiché du type d'événement	ID de type d'événement	Type d'événement	Description	Durée de stockage par défaut
Il est impossible d'installer les certificats racine	7728	KLNAG_EV_ROOT_CERT_INSTALL_ERR	L'événement contient la description de l'erreur d'installation des certificats.	30 jours
Impossible de supprimer les certificats racine	7730	KLNAG_EV_ROOT_CERT_REMOVE_ERR	L'événement contient la description de l'erreur de suppression des certificats.	30 jours

Événements d'avertissement de l'Agent d'administration

Le tableau suivant reprend les événements de l'Agent d'administration de Kaspersky Security Center, regroupés par niveau de gravité **Avertissement**.

Pour chaque événement pouvant être généré par une application, vous pouvez spécifier les paramètres de notification et les paramètres de stockage sous l'onglet **Configuration des événements** dans la stratégie de l'application. Si vous souhaitez configurer les paramètres de notification pour tous les événements à la fois, configurez les paramètres de notification généraux dans les propriétés du Serveur d'administration.

Événements d'avertissement de l'Agent d'administration

Nom affiché du type d'événement	ID de type d'événement	Type d'événement	Durée de stockage par défaut
Avertissement renvoyé lors de l'installation des mises à jour des modules de l'application	7701	KLNAG_EV_PATCH_INSTALL_WARNING	30 jours
L'installation de la mise à jour du logiciel tiers s'est terminée avec un avertissement	7696	KLNAG_EV_3P_PATCH_INSTALL_WARNING	30 jours
L'installation de la mise à jour du logiciel tiers a été reportée	7698	KLNAG_EV_3P_PATCH_INSTALL_SLIPPED	30 jours
Un problème de sécurité est survenu	549	GNRL_EV_APP_INCIDENT_OCCURED	30 jours
Le proxy KSN a démarré. Échec de la vérification de la disponibilité de KSN	7718	KSNPROXY_STARTED_CON_CHK_FAILED	30 jours
Gestion des utilisateurs : avertissements	7722	KLNAG_EV_USR_MNG_WRN	30 jours
Le fichier Sudoers ne correspond pas à la valeur de référence	7724	KLNAG_EV_SUDOER_DIFFERENT	30 jours

Événements informatifs de l'Agent d'administration

Le tableau suivant reprend les événements de l'Agent d'administration de Kaspersky Security Center, regroupés par niveau de gravité **Information**.

Pour chaque événement pouvant être généré par une application, vous pouvez spécifier les paramètres de notification et les paramètres de stockage sous l'onglet **Configuration des événements** dans la stratégie de l'application. Si vous souhaitez configurer les paramètres de notification pour tous les événements à la fois, configurez les paramètres de notification généraux dans les propriétés du Serveur d'administration.

Événements informatifs de l'Agent d'administration

Nom affiché du type d'événement	ID de type d'événement	Type d'événement	Durée de stockage par défaut
La mise à jour des modules de l'application a bien été appliquée	7699	KLNAG_EV_PATCH_INSTALLED_SUCCESSFULLY	30 jours
L'installation de la mise à jour du module logiciel est lancée	7700	KLNAG_EV_PATCH_INSTALL_STARTING	30 jours
L'application a été installée	7703	KLNAG_EV_INV_APP_INSTALLED	30 jours
L'application a été désinstallée	7704	KLNAG_EV_INV_APP_UNINSTALLED	30 jours
L'application contrôlée a été installée	7705	KLNAG_EV_INV_OBS_APP_INSTALLED	30 jours

Nom affiché du type d'événement	ID de type d'événement	Type d'événement	Durée de stockage par défaut
L'application contrôlée a été désinstallée	7706	KLNAG_EV_INV_OBS_APP_UNINSTALLED	30 jours
L'application tierce a été installée	7707	KLNAG_EV_INV_CMPTR_APP_INSTALLED	30 jours
Un nouvel appareil a été ajouté	7708	KLNAG_EV_DEVICE_ARRIVAL	30 jours
L'appareil a été supprimé	7709	KLNAG_EV_DEVICE_REMOVE	30 jours
Un nouvel appareil a été détecté	7710	KLNAG_EV_NAC_DEVICE_DISCOVERED	30 jours
L'appareil a été autorisé	7711	KLNAG_EV_NAC_HOST_AUTHORIZED	30 jours
Partage du bureau Windows : le fichier est lu	7712	KLUSRLOG_EV_FILE_READ	30 jours
Partage du bureau Windows : le fichier a été modifié	7713	KLUSRLOG_EV_FILE_MODIFIED	30 jours
Partage du bureau Windows : l'application a démarré	7714	KLUSRLOG_EV_PROCESS_LAUNCHED	30 jours
Partage du bureau Windows : lancé	7715	KLUSRLOG_EV_WDS_BEGIN	30 jours
Partage du bureau Windows : arrêté	7716	KLUSRLOG_EV_WDS_END	30 jours
L'installation de la mise à jour d'un logiciel tiers a réussi	7694	KLNAG_EV_3P_PATCH_INSTALLED_SUCCESSFULLY	30 jours
L'installation de la mise à jour du logiciel tiers est lancée	7695	KLNAG_EV_3P_PATCH_INSTALL_STARTING	30 jours
Le proxy KSN a démarré. La vérification de la disponibilité de KSN a réussi	7719	KSNPROXY_STARTED_CON_CHK_OK	30 jours
Le serveur proxy KSN a été arrêté	7720	KSNPROXY_STOPPED	30 jours

Événements du Serveur MDM iOS

Cette section contient des informations sur les événements liés au serveur MDM iOS.

Événements liés aux erreurs de fonctionnement du Serveur MDM iOS

Le tableau suivant reprend les événements du Serveur MDM iOS de Kaspersky Security Center, regroupés par niveau de gravité **Erreur de fonctionnement**.

Pour chaque événement pouvant être généré par une application, vous pouvez spécifier les paramètres de notification et les paramètres de stockage sous l'onglet **Configuration des événements** dans la stratégie de l'application. Si vous souhaitez configurer les paramètres de notification pour tous les événements à la fois, configurez les paramètres de notification généraux dans les propriétés du Serveur d'administration.

Événements liés aux erreurs de fonctionnement du Serveur MDM iOS

Nom affiché du type d'événement	Type d'événement	Durée de stockage par défaut
Il est impossible de demander la liste des profils	PROFILELIST_COMMAND_FAILED	30 jours
Il est impossible d'installer le profil	INSTALLPROFILE_COMMAND_FAILED	30 jours
Il est impossible de supprimer le profil	REMOVEPROFILE_COMMAND_FAILED	30 jours
Il est impossible de demander la liste des profils provisioning	PROVISIONINGPROFILELIST_COMMAND_FAILED	30 jours
Il est impossible d'installer le profil provisioning	INSTALLPROVISIONINGPROFILE_COMMAND_FAILED	30 jours
Il est impossible de supprimer le profil provisioning	REMOVEPROVISIONINGPROFILE_COMMAND_FAILED	30 jours
Il est impossible de demander la liste des certificats	CERTIFICATELIST_COMMAND_FAILED	30 jours

Nom affiché du type d'événement	Type d'événement	Durée de stockage par défaut
Il est impossible de demander la liste des applications installées	INSTALLEDAPPLICATIONLIST_COMMAND_FAILED	30 jours
Il est impossible de demander les informations générales sur l'appareil mobile	DEVICEINFORMATION_COMMAND_FAILED	30 jours
Il est impossible de demander les informations sur la sécurité	SECURITYINFO_COMMAND_FAILED	30 jours
Impossible de verrouiller l'appareil mobile	DEVICELOCK_COMMAND_FAILED	30 jours
Il est impossible de purger le mot de passe	CLEARPASSCODE_COMMAND_FAILED	30 jours
Échec de la suppression des données de l'appareil mobile	ERASEDEVICE_COMMAND_FAILED	30 jours
Il est impossible d'installer l'application	INSTALLAPPLICATION_COMMAND_FAILED	30 jours
Il est impossible d'installer le code rédemption pour l'application	APPLYREDEMPTIONCODE_COMMAND_FAILED	30 jours
Il est impossible de demander la liste des apps administrées	MANAGEDAPPLICATIONLIST_COMMAND_FAILED	30 jours
Il est impossible de supprimer l'app administrée	REMOVEAPPLICATION_COMMAND_FAILED	30 jours
Les paramètres d'itinérance sont rejetés	SETROAMINGSETTINGS_COMMAND_FAILED	30 jours
Une erreur s'est produite dans le fonctionnement de l'app	PRODUCT_FAILURE	30 jours
Le résultat d'exécution de la commande contient les données incorrectes	MALFORMED_COMMAND	30 jours
Il est impossible d'envoyer une notification (Push Notification)	SEND_PUSH_NOTIFICATION_FAILED	30 jours
Il est impossible d'envoyer une commande	SEND_COMMAND_FAILED	30 jours
L'appareil est introuvable	DEVICE_NOT_FOUND	30 jours

Événements d'avertissement du Serveur MDM iOS

Le tableau suivant affiche les événements du Serveur MDM iOS de Kaspersky Security Center dont le niveau de gravité est **Avertissement**.

Pour chaque événement pouvant être généré par une application, vous pouvez spécifier les paramètres de notification et les paramètres de stockage sous l'onglet **Configuration des événements** dans la stratégie de l'application. Si vous souhaitez configurer les paramètres de notification pour tous les événements à la fois, configurez les paramètres de notification généraux dans les propriétés du Serveur d'administration.

Événements d'avertissement du Serveur MDM iOS

Nom affiché du type d'événement	Type d'événement	Durée de stockage par défaut
Tentative de connexion d'un appareil mobile verrouillé	INACTICE_DEVICE_TRY_CONNECTED	30 jours
Le profil est supprimé	MDM_PROFILE_WAS_REMOVED	30 jours
Tentative de réutilisation du certificat client	CLIENT_CERT_ALREADY_IN_USE	30 jours
Un appareil inactif a été détecté	FOUND_INACTIVE_DEVICE	30 jours
Le code rédemption est requis	NEED_REDEMPTION_CODE	30 jours
Le profil a été inclus dans une stratégie supprimée de l'appareil	UMDM_PROFILE_WAS_REMOVED	30 jours

Événements d'information du Serveur MDM iOS

Le tableau suivant reprend les événements du Serveur MDM iOS de Kaspersky Security Center, regroupés par niveau de gravité **Information**.

Pour chaque événement pouvant être généré par une application, vous pouvez spécifier les paramètres de notification et les paramètres de stockage sous l'onglet **Configuration des événements** dans la stratégie de l'application. Si vous souhaitez configurer les paramètres de notification pour tous les événements à la fois, configurez les paramètres de notification généraux dans les propriétés du Serveur d'administration.

Événements d'information du Serveur MDM iOS

Nom affiché du type d'événement	Type d'événement	Durée de stockage par défaut
Un nouvel appareil mobile est connecté	NEW_DEVICE_CONNECTED	30 jours
La demande de la liste des profils est exécutée avec succès	PROFILELIST_COMMAND_SUCCESSFULL	30 jours
L'installation du profil est exécutée avec succès	INSTALLPROFILE_COMMAND_SUCCESSFULL	30 jours
La suppression du profil est exécutée avec succès	REMOVEPROFILE_COMMAND_SUCCESSFULL	30 jours
La demande de la liste des profils provisioning est exécutée avec succès	PROVISIONINGPROFILELIST_COMMAND_SUCCESSFULL	30 jours
L'installation du profil provisioning est exécutée avec succès	INSTALLPROVISIONINGPROFILE_COMMAND_SUCCESSFULL	30 jours
La suppression du profil provisioning est exécutée avec succès	REMOVEPROVISIONINGPROFILE_COMMAND_SUCCESSFULL	30 jours
La demande de la liste des certificats numériques est exécutée avec succès	CERTIFICATELIST_COMMAND_SUCCESSFULL	30 jours
La demande de la liste des applications installées est exécutée avec succès	INSTALLEDAPPLICATIONLIST_COMMAND_SUCCESSFULL	30 jours
La demande des informations générales sur l'appareil mobile est exécutée avec succès	DEVICEINFORMATION_COMMAND_SUCCESSFULL	30 jours
La demande des informations sur la sécurité est exécutée avec succès	SECURITYINFO_COMMAND_SUCCESSFULL	30 jours
L'appareil mobile est bloqué avec succès	DEVICELOCK_COMMAND_SUCCESSFULL	30 jours
La purge du mot de passe est exécutée avec succès	CLEARPASSCODE_COMMAND_SUCCESSFULL	30 jours
Les données ont été supprimées de l'appareil mobile	ERASEDEVICE_COMMAND_SUCCESSFULL	30 jours
L'installation de l'application est exécutée avec succès	INSTALLAPPLICATION_COMMAND_SUCCESSFULL	30 jours
L'installation du code rédemption pour l'application a réussi	APPLYREDEMPTIONCODE_COMMAND_SUCCESSFULL	30 jours
La demande de la liste des apps administrées est exécutée avec succès	MANAGEDAPPLICATIONLIST_COMMAND_SUCCESSFULL	30 jours
L'application administrée a été supprimée avec succès	REMOVEAPPLICATION_COMMAND_SUCCESSFULL	30 jours
Les paramètres d'itinérance ont été appliqués	SETROAMINGSETTINGS_COMMAND_SUCCESSFUL	30 jours

Blocage des événements fréquents

Cette section fournit des informations sur la gestion du blocage des événements fréquents et sur la suppression du blocage des événements fréquents.

À propos du blocage des événements fréquents

Une application administrée, par exemple Kaspersky Endpoint Security for Windows, installée sur un ou plusieurs appareils administrés peut envoyer de nombreux événements du même type au Serveur d'administration. La réception d'événements fréquents peut surcharger la base de données du Serveur d'administration et écraser d'autres événements. Le Serveur d'administration commence à bloquer les événements les plus fréquents lorsque le nombre de tous les événements reçus dépasse la limite indiquée pour la base de données.

Le Serveur d'administration bloque la réception automatique des événements fréquents. Vous ne pouvez pas bloquer vous-même les événements fréquents ni choisir les événements à bloquer.

Si vous voulez découvrir si un événement est bloqué, vous pouvez consulter la liste des notifications ou vous pouvez vérifier si cet événement est présent dans la section **Blocage d'événements fréquents** des propriétés du Serveur d'administration. Si l'événement est bloqué, vous pouvez effectuer l'une des opérations suivantes :

- Si vous voulez éviter d'écraser la base de données, vous pouvez continuer à bloquer la réception de ce type d'événements.
- Si vous voulez, par exemple, trouver la raison de l'envoi des événements fréquents au Serveur d'administration, vous pouvez débloquer les événements fréquents et continuer à recevoir les événements de ce type de toute façon.
- Si vous souhaitez continuer à recevoir les événements fréquents jusqu'à ce qu'ils soient de nouveau bloqués, vous pouvez supprimer le blocage des événements fréquents.

Gestion du blocage des événements fréquents

Le Serveur d'administration bloque la réception automatique d'événements fréquents, mais vous pouvez arrêter le blocage et continuer à recevoir des événements fréquents. Vous pouvez également bloquer la réception d'événements fréquents que vous avez débloqués auparavant.

Pour administrer le blocage des événements fréquents, procédez comme suit :

1. Dans le menu principal, cliquez sur l'icône des paramètres ( ) en regard du nom du Serveur d'administration requis.

   La fenêtre des propriétés du Serveur d'administration s'ouvre.

2. Sous l'onglet **Général**, sélectionnez la section **Blocage d'événements fréquents**.

3. Dans la section **Blocage d'événements fréquents** :

   - Si vous souhaitez débloquer la réception d'événements fréquents, procédez comme suit :

     a. Sélectionnez les événements fréquents que vous souhaitez débloquer, puis cliquez sur le bouton **Exclure**.

     b. Cliquez sur le bouton **Enregistrer**.

   - Si vous souhaitez bloquer les événements fréquents, procédez comme suit :

     a. Sélectionnez les événements de masse que vous souhaitez bloquer, puis cliquez sur le bouton **Verrouiller**.

     b. Cliquez sur le bouton **Enregistrer**.

Le Serveur d'administration reçoit les événements fréquents non bloqués et ne reçoit pas les événements fréquents bloqués.

Suppression du blocage des événements fréquents

Vous pouvez supprimer le blocage des événements fréquents et commencer à recevoir ces événements jusqu'à ce que le Serveur d'administration bloque de nouveau ces événements fréquents.

Pour supprimer le blocage des événements fréquents, procédez comme suit :

1. Dans le menu principal, cliquez sur l'icône des paramètres ( ) en regard du nom du Serveur d'administration requis.

   La fenêtre des propriétés du Serveur d'administration s'ouvre.

2. Sous l'onglet **Général**, sélectionnez la section **Blocage d'événements fréquents**.

3. Dans la section **Blocage d'événements fréquents**, sélectionnez les types d'événements fréquents pour lesquels vous souhaitez supprimer le blocage.

4. Cliquez sur le bouton **Retirer du blocage**.

L'événement fréquent est supprimé de la liste des événements fréquents. Le Serveur d'administration recevra des événements de ce type.

Réception des événements de Kaspersky Security for Microsoft Exchange Servers

Les informations sur les événements pendant le fonctionnement des applications administrées, telles que Kaspersky Endpoint Security for Windows, sont transférées des appareils administrés et enregistrées dans la base de données du Serveur d'administration. Par défaut, les événements de Kaspersky Security for Microsoft Exchange Servers version 9.0 MR6 et antérieures ne sont pas enregistrés dans la base de données du Serveur d'administration. Si Kaspersky Security for Microsoft Exchange Servers version 9.0 MR6 et versions antérieures est installé sur les appareils administrés de votre organisation et que vous souhaitez recevoir des événements de cette application, activez l'enregistrement des événements pour cette application à l'aide de l'utilitaire klscflag.

Pour activer l'enregistrement des événements pour Kaspersky Security for Microsoft Exchange Servers :

1. Sur l'appareil du Serveur d'administration, exécutez l'invite de commande Windows sous un compte avec des droits d'administrateur.
2. Remplacez votre répertoire actuel par le dossier d'installation de Kaspersky Security Center (généralement, C:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center).
3. Exécutez l'une des commandes suivantes :

   - Pour le Serveur d'administration installé sur un cluster de basculement Windows Server :

     ```
     klscflag.exe --stp cluster -fset -pv klserver -n
     KLSRV_EVP_ENABLE_HOST_EVENT_BODY_VALIDATION -t d -v 0
     ```

   - Pour le Serveur d'administration installé sur un nœud du cluster de basculement Kaspersky Security Center :

     ```
     klscflag.exe --stp klfoc -fset -pv klserver -n
     KLSRV_EVP_ENABLE_HOST_EVENT_BODY_VALIDATION -t d -v 0
     ```

   - Pour le Serveur d'administration qui ne fonctionne pas sur un cluster :

     ```
     klscflag.exe -fset -pv klserver -n KLSRV_EVP_ENABLE_HOST_EVENT_BODY_VALIDATION -t d
     -v 0
     ```

L'enregistrement des événements pour Kaspersky Security for Microsoft Exchange Servers est activé.

Pour Kaspersky Security for Microsoft Exchange Servers, vous ne pouvez pas définir la durée de stockage des événements ni sélectionner les événements à enregistrer dans le référentiel du Serveur d'administration. Vous pouvez définir le nombre d'événements maximal pouvant être enregistrés dans le référentiel. Ce paramètre s'applique aux événements reçus de toutes les applications Kaspersky.

Notifications et états de l'appareil

Cette section contient des informations sur l'affichage des notifications, la configuration de la diffusion des notifications, l'utilisation des états de l'appareil et l'activation de la modification de l'état de l'appareil.

Utilisation des notifications

Les notifications servent à vous alerter des événements et vous permettent d'accélérer la réaction à ces événements en effectuant rapidement les actions recommandées ou que vous estimez appropriées.

En fonction de la méthode de notification choisie, les types de notifications suivants sont disponibles :

- Notifications à l'écran
- Notifications par SMS
- Notifications par email
- Notifications par fichier exécutable ou script

Notifications à l'écran

Les notifications à l'écran servent à vous alerter des événements regroupés par niveaux d'importance (*Critique*, *Attention* et *Information*).

Une notification à l'écran peut être à un des deux états suivants :

- *Révisé*. Cela signifie que vous avez effectué l'action recommandée pour la notification ou que vous avez affecté manuellement cet état à la notification.
- *Non révisé*. Cela signifie que vous n'avez pas effectué l'action recommandée pour la notification ou que vous n'avez pas affecté manuellement cet état à la notification.

Par défaut, la liste de notifications inclut les notifications à l'état *Non révisé*.

Vous pouvez surveiller le réseau de votre organisation en affichant les notifications à l'écran et en y réagissant en temps réel.

Notifications par email, par SMS et par fichier exécutable ou script

Kaspersky Security Center vous permet de surveiller le réseau de votre organisation en envoyant des notifications sur tout événement que vous considérez comme important. Pour tout événement, vous pouvez configurer les notifications par email, par SMS ou par lancement d'un fichier exécutable ou d'un script.

Dès réception de notifications par email ou par SMS, vous pouvez décider de votre réponse à l'événement. Cette réaction doit être la plus appropriée pour le réseau de votre organisation. Le lancement d'un fichier exécutable ou d'un script vous permet de prédéfinir une réaction à un événement. Vous pouvez également envisager le lancement d'un fichier exécutable ou d'un script comme réponse principale à un événement. Après l'exécution du fichier exécutable, vous pouvez prendre d'autres mesures pour réagir à l'événement.

Affichage des notifications à l'écran

Vous pouvez afficher les notifications à l'écran de trois façons différentes :

- Dans la section **Surveillance et rapports** → **Notifications**. Ici, vous pouvez afficher des notifications concernant les catégories prédéfinies.
- Dans une fenêtre séparée qui peut être ouverte, quelle que soit la section en cours d'utilisation. Dans ce cas, vous pouvez marquer les notifications comme révisées.
- Dans le widget **Notifications en fonction du niveau de gravité sélectionné**, dans la section **Surveillance et rapports** → **Tableau de bord**. Dans le widget, vous pouvez afficher uniquement les notifications des événements qui ont les niveaux d'importance *Critique* et *Attention*.

Vous pouvez effectuer des actions, par exemple, vous pouvez répondre à un événement.

Pour afficher les notifications à partir de catégories prédéfinies :

1. Dans le menu principal, accédez à **Surveillance et rapports** → **Notifications**.

   La catégorie **Toutes les notifications** est sélectionnée dans le volet gauche et toutes les notifications s'affichent dans le volet droit.

2. Dans le volet gauche, sélectionnez une des catégories :

   - **Déploiement**
   - **Appareils**
   - **Protection**
   - **Mises à jour** (ceci inclut les notifications à propos des applications de Kaspersky disponibles au téléchargement et les notifications à propos des mises à jour des bases antivirus que vous avez téléchargées)
   - **Protection contre les Exploits**
   - **Serveur d'administration** (ceci inclut les événements du Serveur d'administration uniquement)
   - **Liens utiles** (ceci inclut des liens vers des ressources Kaspersky, par exemple le support technique de Kaspersky, le forum Kaspersky, la page de renouvellement de licence, ou l'Encyclopédie IT de Kaspersky)

   Une liste des notifications de la catégorie sélectionnée s'affiche. La liste contient les éléments suivants :

- Icône liée au sujet de la notification : déploiement (), protection (), mises à jour (), administration d'appareils (), Protection contre les Exploits (), Serveur d'administration ().
- Niveau d'importance des notifications. Les notifications des niveaux d'importance suivants sont affichées : **Notifications critiques** (), **Notifications d'avertissement** (), **Notifications d'information**. Les notifications dans la liste sont regroupées par niveau d'importance.
- **Notification**. Contient une description de la notification.

- **Action**. Contient un lien vers une action rapide que nous vous recommandons. Par exemple, en cliquant sur ce lien, vous pouvez accéder au stockage et installer les applications de sécurité sur les appareils ou afficher une liste des appareils ou des événements. Après que vous avez effectué l'action recommandée pour la notification, cette notification passe à l'état *révisé*.

- **État enregistré**. Contient le nombre de jours ou écoulé(e)s depuis que la notification a été enregistrée sur le Serveur d'administration.

Pour consulter les notifications à l'écran dans une fenêtre séparée par niveau d'importance :

1. Dans le coin supérieur droit de Kaspersky Security Center Web Console, cliquez sur l'icône drapeau ().

   Si l'icône drapeau a un point rouge, cela signifie que certaines notifications n'ont pas été révisées.

   Une fenêtre s'ouvre avec la liste des notifications. Par défaut, l'onglet **Toutes les notifications** est sélectionné et les notifications sont regroupées par niveau d'importance : *Critique*, *Attention* et *Information*.

2. Sélectionnez l'onglet **Système**.

   La liste des notifications de niveau d'importance *Critique* () et *Attention* () s'affiche. La liste des notification inclut les éléments suivants :

   - Marqueur de couleur. Les notifications critiques sont marquées en rouge. Les notifications d'avertissement sont marquées en jaune.
   - Icône indiquant le sujet de la notification : déploiement (), protection (), mises à jour (), administration d'appareils (), Protection contre les Exploits (), Serveur d'administration ().
   - Description de la notification.
   - Icône du drapeau. L'icône du drapeau est rouge si des notifications se sont vu attribuer l'état *Non révisé*. Quand vous sélectionnez l'icône du drapeau et attribuez l'état *Révisé* à une notification, l'icône passe du gris au blanc.
   - Lien vers l'action recommandée. Lorsque vous effectuez l'action recommandée après avoir cliqué sur le lien, la notification passe à l'état *Révisé*.
   - Nombre de jours qui se sont écoulés depuis la date à laquelle la notification a été enregistrée sur le Serveur d'administration.

3. Sélectionnez l'onglet **Plus**.

   La liste des notifications de niveau d'importance *Information* s'affiche.

   L'organisation de la liste est identique à celle de la liste dans l'onglet **Système** (voir la description ci-dessus). La seule différence est l'absence d'un marqueur de couleur.

Vous pouvez filtrer les notifications par l'intervalle de date lorsqu'elles ont été enregistrées sur le Serveur d'administration. Cochez la case **Consulter le filtre** pour gérer le filtre.

Pour consulter les notifications à l'écran dans le widget :

1. Dans la section **Tableau de bord**, sélectionnez **Ajouter ou restaurer un widget web**.

2. Dans la fenêtre qui s'ouvre, cliquez sur la catégorie **Autre**, sélectionnez le widget **Notifications en fonction du niveau de gravité sélectionné** et cliquez sur Ajouter.

   Le widget apparaît désormais sous l'onglet **Tableau de bord**. Par défaut, les notifications de niveau d'importance *Critique* s'affichent sur le widget.

   Vous pouvez cliquer sur le bouton **Paramètres** du widget et modifier les paramètres du widget pour consulter les notifications du niveau d'importance *Attention*. Sinon, vous pouvez ajouter un autre widget : **Notifications en fonction du niveau de gravité sélectionné** avec un niveau d'importance *Attention*.

   La liste des notifications sur le widget est limitée par sa taille et inclut deux notifications. Ces deux notifications concernent les derniers événements.

La liste des notifications sur le widget inclut les éléments suivants :

- Icône liée au sujet de la notification : déploiement (), protection (), mises à jour (), administration d'appareils (), Protection contre les Exploits (), Serveur d'administration ().

- Description de la notification avec un lien vers l'action recommandée. Lorsque vous effectuez l'action recommandée après avoir cliqué sur le lien, la notification passe à l'état *Révisé*.

- Nombre de jours ou nombre d'heures écoulé(e)s depuis la date à laquelle la notification a été enregistrée sur le Serveur d'administration.

- Lien vers les autres notifications. Ce lien renvoie à la vue des notifications dans la section **Notifications** de la section **Surveillance et rapports**.

À propos des états des appareils

Kaspersky Security Center attribue un état à chaque appareil administré. Chaque état dépend du respect des conditions définies par l'utilisateur. Dans certains cas, lors de l'attribution d'un état à un appareil, Kaspersky Security Center prend en compte l'indicateur de visibilité de l'appareil sur le réseau (voir le tableau ci-dessous). Si Kaspersky Security Center ne trouve pas d'appareil sur le réseau dans un délai de deux heures, l'indicateur de visibilité de l'appareil est défini sur *Non visible*.

Les états sont les suivants :

- *Critique* ou *Critique/Visible*

- *Attention* ou *Attention/Visible*

- *OK* ou *OK/Visible*

Le tableau ci-dessous reprend les conditions d'attribution de l'état *Critique* ou *Attention* à l'appareil et ses valeurs possibles.

Conditions d'attribution des états à l'appareil

Condition	Description de la condition	Valeurs possibles
L'application de sécurité n'est pas installée	L'Agent d'administration est installé sur l'appareil mais une application de sécurité n'est pas installée.	• Le bouton radio est allumé. • Le bouton radio est éteint.
Trop de virus ont été détectés	Certains virus ont été retrouvés sur l'appareil par une tâche de détection de virus, par exemple, la tâches de *Analyse des logiciels malveillants*, et le nombre de virus détectés dépasse la valeur spécifiée.	Plus de 0.
Le niveau de la Protection en temps réel diffère de celui défini par l'Administrateur	L'appareil est visible sur le réseau, mais le niveau de protection en temps réel est différent de celui défini par l'administrateur (dans la condition) pour l'état de l'appareil.	• Arrêté. • Suspendu(e). • En cours.
La recherche d'applications malveillantes n'a pas été exécutée depuis longtemps	L'appareil est visible sur le réseau et une application de sécurité est installée sur l'appareil, mais ni la tâche d'*Analyse des logiciels malveillants* ni une tâche d'analyse locale n'ont été exécutées dans l'intervalle de temps spécifié. La condition s'applique uniquement aux appareils qui ont été ajoutés à la base de données du Serveur d'administration il y a 7 jours ou avant.	Plus de 1 jour.
Les bases sont dépassées	L'appareil est visible sur le réseau, et une application de sécurité est installée sur l'appareil, mais les bases antivirus n'ont pas été mises à jour sur cet appareil dans la période indiquée. La condition s'applique uniquement aux appareils qui ont été ajoutés à la base de données du Serveur d'administration il y a 1 jour ou avant.	Plus de 1 jour.
Ne s'est pas connecté depuis longtemps	L'Agent d'administration est installé sur l'appareil, mais l'appareil ne s'est pas connecté au Serveur d'administration dans la période indiquée car l'appareil était désactivé.	Plus de 1 jour.
Des menaces actives sont détectées	La quantité d'objets non traités dans le dossier **Menaces actives** dépasse la valeur indiquée.	Plus de 0 pièce.
Redémarrage requis	L'appareil est visible sur le réseau, mais une application nécessite le redémarrage de l'appareil depuis la durée indiquée et pour l'une des raisons sélectionnées.	Plus de 0 minute.
Des applications incompatibles sont installées	L'appareil est visible sur le réseau, mais l'inventaire des applications effectué par l'Agent d'administration a détecté des applications incompatibles installées sur l'appareil.	• Le bouton radio est éteint. • Le bouton radio est allumé.
Vulnérabilités dans les applications	L'appareil est visible sur le réseau, et l'Agent d'administration est installé sur l'appareil, mais la tâche *Recherche de vulnérabilités et de mises à jour requises* a détecté des vulnérabilités avec le niveau de gravité indiqué dans les applications installées sur l'appareil.	• Critique. • Élevé. • Normal. • Ignorer s'il est impossible de fermer la vulnérabilité. • Ignorer si la mise à jour a été désignée à l'installation.
La licence a expiré	L'appareil est visible sur le réseau, mais la licence a expiré.	• Le bouton radio est éteint. • Le bouton radio est allumé.
la licence expire bientôt	L'appareil est visible sur le réseau, mais la licence expirera sur l'appareil dans moins de jours que le nombre indiqué.	Moins de 0 jours.
La vérification de mises à jour Windows Update n'a pas eu lieu depuis longtemps	L'appareil est visible sur le réseau, mais la tâche *Synchronisation des mises à jour Windows Update* n'a plus été exécutée dans la période indiquée.	Plus de 1 jour.

Condition	Description de la condition	Valeurs possibles
État de chiffrement non valide	L'Agent d'administration est installé sur l'appareil mais le résultat du chiffrement de l'appareil est égal à la valeur indiquée.	• Ne correspond pas à la stratégie à cause du refus de l'utilisateur (uniquement pour les appareils externes). • Ne correspond pas à la stratégie à cause de l'erreur. • Stratégie en cours d'application – le redémarrage est requis. • La stratégie de chiffrement n'est pas définie. • Non pris en charge. • Stratégie en cours d'application.
Les paramètres de l'appareil mobile ne correspondent pas à la stratégie	Les paramètres de l'appareil mobile se distinguent des paramètres définis dans la stratégie Kaspersky Endpoint Security for Android lors de l'analyse des règles de concordance.	• Le bouton radio est éteint. • Le bouton radio est allumé.
Problèmes de sécurité non traités détectés	Certains problèmes de sécurité non traités ont été détectés sur l'appareil. Les problèmes de sécurité peuvent être créés automatiquement, à l'aide des applications administrées de Kaspersky installées sur l'appareil client, ou manuellement par l'administrateur.	• Le bouton radio est éteint. • Le bouton radio est allumé.
État de l'appareil défini par l'application	L'état de l'appareil est défini par l'application administrée.	• Le bouton radio est éteint. • Le bouton radio est allumé.
Espace disque épuisé sur l'appareil	L'espace disque disponible est inférieur à la valeur indiquée ou l'appareil n'a pas pu être synchronisé avec le Serveur d'administration. L'état *Critique* ou *Attention* est redéfini sur *OK* lorsque l'appareil est synchronisé avec le Serveur d'administration et que l'espace libre sur l'appareil est supérieur ou égal à la valeur spécifiée.	Plus de 0 Mo.
L'appareil n'est plus administré	Lors de la recherche d'appareils, celui-ci est considéré comme visible sur le réseau, mais plus de trois tentatives ratées de synchronisation avec le Serveur d'administration ont eu lieu.	• Le bouton radio est éteint. • Le bouton radio est allumé.
La protection est désactivée	L'appareil est visible sur le réseau, mais l'application de sécurité sur l'appareil est désactivée depuis plus longtemps que la durée indiquée. Dans ce cas, l'état de l'application de sécurité est *arrêté* ou *échec*, et différent de l'état suivant : *démarrage*, *en cours d'exécution* ou *suspendu*.	Plus de 0 minute.
L'application de sécurité n'est pas en cours d'exécution	L'appareil est visible sur le réseau, et une application de sécurité est installée sur l'appareil, mais n'est pas exécutée.	• Le bouton radio est éteint. • Le bouton radio est allumé.

Kaspersky Security Center permet de configurer la permutation automatique de l'état d'un appareil dans un groupe d'administration quand les conditions définies sont remplies. Quand les conditions définies sont remplies, l'appareil client reçoit un des états suivants : *Critique* ou *Attention*. Lorsque les conditions spécifiées ne sont pas remplies, l'état *OK* est affecté à l'appareil client.

Des différents états peuvent correspondre à des différentes valeurs d'une condition. Par exemple, par défaut, si vous respectez la condition **Les bases sont dépassées** avec la valeur **Plus de 3 jours**, l'appareil client se verra affecter l'état *Avertissement*, et avec la valeur **Plus de 7 jours**, l'état *Critique*.

Si vous mettez à niveau Kaspersky Security Center à partir de la version précédente, les valeurs de **Les bases sont dépassées** la condition d'attribution de l'état à *Critique* ou *Avertissement* ne change pas.

Lorsque Kaspersky Security Center attribue un statut à un appareil, pour certaines conditions (voir la colonne Description de la condition), l'indicateur de visibilité est pris en considération. Par exemple, si un appareil administré a reçu l'état *Critique* parce que la condition Les bases sont dépassées a été remplie, et qu'ensuite l'indicateur de visibilité a été placé pour l'appareil, alors l'appareil reçoit l'état *OK*.

Configuration de la permutation des états des appareils

Vous pouvez modifier les conditions pour attribuer le statut *Critique* ou *Avertissement* à un appareil.

Pour activer le changement d'état de l'appareil sur Critique :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Hiérarchie des groupes**.
2. Dans la liste des groupes qui s'affiche, cliquez sur le lien portant le nom d'un groupe dont vous voulez changer les états de l'appareil.
3. Dans la fenêtre des propriétés qui s'ouvre, sélectionnez l'onglet **État de l'appareil**.
4. Dans le volet de gauche, sélectionnez **Critique**.
5. Dans le volet droit, dans la section **Définir l'état comme "Critique" si les options suivantes sont définies**, activez la condition pour basculer un appareil en état *Critique*.

   Vous pouvez modifier seulement les paramètres qui ne sont pas verrouillés dans la stratégie parent.

6. Sélectionnez le bouton radio à côté de la condition dans la liste.
7. Dans le coin supérieur gauche de la liste, cliquez sur le bouton **Modifier**.
8. Définissez la valeur requise pour la condition sélectionnée.

   Certaines conditions n'acceptent pas de valeurs.

9. Cliquez sur le bouton **OK**.

Lorsque les conditions spécifiées sont remplies, l'appareil administré se voit affecter l'état *Critique*.

Pour activer le changement d'état de l'appareil sur Avertissement :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Hiérarchie des groupes**.
2. Dans la liste des groupes qui s'affiche, cliquez sur le lien portant le nom d'un groupe dont vous voulez changer les états de l'appareil.
3. Dans la fenêtre des propriétés qui s'ouvre, sélectionnez l'onglet **État de l'appareil**.
4. Dans le volet gauche, sélectionnez **Avertissement**.

5. Dans le volet droit, dans la section **Définir l'état comme "Avertissement" si les options suivantes sont définies,** activez la condition pour basculer un appareil en état *Avertissement*.

   Vous pouvez modifier seulement les paramètres qui ne sont pas verrouillés dans la stratégie parent.

6. Sélectionnez le bouton radio à côté de la condition dans la liste.
7. Dans le coin supérieur gauche de la liste, cliquez sur le bouton **Modifier**.
8. Définissez la valeur requise pour la condition sélectionnée.

   Certaines conditions n'acceptent pas de valeurs.

9. Cliquez sur le bouton **OK**.

Lorsque certaines conditions spécifiées sont remplies, l'appareil administré se voit affecter l'état *Avertissement*.

Configuration des paramètres d'envoi des notifications

Vous pouvez configurer une notification à propos des événements qui se produisent dans Kaspersky Security Center. En fonction de la méthode de notification choisie, les types de notifications suivants sont disponibles :

- Email : quand un événement se produit, Kaspersky Security Center envoie une notification aux adresses email indiquées.
- SMS : quand un événement se produit, Kaspersky Security Center envoie une notification aux numéros de téléphone indiqués.
- Fichier exécutable : quand un événement se produit, le fichier exécutable est exécuté sur le Serveur d'administration.

Pour configurer les paramètres d'envoi des notifications des événements qui se produisent dans Kaspersky Security Center :

1. Dans le menu principal, cliquez sur l'icône des paramètres ( ) en regard du nom du Serveur d'administration requis.

   La fenêtre des propriétés du Serveur d'administration s'ouvre avec l'onglet **Général** sélectionné.

2. Cliquez sur la section **Notification** et, dans le volet droit, sélectionnez l'onglet de la méthode de notification souhaitée :

   - **Email**

L'onglet **Email** vous permet de configurer la notification d'événement par courrier électronique.

Dans le champ **Destinataires (adresses email)**, indiquez les adresses e-mail auxquelles l'application enverra des notifications. Vous pouvez spécifier plusieurs adresses dans ce champ, en les séparant par un point-virgule.

Dans le champ **Serveurs SMTP**, spécifiez les adresses du serveur de messagerie, en les séparant par un point-virgule. Vous pouvez utiliser les valeurs suivantes du paramètre :

- Adresse IPv4 ou IPv6
- Nom de réseau Windows (nom NetBIOS) de l'appareil
- Nom complet du serveur SMTP

Dans le champ **Port du serveur SMTP**, spécifiez le numéro d'un port de communication du serveur SMTP. Le numéro de port par défaut est 25.

Si vous activez l'option **Utiliser la recherche MX de DNS**, vous pouvez utiliser plusieurs enregistrements MX des adresses IP pour le même nom DNS du serveur SMTP. Le même nom DNS peut avoir plusieurs enregistrements MX avec des priorités différentes pour la réception des emails. Le Serveur d'administration tente d'envoyer des notifications par email au serveur SMTP par ordre croissant de priorité des enregistrements MX.

Si vous activez l'option **Utiliser la recherche MX de DNS** et n'activez pas l'utilisation des paramètres TLS, nous vous recommandons d'utiliser les paramètres DNSSEC sur votre appareil serveur comme mesure supplémentaire de protection pour l'envoi des notifications par email.

Si vous activez l'option **Utiliser l'authentification &ESMTP**, vous pouvez spécifier les paramètres d'authentification ESMTP dans les champs **Nom d'utilisateur** et **Mot de passe**. Par défaut, cette option est décochée et les paramètres d'authentification ESMTP ne sont pas disponibles.

Vous pouvez indiquer les paramètres TLS de connexion au serveur SMTP :

- **Ne pas utiliser le protocole TLS**

Vous pouvez choisir cette option si vous désactivez le chiffrement des emails.

- **Utiliser le protocole TLS si le serveur SMTP le permet**

Vous pouvez choisir cette option si vous voulez utiliser une connexion TLS pour un serveur SMTP. Si le serveur SMTP n'est pas compatible avec TLS, le Serveur d'administration connecte le serveur SMTP sans utiliser TLS.

- **Utiliser toujours le protocole TLS, vérifier la validité du certificat du serveur**

Vous pouvez choisir cette option si vous voulez utiliser les paramètres d'authentification TLS. Si le serveur SMTP n'est pas compatible avec TLS, le Serveur d'administration ne peut pas connecter le serveur SMTP.

Nous vous recommandons d'utiliser cette option pour améliorer la protection de la connexion avec un serveur SMTP. Si vous choisissez cette option, vous pouvez définir les paramètres d'authentification pour une connexion TLS.

Si vous sélectionnez la valeur **Utiliser toujours le protocole TLS, vérifier la validité du certificat du serveur**, vous pouvez définir un certificat pour l'authentification du serveur SMTP et choisir si vous souhaitez activer la communication via n'importe quelle version de TLS ou uniquement via TLS 1.2 ou les versions ultérieures. Vous pouvez également spécifier un certificat pour l'authentification du client sur le serveur SMTP.

Vous pouvez préciser les certificats pour une connexion TLS en cliquant sur le lien **Indiquer les certificats** :

- Recherchez un fichier de certificat de serveur SMTP :

Vous pouvez recevoir un fichier avec la liste des certificats de l'autorité de certification de confiance et charger le fichier sur le Serveur d'administration. Kaspersky Security Center vérifie si le certificat d'un serveur SMTP est également signé par une autorité de certification de confiance ou non. Kaspersky Security Center ne peut pas se connecter à un serveur SMTP si le certificat du serveur SMTP ne provient pas d'une autorité de certification de confiance.

- Recherchez un fichier de certificat client :

Vous pouvez utiliser un certificat que vous avez reçu de n'importe quelle source, par exemple, de n'importe quelle autorité de certification de confiance. Vous devez spécifier le certificat et sa clé privée en utilisant l'un des types de certificats suivants :

- Certificat X-509 :

Vous devez spécifier un fichier avec le certificat et un fichier avec la clé privée. Les deux fichiers ne dépendent pas l'un de l'autre, et l'ordre de chargement des fichiers est sans importance. Lorsque les deux fichiers sont chargés, vous devez spécifier le mot de passe pour décoder la clé privée. Le mot de passe peut présenter une valeur vide si la clé privée n'est pas encodée.

- Conteneur pkcs12 :

Vous devez charger un seul fichier contenant le certificat et sa clé privée. Lorsque le fichier est chargé, vous devez ensuite indiquer le mot de passe pour décoder la clé privée. Le mot de passe peut présenter une valeur vide si la clé privée n'est pas encodée.

Dans le champ **Objet**, spécifiez l'objet de l'email. Vous pouvez laisser ce champ vide.

Dans la liste déroulante **Modèle d'objet**, sélectionnez le modèle de votre objet. Une variable déterminée par le modèle sélectionné est placée automatiquement dans le champ **Objet**. Vous pouvez construire un objet d'email en sélectionnant plusieurs modèles d'objet.

Dans le champ **Adresse email de l'expéditeur**, indiquez l'adresse email de l'expéditeur. Si vous laissez ce champ vide, c'est par défaut l'adresse du destinataire qui est utilisée. Il n'est pas recommandé d'utiliser une adresse email fictive.

Le champ **Message de notification** contient du texte standard avec des informations sur l'événement que l'application envoie lors d'un événement. Ce texte inclut des paramètres de remplacement, comme le nom de l'événement, le nom de l'appareil et le nom de domaine. Vous pouvez modifier le texte du message en ajoutant d'autres paramètres de remplacement avec des détails plus pertinents de l'événement.

> Si le texte de notification contient un caractère en pourcentage (%), vous devez l'indiquer deux fois de suite pour autoriser l'envoi du message. Par exemple, "La charge du processeur est de 100 %%".

Cliquez sur le lien **Configurer la limite du nombre de notifications** pour indiquer le nombre maximum de notifications que l'application peut envoyer sur l'intervalle de temps spécifié.

Cliquez sur le bouton **Envoyer un message d'essai** pour vérifier si vous avez bien configuré les notifications : l'application envoie une notification de test aux adresses électroniques que vous avez indiquées.

- SMS

L'onglet **SMS** vous permet de configurer la transmission de notifications par SMS des divers événements à un téléphone portable. Les messages SMS sont envoyés via une passerelle de messagerie.

Dans le champ **Serveurs SMTP**, spécifiez les adresses du serveur de messagerie, en les séparant par un point-virgule. Vous pouvez utiliser les valeurs suivantes du paramètre :

- Adresse IPv4 ou IPv6
- Nom de réseau Windows (nom NetBIOS) de l'appareil
- Nom complet du serveur SMTP

Dans le champ **Port du serveur SMTP**, spécifiez le numéro d'un port de communication du serveur SMTP. Le numéro de port par défaut est 25.

Si vous activez l'option **Utiliser l'authentification &ESMTP**, vous pouvez spécifier les paramètres d'authentification ESMTP dans les champs **Nom d'utilisateur** et **Mot de passe**. Par défaut, cette option est décochée et les paramètres d'authentification ESMTP ne sont pas disponibles.

Vous pouvez indiquer les paramètres TLS de connexion au serveur SMTP :

- **Ne pas utiliser le protocole TLS**

Vous pouvez choisir cette option si vous désactivez le chiffrement des emails.

- **Utiliser le protocole TLS si le serveur SMTP le permet**

Vous pouvez choisir cette option si vous voulez utiliser une connexion TLS pour un serveur SMTP. Si le serveur SMTP n'est pas compatible avec TLS, le Serveur d'administration connecte le serveur SMTP sans utiliser TLS.

- **Utiliser toujours le protocole TLS, vérifier la validité du certificat du serveur**

Vous pouvez choisir cette option si vous voulez utiliser les paramètres d'authentification TLS. Si le serveur SMTP n'est pas compatible avec TLS, le Serveur d'administration ne peut pas connecter le serveur SMTP.

Nous vous recommandons d'utiliser cette option pour améliorer la protection de la connexion avec un serveur SMTP. Si vous choisissez cette option, vous pouvez définir les paramètres d'authentification pour une connexion TLS.

Si vous sélectionnez la valeur **Utiliser toujours le protocole TLS, vérifier la validité du certificat du serveur**, vous pouvez définir un certificat pour l'authentification du serveur SMTP et choisir si vous souhaitez activer la communication via n'importe quelle version de TLS ou uniquement via TLS 1.2 ou les versions ultérieures. Vous pouvez également spécifier un certificat pour l'authentification du client sur le serveur SMTP.

Vous pouvez préciser le fichier de certificat du serveur SMTP en cliquant sur le lien **Indiquer les certificats** :

Vous pouvez recevoir un fichier avec la liste des certificats de l'autorité de certification de confiance et charger le fichier sur le Serveur d'administration. Kaspersky Security Center vérifie si le certificat d'un serveur SMTP est également signé par une autorité de certification de confiance ou non. Kaspersky Security Center ne peut pas se connecter à un serveur SMTP si le certificat du serveur SMTP ne provient pas d'une autorité de certification de confiance.

Dans le champ **Destinataires (adresses email)**, indiquez les adresses e-mail auxquelles l'application enverra des notifications. Vous pouvez spécifier plusieurs adresses dans ce champ, en les séparant par un point-virgule. Les notifications seront envoyées aux numéros de téléphone associés aux adresses email spécifiées.

Dans le champ **Objet**, spécifiez l'objet de l'email.

Dans la liste déroulante **Modèle d'objet**, sélectionnez le modèle de votre objet. Une variable conforme au modèle sélectionné est insérée dans le champ **Objet**. Vous pouvez construire un objet d'email en sélectionnant plusieurs modèles d'objet.

Dans le champ **Adresse email de l'expéditeur : Si ce paramètre n'est pas défini, l'adresse du destinataire sera utilisée à la place. Attention : Nous déconseillons l'utilisation d'une fausse adresse email**, indiquez l'adresse email de l'expéditeur. Si vous laissez ce champ vide, c'est par défaut l'adresse du destinataire qui est utilisée. Il n'est pas recommandé d'utiliser une adresse email fictive.

Dans le champ **Numéros de téléphone des destinataires du message SMS**, indiquez les numéros de téléphone mobile des destinataires des notifications SMS.

Dans le champ **Message de notification**, spécifiez un texte avec des informations sur l'événement que l'application envoie lors d'un événement. Ce texte peut inclure des paramètres de remplacement, comme le nom de l'événement, le nom de l'appareil et le nom du domaine.

Si le texte de notification contient un caractère en pourcentage (%), vous devez l'indiquer deux fois de suite pour autoriser l'envoi du message. Par exemple, « La charge du processeur est de 100 %% ».

Cliquez sur le lien **Configurer la limite du nombre de notifications** pour indiquer le nombre maximum de notifications que l'application peut envoyer pendant l'intervalle de temps spécifié.

Cliquez sur **Envoyer un message d'essai** pour vérifier si vous avez correctement configuré les notifications : l'application envoie une notification de test au destinataire que vous avez indiqué.

- **Fichier exécutable à exécuter**

  Si cette méthode de notification est sélectionnée, dans le champ de saisie, vous pouvez indiquer quelle application démarre selon l'événement qui se produit.

  Dans le champ **Fichier exécutable qui doit être lancé sur le Serveur d'administration en cas d'événement**, indiquez le dossier et le nom du fichier à exécuter. Avant d'indiquer le fichier, préparez le fichier et indiquez les variables qui définissent les détails de l'événement à envoyer dans le message de notification. Le dossier et le fichier que vous indiquez doivent se trouver sur le Serveur d'administration.

  Cliquez sur le lien **Configurer la limite du nombre de notifications** pour indiquer le nombre maximum de notifications que l'application peut envoyer sur l'intervalle de temps spécifié.

3. Dans l'onglet, définissez les paramètres des notifications.
4. Cliquez sur **OK** pour fermer la fenêtre des propriétés du Serveur d'administration.

Les paramètres de remise des notifications enregistrées sont appliqués à tous les événements qui se produisent dans Kaspersky Security Center.

Vous pouvez remplacer les paramètres de remise des notifications de certains événements dans la section **Configuration des événements** des paramètres du Serveur d'administration, des paramètres d'une stratégie ou des paramètres d'une application.

Notification relative aux événements via un fichier exécutable

Kaspersky Security Center permet de lancer un fichier exécutable afin de signaler à l'administrateur les événements survenus sur les appareils clients. Le fichier exécutable doit contenir un autre fichier exécutable avec les paramètres variables à envoyer à l'administrateur (voir le tableau ci-dessous).

Paramètres variables de description de l'événement

Variable	Description du paramètre secondaire
%SEVERITY%	Importance de l'événement. Valeurs possibles : • **Information** • **Avertissement** • **Erreur** • **Critique**
%COMPUTER%	Nom de l'appareil où l'événement s'est produit. La longueur maximale du nom de l'appareil est de 256 caractères.
%DOMAIN%	Nom de domaine de l'appareil où l'événement s'est produit.
%EVENT%	Nom du type d'événement. La longueur maximale du nom du type d'événement est de 50 caractères.
%DESCR%	Description de l'événement. La longueur maximale de la description est de 1 000 caractères.
%RISE_TIME%	Heure de création de l'événement.
%KLCSAK_EVENT_TASK_DISPLAY_NAME%	Nom de la tâche. La longueur maximale du nom de la tâche est de 100 caractères.
%KL_PRODUCT%	Nom de l'application.
%KL_VERSION%	Numéro de version de l'application.
%KLCSAK_EVENT_SEVERITY_NUM%	Numéro d'importance de l'événement. Valeurs possibles : • 1—**Information** • 2—**Avertissement** • 3—**Erreur** • 4—**Critique**
%HOST_IP%	Adresse IP de l'appareil où l'événement s'est produit.
%HOST_CONN_IP%	Adresse IP de connexion de l'appareil où l'événement s'est produit.

Exemple :
La notification de l'événement s'opère via un fichier exécutable (par exemple, script1.bat) au sein duquel un autre fichier exécutable (par exemple, script2.bat) contenant la variable %COMPUTER% est lancé. Quand l'événement se produit, le fichier script1.bat est lancé sur l'appareil de l'administrateur. Ce fichier lance à son tour le fichier script2.bat avec la variable %COMPUTER%. L'administrateur reçoit le nom de l'appareil sur lequel l'événement s'est produit.

Annonces de Kaspersky

Cette section décrit comment utiliser, configurer et désactiver les annonces de Kaspersky.

À propos des annonces de Kaspersky

La section des annonces de Kaspersky (**Surveillance et rapports → Annonces de Kaspersky**) vous tient informé en fournissant des informations relatives à votre version de Kaspersky Security Center et aux applications administrées installées sur les appareils administrés. Kaspersky Security Center met régulièrement à jour les informations de la section en supprimant les annonces obsolètes et en ajoutant de nouvelles informations.

Kaspersky Security Center affiche uniquement les annonces Kaspersky relatives au Serveur d'administration actuellement connecté et aux applications Kaspersky installées sur les appareils administrés de ce Serveur d'administration. Les annonces sont affichées individuellement pour tout type de Serveur d'administration : principal, secondaire ou virtuel.

Le Serveur d'administration doit disposer d'une connexion Internet pour recevoir les annonces de Kaspersky.

Les annonces contiennent des informations des types suivants :

- Annonces relatives à la sécurité

  Les annonces relatives à la sécurité visent à maintenir les applications Kaspersky installées sur votre réseau à jour et pleinement fonctionnelles. Les annonces peuvent inclure des informations concernant les mises à jour critiques des applications Kaspersky, des correctifs pour des vulnérabilités détectées et des moyens de résoudre d'autres problèmes dans les applications Kaspersky. Les annonces relatives à la sécurité sont activées par défaut. Si vous ne souhaitez pas recevoir les annonces, vous pouvez désactiver cette fonctionnalité.

  Pour vous montrer les informations correspondant à la configuration de la protection de votre réseau, Kaspersky Security Center envoie des données aux serveurs cloud de Kaspersky et ne reçoit que les annonces relatives aux applications Kaspersky installées sur votre réseau. L'ensemble de données qui peut être envoyé aux serveurs est décrit dans le Contrat de licence utilisateur final que vous acceptez lors de l'installation du Serveur d'administration de Kaspersky Security Center.

- Annonces marketing

  Les annonces marketing incluent des informations concernant les offres spéciales pour vos applications Kaspersky, la publicité et les actualités de Kaspersky. Les annonces marketing sont désactivées par défaut. Vous ne recevez ce type d'annonces que si vous avez activé Kaspersky Security Network (KSN). Vous pouvez désactiver les annonces marketing en désactivant KSN.

  Pour ne vous montrer que les informations pertinentes susceptibles de vous aider à protéger vos appareils réseau et de vous être utiles dans vos tâches quotidiennes, Kaspersky Security Center envoie des données aux serveurs cloud de Kaspersky et reçoit les annonces appropriées. L'ensemble des données qui peut être envoyé aux serveurs est décrit dans la section Données traitées de la Déclaration KSN.

Les nouvelles informations sont réparties dans les catégories suivantes, selon leur importance :

1. Informations critiques
2. Nouvelles importantes
3. Avertissement
4. Information

Lorsque de nouvelles informations apparaissent dans la section des annonces de Kaspersky, Kaspersky Security Center Web Console affiche une étiquette de notification correspondant au niveau d'importance des annonces. Vous pouvez cliquer sur l'étiquette pour afficher cette annonce dans la section des annonces de Kaspersky.

Vous pouvez préciser les paramètres des annonces de Kaspersky, y compris les catégories d'annonces que vous souhaitez afficher et l'endroit où vous souhaitez afficher l'étiquette de notification.

Spécification des paramètres d'annonces de Kaspersky

Dans la section Annonces de Kaspersky, vous pouvez spécifier les paramètres des annonces de Kaspersky, y compris les catégories d'annonces que vous souhaitez afficher et l'endroit où vous souhaitez afficher l'étiquette de notification.

Pour configurer les annonces de Kaspersky, procédez comme suit :

1. Dans le menu principal, accédez à **Surveillance et rapports** → **Annonces de Kaspersky**.
2. Cliquez sur le lien **Paramètres**.

   La fenêtre relative aux paramètres des annonces de Kaspersky s'ouvre.
3. Définissez les paramètres suivants :

   - Sélectionnez le niveau d'importance des annonces que vous souhaitez afficher. Les annonces des autres catégories ne seront pas affichées.
   - Sélectionnez l'endroit où vous souhaitez voir l'étiquette de notification. L'étiquette peut être affichée dans toutes les sections de la console ou dans la section **Surveillance et rapports** et ses sous-sections.
4. Cliquez sur le bouton **OK**.

   Les paramètres des annonces de Kaspersky sont précisés.

Désactivation des annonces de Kaspersky

La section Annonces de Kaspersky (**Surveillance et rapports** → **Annonces de Kaspersky**) vous tient informé en fournissant des informations relatives à votre version de Kaspersky Security Center et aux applications administrées installées sur les appareils administrés. Si vous ne souhaitez pas recevoir les annonces de Kaspersky, vous pouvez désactiver cette fonctionnalité.

Les annonces de Kaspersky incluent deux types d'informations : les annonces relatives à la sécurité et les annonces marketing. Vous pouvez désactiver les annonces de chaque type séparément.

Pour désactiver les annonces relatives à la sécurité, procédez comme suit :

1. Dans le menu principal, cliquez sur l'icône des paramètres ( ) en regard du nom du Serveur d'administration requis.

   La fenêtre des propriétés du Serveur d'administration s'ouvre.
2. Sous l'onglet **Général**, sélectionnez la section **Annonces de Kaspersky**.
3. Basculez le commutateur sur **Annonces relatives à la sécurité Désactivées**.
4. Cliquez sur le bouton **Enregistrer**.

   Les annonces de Kaspersky sont désactivées.

Les annonces marketing sont désactivées par défaut. Vous ne recevez des annonces marketing que si vous avez activé Kaspersky Security Network (KSN). Vous pouvez désactiver ce type d'annonces en désactivant KSN.

Pour désactiver les annonces marketing, procédez comme suit :

1. Dans le menu principal, cliquez sur l'icône des paramètres ( ) en regard du nom du Serveur d'administration requis.

   La fenêtre des propriétés du Serveur d'administration s'ouvre.

2. Sous l'onglet **Général**, sélectionnez la section **Paramètres du proxy KSN**.

3. Désactivez l'option **Utiliser Kaspersky Security Network Activé**.

4. Cliquez sur le bouton **Enregistrer**.

   Les annonces marketing sont désactivées.

Affichage d'informations sur les détections de menaces

Vous pouvez activer ou désactiver l'affichage des informations sur les alertes.

*Pour activer ou désactiver l'affichage de la section **Alerte** dans le menu principal :*

1. Dans le menu principal, allez dans les paramètres de votre compte et sélectionnez **Options d'interface**.

2. Dans la fenêtre **Options d'interface** qui s'ouvre, activez ou désactivez l'option **Afficher les alertes EDR**.

3. Cliquez sur **Enregistrer**.

La console affiche la sous-section **Alerte** dans la section **Surveillance et rapports** du menu principal. Dans la sous-section **Alerte**, vous pouvez voir des informations sur les détections de menaces sur les appareils des points de terminaison. Si vous ajoutez une clé de licence pour EDR Optimum, Kaspersky Security Center Web Console affiche automatiquement la sous-section **Alerte** dans la section **Surveillance et rapports** du menu principal. Vous pouvez également ajouter un widget qui affiche des informations à propos des alertes.

> La sous-section **Alerte** s'affiche automatiquement uniquement si vous avez ajouté la clé de licence pour EDR Optimum avant d'activer l'option **Afficher les alertes EDR**. Si vous avez ajouté la clé de licence après avoir activé l'option **Afficher les alertes EDR**, la sous-section **Alerte** ne s'affichera qu'après avoir réactivé cette option.

Pour afficher correctement les informations détaillées sur les menaces détectées dans la fiche d'alertes, vous devez installer le plug-in de Kaspersky Endpoint Agent et la version compatible du plug-in Kaspersky Endpoint Security (Kaspersky Endpoint Security for Linux 12.1 ou version ultérieure, Kaspersky Endpoint Security for Mac 12.1 ou version ultérieure ou Kaspersky Endpoint Security for Windows 12.6 ou version ultérieure).

Utilisez le menu **Filtre** pour filtrer les alertes sur la base de la date et de la valeur des champs.

Le champ **Type d'objet** contient les valeurs suivantes :

- Inconnu
- Lien de phishing
- Virus
- cheval de Troie

- Outil malveillant
- Cheval de troie de l'administration à distance
- Ver
- Autre application
- Programme publicitaire
- Programme pornographique
- Paquet de programmes dangereux
- Comportement dangereux

Le champ **Réponse automatique** contient les valeurs suivantes :

- Un objet malveillant a été détecté
- Un objet a été supprimé
- Un objet a été désinfecté
- Impossible de désinfecter l'objet
- Objet placé en Quarantaine
- Archive protégée par un mot de passe détectée
- Virus détecté

Cloud Discovery

Kaspersky Security Center vous permet de surveiller l'utilisation des services cloud sur les appareils administrés sous Windows et de bloquer l'accès aux services cloud que vous considérez comme indésirables. La fonctionnalité Cloud Discovery suit les tentatives des utilisateurs d'accéder à ces services via les navigateurs et les applications de bureau. Cette fonctionnalité suit également les tentatives des utilisateurs d'accéder aux services cloud via des connexions non chiffrées (par exemple, en utilisant le protocole HTTP). Cette fonctionnalité vous permet de détecter et d'interrompre l'utilisation des services cloud sous la forme de Shadow IT.

La fonction de blocage est disponible uniquement si vous avez activé Kaspersky Security Center sous une licence Kaspersky Next EDR Optimum ou Kaspersky Next XDR Expert.

La fonctionnalité de blocage est disponible uniquement si vous utilisez Kaspersky Endpoint Security 11.2 for Windows ou une version ultérieure. Les versions antérieures de l'application de sécurité vous permettent uniquement de surveiller l'utilisation des services cloud.

Vous pouvez activer la fonctionnalité Cloud Discovery et sélectionner les stratégies ou les profils de sécurité pour lesquels vous souhaitez activer la fonctionnalité. Vous pouvez également activer ou désactiver la fonctionnalité séparément dans chaque stratégie ou profil de sécurité. Vous pouvez interdire l'accès aux services cloud auxquels vous ne souhaitez pas que les utilisateurs accèdent.

Pour pouvoir interdire l'accès aux services cloud indésirables, assurez-vous que les conditions préalables suivantes sont remplies :

- Vous utilisez Kaspersky Endpoint Security 11.2 for Windows ou une version ultérieure. Les versions antérieures de l'application de sécurité vous permettent uniquement de surveiller l'utilisation des services cloud.
- Vous avez acheté un niveau de licence Kaspersky Next qui offre la possibilité de bloquer l'accès aux services cloud indésirables. Pour en savoir plus, consultez l'aide de Kaspersky Next.

Le widget Cloud Discovery et les rapports Cloud Discovery affichent des informations sur les tentatives d'accès aux services cloud réussies et bloquées. Le widget affiche également le niveau de risque de chaque service cloud. Kaspersky Security Center obtient les informations sur l'utilisation des services cloud pour tous les appareils administrés qui sont protégés uniquement par des stratégies ou des profils de sécurité pour lesquels la fonctionnalité est activée.

Activation de Cloud Discovery à l'aide du widget

La fonctionnalité Cloud Discovery vous permet d'obtenir des informations sur l'utilisation des services cloud par tous les appareils administrés protégés uniquement par des stratégies de sécurité pour lesquelles la fonctionnalité est activée. Vous pouvez activer ou désactiver Cloud Discovery uniquement pour la stratégie Kaspersky Endpoint Security for Windows.

Il existe deux manières d'activer la fonctionnalité Cloud Discovery :

- En utilisant le widget Cloud Discovery.
- Dans les propriétés de la stratégie Kaspersky Endpoint Security for Windows.

  Pour en savoir plus sur l'activation de la fonctionnalité Cloud Discovery dans les propriétés de la stratégie Kaspersky Endpoint Security for Windows, veuillez consulter la section Cloud Discovery de l'aide de Kaspersky Endpoint Security for Windows.

Notez que vous pouvez désactiver la fonctionnalité Cloud Discovery dans les paramètres de la stratégie Kaspersky Endpoint Security for Windows uniquement.

Pour activer Cloud Discovery, vous devez disposer du droit **Écrire** dans la zone fonctionnelle **Caractéristiques générales : fonctionnalité de base**.

Pour activer la fonctionnalité Cloud Discovery à l'aide du widget Cloud Discovery, procédez comme suit :

1. Accédez à Kaspersky Security Center.
2. Dans le menu principal, accédez à **Surveillance et rapports** → **Tableau de bord**.

3. Sur le widget **Cloud Discovery**, cliquez sur le bouton **Activer**.

   Si Kaspersky Endpoint Security for Windows version 12.4 est installé, activez la fonctionnalité Cloud Discovery dans les propriétés de la stratégie de Kaspersky Endpoint Security for Windows. Pour en savoir plus, consultez la section Cloud Discovery de l'aide de Kaspersky Endpoint Security for Windows.

   Si vous disposez d'une version de Kaspersky Endpoint Security for Windows antérieure à la version 12.4, mettez à jour le plug-in Kaspersky Endpoint Security for Windows vers la version 12.5.

4. Dans la fenêtre **Nom de la stratégie** qui s'ouvre, sélectionnez les stratégies de sécurité pour lesquelles vous souhaitez activer la fonctionnalité, puis cliquez sur le bouton **Activer**.

   Les paramètres de stratégie suivants seront activés automatiquement : **Implanter un script dans le trafic Internet pour interagir avec les pages Internet**, **Moniteur de session Internet** et **Analyse des connexions chiffrées**.

La fonctionnalité Cloud Discovery est activée, et le widget est ajouté au tableau de bord.

Ajout du widget Cloud Discovery au tableau de bord

Vous pouvez ajouter le widget **Cloud Discovery** au tableau de bord pour surveiller l'utilisation des services cloud sur les appareils administrés.

Pour ajouter le widget Cloud Discovery à votre tableau de bord, vous devez disposer du droit **Écrire** dans la zone fonctionnelle **Caractéristiques générales : fonctionnalité de base**.

Pour ajouter le widget Cloud Discovery au tableau de bord, procédez comme suit :

1. Accédez à Kaspersky Security Center.
2. Dans le menu principal, accédez à **Surveillance et rapports** → **Tableau de bord**.
3. Cliquez sur le bouton **Ajouter ou restaurer un widget web**.
4. Dans la liste des widgets disponibles, cliquez sur l'icône en forme de chevron (>) en regard de la catégorie **Autres**.
5. Sélectionnez le widget **Cloud Discovery**, puis cliquez sur le bouton **Ajouter**.

   Si la fonctionnalité Cloud Discovery est désactivée, suivez les instructions de la section Activation de Cloud Discovery à l'aide du widget.

Le widget sélectionné est ajouté à la fin du tableau de bord.

Affichage d'informations sur l'utilisation des services cloud

Vous pouvez afficher le widget **Cloud Discovery** qui affiche des informations sur les tentatives d'accès aux services cloud. Le widget affiche également le niveau de risque de chaque service cloud. Kaspersky Security Center obtient les informations sur l'utilisation des services cloud pour tous les appareils administrés qui sont protégés uniquement par des profils de sécurité pour lesquelles la fonctionnalité est activée.

Avant d'afficher les informations, assurez-vous que :

- le widget Cloud Discovery est ajouté au tableau de bord.
- la fonctionnalité Cloud Discovery est activée.
- le droit **Lire** figure dans la zone fonctionnelle **Caractéristiques générales : fonctionnalité de base**.

Pour afficher le widget Cloud Discovery :

1. Accédez à Kaspersky Security Center.
2. Dans le menu principal, accédez à **Surveillance et rapports** → **Tableau de bord**.

   Le widget **Cloud Discovery** s'affiche sur le tableau de bord.
3. Dans la partie gauche du widget **Cloud Discovery**, sélectionnez une catégorie de services cloud.

   Le tableau à droite du widget affiche jusqu'à cinq services, issus de la catégorie sélectionnée, auxquels les utilisateurs tentent le plus souvent d'accéder. Les tentatives réussies et bloquées sont comptabilisées.
4. Dans la partie droite du widget, sélectionnez un service spécifique.

   Le tableau ci-dessous affiche une dizaine d'appareils qui tentent le plus souvent d'accéder au service. Ce tableau permet de créer deux types de rapports : le rapport sur les tentatives d'accès réussies et le rapport sur les tentatives d'accès bloquées.

   De plus, ce tableau permet de bloquer l'accès au service cloud pour un appareil défini.

Le widget affiche les informations demandées.

À partir du widget affiché, vous pouvez effectuer les opérations suivantes :

- Passer à la section **Surveillance et rapports** → **Rapports** pour consulter les rapports de Cloud Discovery.
- Interdire ou autoriser l'accès au service cloud sélectionné.

La fonction de blocage est disponible uniquement si vous avez activé Kaspersky Security Center sous une licence Kaspersky Next EDR Optimum ou Kaspersky Next XDR Expert.

La fonctionnalité de blocage est disponible uniquement si vous utilisez Kaspersky Endpoint Security 11.2 for Windows ou une version ultérieure. Les versions antérieures de l'application de sécurité vous permettent uniquement de surveiller l'utilisation des services cloud.

Niveau de risque d'un service cloud

Cloud Discovery indique un niveau de risque pour chaque service cloud. Le niveau de risque vous aide à déterminer les services qui ne correspondent pas aux exigences de sécurité de votre organisation. Par exemple, vous souhaiterez peut-être prendre en considération le niveau de risque lorsque vous déciderez d'interdire ou non l'accès à un service.

> Le niveau de risque est un indice estimé et ne dit rien sur la qualité d'un service cloud ou sur le fabricant du service. Le niveau de risque est simplement une recommandation des experts de Kaspersky.

Le widget Cloud Discovery affiche les niveaux de risque des services cloud dans la liste de tous les services cloud surveillés.

Bloquer l'accès aux services cloud indésirables

Vous pouvez bloquer l'accès aux services cloud auxquels vous ne souhaitez pas que les utilisateurs accèdent. Vous pouvez également autoriser l'accès à des services cloud qui ont été précédemment bloqués.

Vous souhaiterez peut-être prendre, entre autres, le niveau de risque en considération lorsque vous déciderez d'interdire ou non l'accès à un service.

Vous pouvez interdire ou autoriser l'accès aux services cloud pour une stratégie ou un profil de sécurité.

Il existe deux manières de bloquer l'accès aux services cloud indésirables :

- En utilisant le widget Cloud Discovery.

  Dans ce cas, vous pouvez bloquer l'accès aux services un par un.

- Dans les propriétés de la stratégie Kaspersky Endpoint Security for Windows.

  Dans ce cas, vous pouvez interdire l'accès aux services un par un ou interdire l'ensemble d'une catégorie à la fois.

  Pour en savoir plus sur l'activation de la fonctionnalité Cloud Discovery dans les propriétés de la stratégie Kaspersky Endpoint Security for Windows, veuillez consulter la section Cloud Discovery de l'aide de Kaspersky Endpoint Security for Windows.

Pour interdire ou autoriser l'accès à un service cloud en utilisant le widget, procédez comme suit :

1. Ouvrez le widget Cloud Discovery, puis sélectionnez le service cloud requis.

2. Dans le **Les 10 principaux appareils qui utilisent le service**, trouvez la stratégie ou le profil de sécurité pour lequel vous souhaitez interdire ou autoriser le service.

3. Sur la ligne requise, dans la colonne **État d'accès dans la stratégie/le profil**, exécutez une des actions suivantes :

   - Pour bloquer le service, sélectionnez **Bloqué** dans la liste déroulante.
   - Pour autoriser le service, sélectionnez **Autorisé** dans la liste déroulante.

4. Cliquez sur **Enregistrer**.

L'accès au service sélectionné est bloqué ou autorisé pour la stratégie ou le profil de sécurité.

Journal d'activité de Kaspersky Security Center Web Console

Le journal d'activité de Kaspersky Security Center Web Console peut vous aider à rechercher les causes du dysfonctionnement du logiciel. Lorsque vous contactez le Support Technique de Kaspersky pour un dysfonctionnement de Kaspersky Security Center Web Console, les experts du Support Technique de Kaspersky peuvent vous demander les fichiers journaux de Kaspersky Security Center Web Console. Les fichiers journaux de Kaspersky Security Center Web Console sont stockés dans le dossier <Kaspersky Security Center Web Console installation folder>/logs, tant que vous utilisez l'application. Les fichiers log ne sont pas envoyés automatiquement aux spécialistes du support technique de Kaspersky.

Pour activer le journal d'activité de Kaspersky Security Center Web Console,

Cochez la case **Activer la journalisation des activités de Kaspersky Security Center Web Console** dans la fenêtre **Paramètres de connexion de Kaspersky Security Center Web Console** de l'Assistant d'installation de Kaspersky Security Center Web Console.

Les fichiers log sont au format texte.

Les noms de fichier log sont au format logs- <nom du module>.<nom d'appareil>-<numéro de révision du fichier>.AAAA-MM-JJ, où :

- <nom du module> est le nom du module de Kaspersky Security Center ou le nom du plug-in d'administration de Kaspersky Security Center Web Console.
- <nom d'appareil> est le nom de l'appareil sur lequel le <nom du module> est exécuté.
- <numéro de révision du fichier> est le numéro du fichier journal créé pour <nom du module> exécuté sur <nom d'appareil>. Dans une journée, plusieurs fichiers journaux peuvent être créés pour le même <nom du module> et <nom d'appareil>. La taille maximale d'un fichier log est de 50 Mo. Si la taille maximale du fichier est atteinte, un nouveau fichier log est créé. Un nouveau fichier journal <numéro de révision du fichier> est incrémenté de 1.
- AAAA, MM et JJ représentent l'année, le mois et le jour de la création du log. Lorsqu'un nouveau jour commence, un nouveau fichier log est créé.

Intégration entre Kaspersky Security Center et d'autres solutions

Cette section décrit comment configurer l'accès de Kaspersky Security Center Web Console à une autre application Kaspersky, comme Kaspersky Managed Detection and Response. Cette section décrit également comment configurer l'exportation vers des systèmes SIEM.

Établissement d'une connexion en arrière-plan

Pour permettre à Kaspersky Security Center Web Console d'effectuer ses tâches en arrière-plan, vous devez établir une connexion en arrière-plan entre Kaspersky Security Center Web Console et le Serveur d'administration. Vous ne pouvez établir cette connexion que si votre compte dispose du droit **Modifier les ACL des objets** de la zone fonctionnelle **Fonctions générales : Autorisations utilisateur**.

Si vous installez le plug-in de Kaspersky Endpoint Security for Windows 12.6 ou si vous mettez à jour le plug-in de Kaspersky Endpoint Security for Windows à partir d'une version antérieure à 11.7 et qu'une connexion en arrière-plan n'est pas encore établie, une notification s'affiche vous indiquant que vous devez établir une connexion en arrière-plan. De plus, vous devrez accorder au compte de service les droits de **Fonctions générales** : zone fonctionnelle **Opérations sur le Serveur d'administration**.

Pour établir une connexion en arrière-plan :

1. Dans le menu principal, accédez à **Paramètres** → **Intégration**.
2. Dans la section **Intégration**, basculez le commutateur permettant d'établir une connexion en arrière-plan sur la position suivante : **Connexion en arrière-plan pour l'intégration Activé**.
3. Dans la section **Activer une connexion en arrière-plan** ouverte, cliquez sur le bouton **OK**.

La connexion en arrière-plan entre Kaspersky Security Center Web Console et le Serveur d'administration est établie. Le Serveur d'administration crée un compte pour la connexion en arrière-plan, et ce compte est utilisé comme compte de service pour maintenir l'interaction entre Kaspersky Security Center et une autre application ou solution de Kaspersky. Le nom de ce compte de service contient le préfixe NWCSvcUser.

Pour des raisons de sécurité, le Serveur d'administration modifie automatiquement le mot de passe du compte de service une fois tous les 30 jours. Vous ne pouvez pas supprimer le compte de service manuellement. Le Serveur d'administration supprime ce compte automatiquement lorsque vous désactivez une connexion interservices. Le Serveur d'administration crée un compte de service unique pour chaque Console d'administration et affecte tous les comptes de service au groupe de sécurité portant le nom ServiceNwcGroup. Le Serveur d'administration crée automatiquement ce groupe de sécurité lors du processus d'installation de Kaspersky Security Center. Vous ne pouvez pas supprimer ce groupe de sécurité manuellement.

Exportation des événements dans les systèmes SIEM

Cette section décrit comment configurer l'exportation des événements vers les systèmes SIEM.

Configuration de l'export d'événements vers des systèmes SIEM

Kaspersky Security Center permet la configuration par l'une des méthodes suivantes : exportation vers n'importe quel système SIEM utilisant le format Syslog, exportation vers les systèmes QRadar, Splunk, ArcSight SIEM utilisant les formats LEEF et CEF ou exportation d'événements vers les systèmes SIEM directement depuis la base de données Kaspersky Security Center. Une fois ce scénario terminé, le Serveur d'administration envoie automatiquement les événements au système SIEM.

Prérequis

Avant de lancer l'exportation de la configuration des événements vers Kaspersky Security Center :

- En savoir plus sur les méthodes d'export d'événements.
- Assurez-vous de disposer des valeurs des paramètres système.

> Vous pouvez exécuter les étapes de ce scénario dans n'importe quel ordre.

Le processus d'exportation des événements vers le système SIEM comprend les étapes suivantes :

- **Configuration du système SIEM pour recevoir les événements de Kaspersky Security Center**

  Procédure : Configuration de l'exportation d'événements dans un système SIEM

- **Sélection des événements que vous souhaitez exporter vers le système SIEM :**

  Instructions pour :

  - Console d'administration : Marquage des événements d'une application Kaspersky pour l'exportation au format Syslog, Marquage des événements généraux pour l'exportation au format Syslog
  - Kaspersky Security Center Web Console : Marquage des événements d'une application Kaspersky pour l'exportation au format Syslog, Marquage d'événements généraux pour l'exportation au format Syslog

- **Configuration de l'exportation des événements dans le système SIEM en utilisant l'une des méthodes suivantes :**

  - Avec les protocoles TCP/IP, UDP ou TLS par TCP.

    Instructions pour :

    - Console d'administration : Configuration de l'exportation des événements vers les systèmes SIEM
    - Kaspersky Security Center Web Console : configuration de l'exportation des événements vers les systèmes SIEM

  - En utilisant l'exportation d'événements directement depuis la base de données Kaspersky Security Center (Un ensemble de représentations publiques se trouve dans la base de données de Kaspersky Security Center ; la description de ces représentations publiques figurent dans le document klakdb.chm).

Résultats

Une fois l'exportation des événements vers le système SIEM configurée, si vous avez sélectionné des événements que vous souhaitez exporte, vous pouvez afficher résultats de l'exportation.

Conditions préalables

Dans le cadre de la configuration de l'exportation des événements automatique dans Kaspersky Security Center, il faut définir certains paramètres du système SIEM. Il est recommandé de préciser ces paramètres au préalable afin de se préparer pour la configuration de Kaspersky Security Center.

Pour configurer l'exportation des événements automatique vers le système SIEM, il faut connaître la valeur des paramètres suivants :

- **Adresse du serveur du système SIEM**

  Adresse du serveur hébergeant le système SIEM à utiliser. Cette valeur doit être définie dans les paramètres du système SIEM.

- **Port du serveur du système SIEM**

  Le numéro de port pour une connexion entre Kaspersky Security Center et le serveur du système SIEM. Il faut définir cette valeur dans les paramètres de Kaspersky Security Center et les paramètres du récepteur du système SIEM.

- **Protocole**

  Le protocole utilisé pour la transmission des messages depuis Kaspersky Security Center vers le système SIEM. Il faut définir cette valeur dans les paramètres de Kaspersky Security Center et les paramètres du récepteur du système SIEM.

À propos des événements de Kaspersky Security Center

Kaspersky Security Center vous permet d'obtenir des informations sur les événements survenus pendant le fonctionnement du Serveur d'administration et des applications Kaspersky installées sur les appareils administrés. Les informations relatives aux événements sont conservées dans la base de données du Serveur d'administration. Vous pouvez exporter ces informations dans des systèmes SIEM externes. L'exportation des informations relatives aux événements vers des systèmes SIEM externes permet à l'administrateur des systèmes SIEM de réagir efficacement aux événements du système de sécurité survenus sur les appareils administrés ou dans les groupes d'administration.

Types d'événement

Dans Kaspersky Security Center, il existe les types d'événements suivants :

- Événements généraux. Ces événements se produisent dans toutes les applications Kaspersky administrées. Voici un exemple d'événement général : Attaque de virus. Les événements généraux ont une syntaxe et une sémantique strictement définies. Les événements généraux sont utilisés, par exemple, dans les rapports et les tableaux de bord.

- Événements spécifiques aux applications Kaspersky administrées. Chaque application de Kaspersky administrée possède son propre ensemble d'événements.

Sources de l'événement

Les événements peuvent être générés par les applications suivantes :

- Modules de Kaspersky Security Center :
  - Serveur d'administration
  - Agent d'administration
  - Serveur MDM iOS
- Applications Kaspersky administrées

  Pour en savoir plus sur les événements générés par les applications administrées par Kaspersky, veuillez consulter la documentation de l'application correspondante.

Vous pouvez consulter la liste complète des événements qui peuvent être générés par une application sous l'onglet **Configuration des événements** dans la stratégie de l'application. Pour le Serveur d'administration, vous pouvez également consulter la liste des événements dans les propriétés du Serveur d'administration.

Niveau d'importance des événements

Chaque événement possède le niveau d'importance personnel. En fonction des conditions dans lesquelles l'événement s'est produit, il peut recevoir un niveau d'importance différent. Il existe quatre niveaux d'importance pour les événements :

- *Événement critique* : événement qui indique l'apparition d'un problème critique qui peut entraîner une perte de données, un échec ou une erreur critique.

- *Erreur de fonctionnement* : événement qui indique l'apparition d'un problème sérieux, d'une erreur ou d'un échec survenu pendant le fonctionnement de l'application ou l'exécution de la procédure.

- *Avertissement* événement qui n'est pas forcément sérieux, mais qui pourrait entraîner des problèmes à l'avenir. Le plus souvent les événements appartiennent à la catégorie Avertissement, si vous pouvez rétablir le fonctionnement de l'application par la suite, sans perte de données ou de fonctions.

- *Information* : événement qui vise à informer sur la réussite d'une opération, le fonction adéquat de l'application ou la fin d'une procédure.

On définit pour chaque événement la durée de conservation pendant laquelle l'événement peut être consulté ou modifié dans Kaspersky Security Center. Certains événements ne sont pas conservés par défaut dans la base de données du Serveur d'administration car la durée de conservation définie pour ceux-ci est égale à zéro. L'exportation vers des systèmes externes est uniquement possible pour les événements conservés dans la base de données du Serveur d'administration depuis moins d'un jour.

À propos de l'exportation des événements

L'exportation des événements peut être utilisée dans les systèmes centralisés qui traitent des questions de sécurité au niveau organisationnel et technique, qui surveillent les systèmes de sécurité et consolident les données issues de différentes solutions. Parmi ces système, il y a les systèmes SIEM qui garantissent l'analyse des alertes des systèmes de sécurité et des événements de la configuration matérielle réseau et des applications en temps réel, sans oublier les centres d'administration de la sécurité (Security Operation Center, SOC).

Les systèmes SIEM récoltent des données auprès de différentes sources, dont des réseaux des systèmes de sécurité, des serveurs, des bases de données et des applications. Ils assurent aussi la fonction de regroupement des données traitées, ce qui ne vous permet pas d'ignorer les événements critiques. De plus, ces systèmes exécutent l'analyse automatique des événements associés et des signaux d'alerte pour prévenir les administrateurs des problèmes du système de sécurité qui requièrent une solution immédiate. Les notifications peuvent s'afficher sur les barres des indicateurs ou être envoyées par des canaux tiers, par exemple, par email.

La procédure d'exportation des événements de Kaspersky Security Center vers les systèmes SIEM fait intervenir deux parties : l'expéditeur des événements (Kaspersky Security Center), et le destinataire de ceux-ci (le système SIEM). Pour que l'exportation des événements réussisse, il faut réaliser une configuration dans le système SIEM utilisé et dans Kaspersky Security Center. L'ordre des configurations n'a pas d'importance : Vous pouvez commencer par configurer l'envoi des événements à Kaspersky Security Center, puis passer à la configuration de la réception de ceux-ci du côté du système SIEM ou inversement.

Modes d'envoi des événements de Kaspersky Security Center

Il existe trois modes d'envoi des événements depuis Kaspersky Security Center vers les systèmes externes :

- Envoi des événements via le protocole Syslog à n'importe quel système SIEM.

  Le protocole Syslog permet de transmettre n'importe quel événement survenu sur le Serveur d'administration de Kaspersky Security Center et dans les applications de Kaspersky installées sur les appareils administrés. Le protocole Syslog est un protocole standard d'enregistrement de messages. Vous pouvez l'utiliser pour exporter des événements vers n'importe quel système SIEM.

  Pour cela, vous devez marquer les événements que vous souhaitez relayer au système SIEM. Vous pouvez marquer les événements dans la Console d'administration ou dans Kaspersky Security Center Web Console). Seuls les événements marqués seront relayés au système SIEM. Si vous n'avez rien coché, aucun événement ne sera relayé.

- Envoi des événements via les protocoles CEF et LEEF vers les systèmes QRadar, Splunk et ArcSight.

  Vous pouvez utiliser les protocoles CEF et LEEF pour exporter des événements généraux. Dans le cadre de l'exportation des événements via les protocoles CEF et LEEF, vous ne pouvez pas sélectionner les événements à exporter. Tous les événements généraux sont exportés. Pour convertir les événements de Kaspersky Security Center en événements au format CEF et LEEF, vous devez utiliser le fichier siem_conversion_rules.xml. Ce fichier contient la liste des attributs d'événements de Kaspersky Security Center et les attributs correspondants des événements au format CEF et LEEF. De plus, le fichier siem_conversion_rules.xml contient les règles de génération de messages correspondant aux événements. Ce fichier figure dans le kit de distribution de Kaspersky Security Center.

  A la différence du protocole Syslog, les protocoles CEF et LEEF ne sont pas universels. CEF et LEEF sont destinés aux systèmes SIEM correspondants (QRadar, Splunk et ArcSight). Par conséquent, quand vous décidez d'exporter des événements via un de ces protocoles, vous devez utiliser l'analyseur requis dans le système SIEM.

- Directement depuis la base de données de Kaspersky Security Center vers n'importe quel système SIEM.

  Ce mode d'exportation des événements peut être utilisé pour obtenir des événements directement depuis les représentations publiques de la base de données avec l'l'aide des de requêtes SQL. Les résultats de l'exécution de la requête sont enregistrés dans le fichier .xml qui peut être utilisé pour les données d'entrée du système externe. L'exportation directe depuis la base de données concerne uniquement les événements accessibles dans les représentations publiques.

Réception des événements par le système SIEM

Le système SIEM doit accepter et analyser correctement les événements en provenance de Kaspersky Security Center. Il faut pour cela configurer le système SIEM. La configuration dépend du système SIEM utilisé en particulier. Toutefois, il existe une série d'étapes communes à l'ensemble des systèmes SIEM : la configuration du récepteur et de l'analyseur.

À propos de la configuration de l'exportation d'événements dans le système SIEM

La procédure d'exportation des événements de Kaspersky Security Center vers les systèmes SIEM fait intervenir deux parties : l'expéditeur des événements (Kaspersky Security Center), et le destinataire de ceux-ci (le système SIEM). Vous devez configurer l'exportation dans votre système SIEM et dans Kaspersky Security Center.

Les configurations réalisées du système SIEM dépendent du système que vous utilisez. Quoi qu'il en soit, il faut configurer le récepteur des messages pour tous les systèmes SIEM et, le cas échéant, l'analyseur des messages afin de pouvoir décomposer les messages reçus en champs.

Configuration du récepteur des messages

Pour le système SIEM, il faut configurer le récepteur des événements envoyés par Kaspersky Security Center. En général, il faut définir les paramètres suivants dans le système SIEM :

- **Protocole de l'exportation ou type de données entrantes**

  Le protocole de transmission des messages peut être TCP/IP ou UDP. Il est nécessaire d'indiquer le même protocole que celui qui a été choisi dans Kaspersky Security Center pour envoyer les événements.

- **Port**

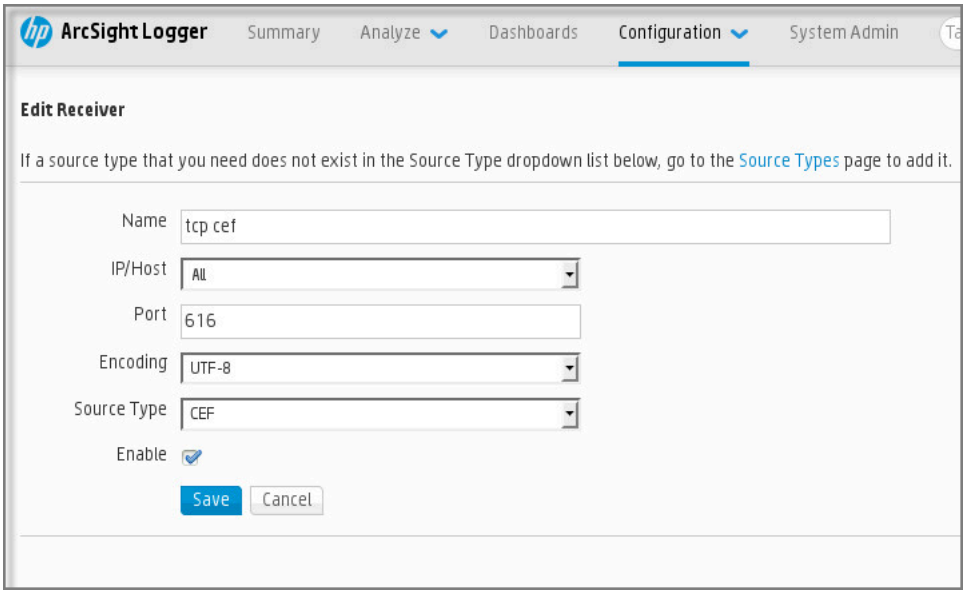
  Le numéro de port pour se connecter à Kaspersky Security Center. Il est nécessaire d'indiquer le même numéro de port que celui qui a été choisi dans Kaspersky Security Center pour envoyer les événements.

- **Protocole de transfert de messages ou type de données sortantes**

  Le protocole utilisé pour l'exportation des événements vers le système SIEM. Il peut s'agir d'un des protocoles standard : Syslog, CEF ou LEEF. Le système SIEM choisit l'analyseur d'événements qui correspond au protocole indiqué.

En fonction du système SIEM utilisé, vous devrez peut-être définir des paramètres avancés pour le récepteur de messages.

La figure ci-dessous représente la configuration d'un récepteur dans ArcSight.



Configuration du récepteur dans ArcSight

Analyseur des messages

Les événements exportés sont transmis au systèmes SIEM sous la forme de messages. Ces messages sont ensuite soumis à l'analyseur afin que les informations relatives aux événements soient transmises correctement au système SIEM. L'analyseur des messages est inséré au système SIEM il permet de décomposer le message en ses champs comme l'identifiant du message, le niveau d'importance, la description et d'autres paramètres. Le système SIEM peut ainsi traiter les événements envoyés par Kaspersky Security Center afin qu'ils soient enregistrés dans la base de données du système SIEM.

Marquage des événements pour l'export vers les systèmes SIEM au format Syslog

Une fois que l'exportation automatique des événements a été activée, il faut sélectionner les événements à exporter dans le système SIEM externe.

Vous pouvez configurer l'exportation des événements au format Syslog dans le système externe selon une des conditions suivantes :

- Marquage d'événements généraux. Si vous marquez des événements à exporter dans une stratégie, dans les paramètres d'un événement ou dans les paramètres du Serveur d'administration, le système SIEM recevra les événements marqués qui se sont produits dans toutes les applications administrées par la stratégie spécifique. Si des événements à exporter ont été choisis dans la stratégie, vous ne serez pas en mesure de les redéfinir pour une application distincte administrée par cette stratégie.

- Marquage des événements pour une application administrée. Si vous marquez les événements à exporter pour une application administrée installée sur un appareil administré, le système SIEM reçoit uniquement les événements survenus dans cette application.

À propos du marquage des événements pour l'exportation vers les systèmes SIEM au format Syslog

Une fois que l'exportation automatique des événements a été activée, il faut sélectionner les événements à exporter dans le système SIEM externe.

Vous pouvez configurer l'exportation des événements au format Syslog dans le système externe selon une des conditions suivantes :

- Marquage d'événements généraux. Si vous marquez des événements à exporter dans une stratégie, dans les paramètres d'un événement ou dans les paramètres du Serveur d'administration, le système SIEM recevra les événements marqués qui se sont produits dans toutes les applications administrées par la stratégie spécifique. Si des événements à exporter ont été choisis dans la stratégie, vous ne serez pas en mesure de les redéfinir pour une application distincte administrée par cette stratégie.

- Marquage des événements pour une application administrée. Si vous marquez les événements à exporter pour une application administrée installée sur un appareil administré, le système SIEM reçoit uniquement les événements survenus dans cette application.

Marquage des événements d'une application Kaspersky pour l'exportation au format Syslog

Si vous souhaitez exporter des événements qui se sont produits dans une application administrée spécifique installée sur les appareils administrés, marquez les événements à exporter dans la stratégie de l'application. Dans ce cas, les événements marqués sont exportés depuis tous les appareils inclus dans la zone de la stratégie.

Pour marquer les événements à exporter pour une application administrée spécifique, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Stratégies et profils**.
2. Cliquez sur la stratégie de l'application pour laquelle vous souhaitez marquer des événements.

   La fenêtre des paramètres de la stratégie s'ouvre.
3. Passez à la section **Configuration des événements**.
4. Cochez la case en regard des événements que vous souhaitez exporter dans un système SIEM.
5. Cliquez sur le bouton **Marquer pour l'exportation vers le système SIEM en utilisant Syslog**.

   Vous pouvez aussi marquer un événement pour l'exporter vers le système SIEM dans la section **Enregistrement des événements**, qui s'ouvre en cliquant sur le lien de l'événement.
6. Une coche (✓) s'affiche dans la colonne **Syslog** de l'événement ou des événements que vous avez marqués pour l'exportation vers le système SIEM.
7. Cliquez sur le bouton **Enregistrer**.

Les événements marqués de l'application administrée sont prêts à être exportés vers un système SIEM.

Vous pouvez marquer les événements à exporter vers un système SIEM pour un appareil administré spécifique. Si des événements précédemment exportés ont été marqués dans une stratégie de l'application, vous ne pourrez pas redéfinir les événements marqués pour un appareil administré.

Pour marquer les événements à exporter pour un appareil administré, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Appareils administrés**.

   La liste des appareils administrés s'affiche.
2. Cliquez sur le lien avec le nom de l'appareil requis dans la liste des appareils administrés.

   La fenêtre des propriétés de l'appareil sélectionné s'affiche.
3. Accédez à la section **Applications**.
4. Cliquez sur le lien avec le nom de l'application requise dans la liste des applications.
5. Passez à la section **Configuration des événements**.
6. Cochez la case en regard des événements que vous souhaitez exporter dans un système SIEM.

7. Cliquez sur le bouton **Marquer pour l'exportation vers le système SIEM en utilisant Syslog**.

   En outre, vous pouvez marquer un événement pour l'exporter vers le système SIEM dans la section **Enregistrement des événements**, qui s'ouvre en cliquant sur le lien de l'événement.

8. Une coche (✓) s'affiche dans la colonne **Syslog** de l'événement ou des événements que vous avez marqués pour l'exportation vers le système SIEM.

Désormais, le Serveur d'administration envoie au système SIEM les événements marqués si l'exportation vers le système SIEM est configurée.

Marquage d'événements généraux pour l'exportation au format Syslog

Vous pouvez marquer les événements généraux que le Serveur d'administration exportera vers les systèmes SIEM en utilisant le format Syslog.

Pour marquer des événements généraux à exporter vers un système SIEM, procédez comme suit :

1. Exécutez une des actions suivantes :

   - Dans le menu principal, cliquez sur l'icône des paramètres (⚙) en regard du nom du Serveur d'administration requis.
   - Dans le menu principal, accédez à **Ressources (Appareils)** → **Stratégies et profils**, puis cliquez sur le lien d'une stratégie.

2. Dans la fenêtre qui s'ouvre, sélectionnez l'onglet **Configuration des événements**.

3. Cliquez sur **Marquer pour l'exportation vers le système SIEM en utilisant Syslog**.

   En outre, vous pouvez marquer un événement pour l'exporter vers le système SIEM dans la section **Enregistrement des événements**, qui s'ouvre en cliquant sur le lien de l'événement.

4. Une coche (✓) s'affiche dans la colonne **Syslog** de l'événement ou des événements que vous avez marqués pour l'exportation vers le système SIEM.

Désormais, le Serveur d'administration envoie au système SIEM les événements marqués si l'exportation vers le système SIEM est configurée.

À propos de l'exportation des événements via les formats CEF et LEEF

Vous pouvez utiliser les formats CEF et LEEF pour exporter vers les systèmes SIEM des événements généraux, ainsi que les événements transférés par les applications Kaspersky vers le Serveur d'administration. L'ensemble des événements à exporter est défini préalablement et il est impossible de sélectionner les événements à exporter. Avant d'envoyer des événements au système SIEM (QRadar, ArcSight ou Splunk), il est nécessaire d'interpréter les événements de Kaspersky Security Center en événements au format CEF et LEEF en utilisant les règles indiquées dans le fichier siem_conversion_rules.xml.

Choisissez le format d'exportation en fonction du système SIEM que vous utilisez. Le tableau suivant reprend les systèmes SIEM et les formats d'exportation qui leur correspond.

Système SIEM	Format d'exportation
QRadar	LEEF
ArcSight	CEF
Splunk	CEF

- LEEF est un format spécial des événements pour IBM Security QRadar SIEM. QRadar peut intégrer, identifier et traiter les événements LEEF. Le protocole LEEF requiert l'utilisation du codage UTF-8. Pour en savoir plus sur le protocole LEEF, consultez la page Internet du IBM Knowledge Center.

- CEF est un standard d'administration de type " journal ouvert " qui améliore la compatibilité des informations du système de sécurité de différents appareils et applications réseau. Le protocole CEF permet d'utiliser le format général du journal des événements pour que les systèmes d'administration de l'entreprise puissent recevoir et regrouper facilement les données pour l'analyse. Le protocole CEF requiert l'utilisation du codage UTF-8.

Lors de l'exportation automatique, Kaspersky Security Center envoie les événements généraux au système SIEM. L'exportation automatique des événements dès l'activation. Cette section décrit la procédure d'activation de l'exportation des événements automatique.

Conversion d'événements au format CEF ou LEEF

Avant d'envoyer des événements au système SIEM (QRadar, ArcSight ou Splunk), il est nécessaire d'interpréter les événements de Kaspersky Security Center en événements au format CEF et LEEF en utilisant les règles indiquées dans le fichier siem_conversion_rules.xml. Ce fichier figure dans le kit de distribution de Kaspersky Security Center.

Le fichier siem_conversion_rules.xml contient les règles d'interprétation prédéfinies pour convertir les événements au format CEF et LEEF. Si vous souhaitez utiliser d'autres règles d'interprétation d'événements, vous pouvez les ajouter manuellement au fichier.

Le fichier siem_conversion_rules.xml inclut les sections `<product name="SP_QRADAR" vendor="IBM">` et `<product name="SP_QRADAR" vendor="IBM">`. La section `<product name="SP_QRADAR" vendor="IBM">` contient des règles pour générer des événements au format LEEF, qui peuvent être exportés vers le système QRadar SIEM. La section `<product name="SP_ARCSIGHT" vendor="HP">` contient des règles pour générer des événements au format CEF, qui peuvent être exportés vers le système ArcSight ou Splunk SIEM.

Chaque section contient la sous-section `<common>` dans laquelle se trouvent les attributs d'événements de Kaspersky Security Center et les attributs correspondants des événements au format LEEF. Ces attributs communs sont utilisés pour tous les types d'événements pouvant être exportés.

De plus, chaque section contient les sous-sections `<event>`. Chaque sous-section `<event>` contient des attributs supplémentaires qui s'ajoutent à ceux répertoriés dans la section `<common>`.

Vous pouvez ajouter manuellement une nouvelle règle de génération d'événements au fichier siem_conversion_rules.xml.

Pour ajouter une nouvelle règle de génération d'événements :

1. Ajoutez une nouvelle sous-section `<event>` à la section `<product name="SP_QRADAR" vendor="IBM">` ou `<product name="SP_QRADAR" vendor="IBM">`, puis indiquez les attributs d'événement supplémentaires, si nécessaire.

2. Si un événement est constitué uniquement d'attributs communs, la sous-section `<event>` sera vide.

siem_conversion_rules.xml

```
<conversion_rules>
    <product name="SP_QRADAR" vendor="IBM">
        <common> <!-- Common Kaspersky Security Center event attributes and corresponding LEEF event attributes --
>
            <param name="KLSPLG_HOST_DISP_NAME" type="STRING_T">
                <attr name="EVC_EV_DISP_HOST_NAME" type="AT_STRING" limit="255"/>
            </param>
            ...
        </common>
        <event id="GNRL_EV_VIRUS_FOUND"> <!-- Generation rule for the GNRL_EV_VIRUS_FOUND event with additional
attributes -->
            <param name="GNRL_EA_PARAM_1" type="STRING_T">
                <attr name="EVC_EV_SHA256" type="AT_STRING" limit="255"/>
            </param>
            ...
        </event>
...
</product>
    <product name="SP_ARCSIGHT" vendor="HP">
        <common> <!-- Common Kaspersky Security Center event attributes and corresponding LEEF event attributes --
>
            <param name="KLSPLG_HOST_DISP_NAME" type="STRING_T">
                <attr name="dhost" type="AT_STRING" limit="1023"/>
            </param>
            ...
        </common>
        <event id="GNRL_EV_VIRUS_FOUND">
            <param name="GNRL_EA_PARAM_1" type="STRING_T">
                <attr name="cs4" type="AT_STRING" limit="255"/>
                <attr name="cs4Label" type="AT_STRING" val="SHA256"/>
            </param>
            ...
</product>
</conversion_rules>
```

À propos de l'exportation des événements via le format Syslog

Le format Syslog permet d'exporter dans les systèmes SIEM les événements survenus sur le Serveur d'administration et dans d'autres applications de Kaspersky installées sur les appareils administrés.

Syslog est un protocole standard d'enregistrement des messages. Ce protocole permet de distinguer le logiciel qui génère les messages, le système dans lequel les messages sont enregistrés et le logiciel qui analyse les messages et génère les rapports. Chaque message reçoit un code d'appareil qui indique le type de logiciel qui a permis de créer le message et le niveau de gravité.

Le format Syslog est défini par les documents Request for Comments, RFC, publié par l'Internet Engineering Task Force (standards Internet). Le standard RFC 5424 est le standard utilisé pour exporter les événements de Kaspersky Security Center vers les systèmes externes.

Il est possible de configurer l'exportation des événements vers des systèmes externes à l'aide du format Syslog dans Kaspersky Security Center.

Le processus d'exportation comprend deux étapes :

1. Activation de l'exportation des événements automatique. Cette étape correspond à la configuration de Kaspersky Security Center de telle sorte que les événements soient envoyés au système SIEM. L'envoi des événements de Kaspersky Security Center commence dès l'activation de l'exportation automatique.

2. Sélection des événements à exporter vers le système externe. Cette étape correspond à la sélection des événements à exporter vers le système SIEM.

Configuration de Kaspersky Security Center pour l'exportation des événements vers le système SIEM

Pour exporter des événements vers le système SIEM, vous devez configurer le processus d'exportation dans Kaspersky Security Center Web Console.

Avant d'envoyer des événements au système SIEM (QRadar, ArcSight ou Splunk), il est nécessaire d'interpréter les événements de Kaspersky Security Center en événements au format CEF et LEEF en utilisant les règles indiquées dans le fichier siem_conversion_rules.xml.

Pour configurer l'exportation vers les systèmes SIEM dans Kaspersky Security Center Web Console :

1. Dans le menu principal, cliquez sur l'icône paramètres ( ) en face du nom du Serveur d'administration requis.

   La fenêtre des propriétés du Serveur d'administration s'ouvre.

2. Sous l'onglet **Général**, sélectionnez la section **Exporter vers SIEM**.

3. Cliquez sur le lien **Paramètres**.

   La section **Exporter les paramètres** s'ouvre.

4. Configurez les paramètres dans la section **Exporter les paramètres** :

- **Adresse du serveur du système SIEM**

  Adresse du serveur hébergeant le système SIEM à utiliser. Cette valeur doit être définie dans les paramètres du système SIEM.

- **Port du système SIEM**

  Le numéro de port pour une connexion entre Kaspersky Security Center et le serveur du système SIEM. Il faut définir cette valeur dans les paramètres de Kaspersky Security Center et les paramètres du récepteur du système SIEM.

- **Protocole**

Choisissez le protocole de transfert des messages dans le système SIEM. Vous avez le choix entre les protocoles TCP, UDP ou TLS par TCP.

Précisez les paramètres TLS suivants si vous sélectionnez le protocole TLS par TCP :

- **Authentification du Serveur**

  Dans le champ **Authentification du Serveur**, vous pouvez sélectionner les valeurs des **Certificats de confiance** ou des **Empreintes SHA** :

  - **Certificats de confiance**. Vous pouvez recevoir une chaîne de certificats complète (y compris le certificat racine) d'une autorité de certification de confiance et charger le fichier dans Kaspersky Security Center. Kaspersky Security Center vérifie si la chaîne de certificats du serveur du système SIEM est également signé par une autorité de certification de confiance ou non.

    Pour ajouter un certificat de confiance, cliquez sur le bouton **Rechercher le fichier des certificats CA**, puis téléchargez le certificat.

  - **Empreintes SHA**. Vous pouvez créer des empreintes digitales SHA1 de la chaîne complète de certificats du système SIEM (y compris le certificat racine) dans Kaspersky Security Center. Pour ajouter une empreinte numérique SHA1, saisissez-la dans le champ **Empreintes**, puis cliquez sur le bouton **Ajouter**.

  Le paramètre **Ajouter l'authentification du client** permet de générer un certificat pour authentifier Kaspersky Security Center. Ainsi, vous utiliserez un certificat auto-signé délivré par Kaspersky Security Center. Dans ce cas, vous pouvez utiliser à la fois un certificat de confiance et une empreinte digitale SHA pour authentifier le serveur système SIEM.

- **Ajouter le nom d'objet/le nom alternatif de l'objet**

  Le nom du sujet est un nom de domaine pour lequel le certificat est reçu. Kaspersky Security Center ne peut pas se connecter au serveur du système SIEM si le nom de domaine du serveur du système SIEM ne correspond pas au nom du sujet du certificat du serveur du système SIEM. Cependant, le serveur du système SIEM peut changer son nom de domaine si le nom a changé dans le certificat. Dans ce cas, vous pouvez indiquer des noms de sujet dans le champ **Ajouter le nom d'objet/le nom alternatif de l'objet** de sujet. Si l'un des noms du sujet spécifiés correspond au nom du sujet du certificat du système SIEM, Kaspersky Security Center valide le certificat du serveur du système SIEM.

- **Ajouter l'authentification du client**

  Pour l'authentification du client, vous pouvez insérer votre certificat ou le générer dans Kaspersky Security Center.

  - **Insérer le certificat**. Vous pouvez utiliser un certificat que vous avez reçu de n'importe quelle source, par exemple, de n'importe quelle autorité de certification de confiance. Vous devez spécifier le certificat et sa clé privée en utilisant l'un des types de certificats suivants :

    - **Certificat X.509 PEM**. Téléchargez un fichier avec un certificat dans le champ **Fichier avec certificat** et un fichier avec une clé privée dans le champ **Fichier avec clé**. Les deux fichiers ne dépendent pas l'un de l'autre, et l'ordre de chargement des fichiers est sans importance. Lorsque les deux fichiers sont téléchargés, indiquez le mot de passe pour le décodage de la clé privée dans le champ **Vérification du mot de passe ou du certificat**. Le mot de passe peut présenter une valeur vide si la clé privée n'est pas encodée.

    - **Certificat X.509 PKCS12**. Téléchargez un seul fichier qui contient un certificat et sa clé privée dans le champ **Fichier avec certificat**. Lors du téléchargement du fichier, indiquez le mot de passe pour le décodage de la clé privée dans le champ **Vérification du mot de passe ou du certificat**. Le mot de passe peut présenter une valeur vide si la clé privée n'est pas encodée.

- **Générer une clé**. Vous pouvez générer un certificat auto-signé dans Kaspersky Security Center. Par conséquent, Kaspersky Security Center stocke le certificat auto-signé généré, et vous pouvez transmettre la partie publique du certificat ou l'empreinte SHA1 au système SIEM.

- Format de données

  Vous pouvez sélectionner les formats System log, CEF ou LEEF, selon les exigences du système SIEM.

Si vous sélectionnez le format de données System log, vous devez indiquer :

- Taille maximale du message en octets

  Indiquez la taille maximale en octets d'un message transmis au système SIEM. Chaque événement entraîne l'envoi d'un message. Si la longueur réelle du message dépasse la valeur indiquée, le message est tronqué et vous risquez de perdre des données. Par défaut, la taille du message est de 2048 octets. Ce champ est accessible uniquement si vous avez choisi le format System log dans le champ **Protocole**.

5. Si vous le souhaitez, vous pouvez exporter des événements archivés à partir de la base de données du Serveur d'administration et définir la date de début à partir de laquelle vous souhaitez lancer l'exportation des événements archivés :

   a. Cliquez sur le lien **Définir la date de début de l'exportation**.

   b. Dans la section qui s'ouvre, indiquez la date de début dans le champ **Date de début de l'exportation des événements système**.

   c. Cliquez sur le bouton **OK**.

6. Basculez l'option en position **Exporter automatiquement les événements dans la base du système SIEM Activé**.

7. Pour vérifier que la connexion au système SIEM a été configurée, cliquez sur le bouton **Analyser la connexion**.

   La connexion avec le serveur système SIEM est établie et un événement de test est envoyé. L'état de la connexion s'affiche.

   La vérification est effectuée uniquement pour les protocoles TCP/IP et TLS sur TCP.

8. Cliquez sur le bouton **Enregistrer**.

L'exportation vers le système SIEM est configurée.

Exportation des événements directement depuis la base de données

Vous pouvez extraire les événements directement de la base de données de Kaspersky Security Center sans passer par l'interface de Kaspersky Security Center. Il est possible de créer des requêtes directement pour des représentations publiques et d'extraire de celles-ci les données relatives aux événements ou de créer vos propres représentations sur la base des représentations publiques existantes et de les sonder pour obtenir les données requises.

Représentations publiques

Pour vous simplifier la tâche, la base de données de Kaspersky Security Center contient une sélection de représentations publiques. Le document klakdb.chm contient une description des représentations publiques.

La représentation publique v_akpub_ev_event contient un ensemble des champs correspondant aux paramètres des événements dans la base de données. Le document klakdb.chm contient aussi les informations relatives aux représentations publiques en rapport avec d'autres objets de Kaspersky Security Center, par exemple, les appareils, les applications, les utilisateurs. Vous pouvez utiliser ces informations lors de la création des requêtes.

Cette section fournit les instructions relatives à l'exécution d'une requête SQL à l'aide de l'utilitaire klsql2 ainsi qu'un exemple d'une telle requête.

Vous pouvez également utiliser n'importe quelles autres applications de gestion de bases de données pour créer des requêtes SQL et des représentations de bases de données. Les informations sur l'affichage des paramètres de connexion à la base de données de Kaspersky Security Center, comme le nom d'instance et le nom de la base de données figurent dans la section correspondante.

Exécution d'une requête SQL à l'aide de l'utilitaire klsql2

Cette section fournit des instructions sur le téléchargement et l'utilisation de l'utilitaire klsql2 ainsi que sur l'exécution d'une requête SQL à l'aide de cet utilitaire.

Pour utiliser l'utilitaire klsql2 :

1. Localisez l'utilitaire klsql2 dans le dossier d'installation de Kaspersky Security Center. Chemin d'installation par défaut est <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center. N'utilisez pas les versions de l'utilitaire klsql2 destinées aux anciennes versions de Kaspersky Security Center.

2. Créez un fichier avec l'extension .sql dans n'importe quel éditeur de texte et placez le fichier dans le même dossier que l'utilitaire.

3. Dans le fichier .sql créé, entrez la requête SQL souhaitée, puis enregistrez le fichier.

4. Sur l'appareil sur lequel le Serveur d'administration de Kaspersky Security Center est installé, saisissez la commande suivante dans la ligne de commande pour exécuter la requête SQL depuis le fichier .sql et enregistrer les résultats dans le fichier result.xml :

   ```
   klsql2 -i src.sql -u <nom d'utilisateur> -p <mot de passe> -o result.xml
   ```

   où `<nom d'utilisateur>` et `<mot de passe>` sont les identifiants du compte qui a accès à la base de données.

5. Si nécessaire, saisissez le login et le mot de passe du compte qui a accès à la base de données.

6. Ouvrez les fichiers result.xml obtenus et consultez les résultats de l'exécution de la requête SQL.

Vous pouvez modifier le fichier .sql et créer dans celui-ci, n'importe quelle requête SQL de représentation publique. Ensuite, lancez la requête SQL et l'enregistrement des résultats dans un fichier via la ligne de commande.

Exemple de requête SQL créée à l'aide de l'utilitaire klsql2

Cette section fournit un exemple de requête SQL exécutée à l'aide de l'utilitaire klsql2.

Les exemples suivants montrent comment récupérer la liste des événements survenus sur les appareils des utilisateurs au cours des sept derniers jours et la trier selon l'heure de l'événement. Les événements les plus récents sont affichés en premier.

Exemple pour Microsoft SQL Server :

```
SELECT
  /* identificateur d'événement */
  e.nId,

  /* heure de l'événement */
  e.tmRiseTime,

  /* nom interne du type d'événement */
  e.strEventType,

  /* nom de l'événement affiché */
  e.wstrEventTypeDisplayName,

  /* description de l'événement affichée */
  e.wstrDescription,

  /* nom du groupe où se trouve l'appareil */
  e.wstrGroupName,

  /* nom de l'appareil affiché sur lequel l'événement s'est produit */
  h.wstrDisplayName,
  CAST(((h.nIp / 16777216) & 255) AS varchar(4)) + '.' +
  CAST(((h.nIp / 65536) & 255) AS varchar(4)) + '.' +
  CAST(((h.nIp / 256) & 255) AS varchar(4)) + '.' +

  /* adresse IP de l'appareil sur lequel l'événement s'est produit */
  CAST(((h.nIp) & 255) AS varchar(4)) as strIp
FROM v_akpub_ev_event e
  INNER JOIN v_akpub_host h ON h.nId=e.nHostId
WHERE e.tmRiseTime>=DATEADD(Day, -7, GETUTCDATE())
ORDER BY e.tmRiseTime DESC
```

Exemple pour PostgreSQL :

```
SELECT
  /* identificateur d'événement */
  "e"."nId",

  /* heure de l'événement */
  "e"."tmRiseTime",

  /* nom interne du type d'événement */
  "e"."strEventType",

  /* nom de l'événement affiché */
  "e"."wstrEventTypeDisplayName",

  /* description de l'événement affichée */
  "e"."wstrDescription",

  /* description de l'événement affichée */
  "e"."wstrGroupName",

  /* nom de l'appareil affiché sur lequel l'événement s'est produit */
  "h"."wstrDisplayName",
  (
    CAST(("h"."nIp" / 16777216 )& 255 ) AS VARCHAR(4))  || '.'  ||
    CAST(("h"."nIp" / 65536 )& 255 ) AS VARCHAR(4))  || '.'  ||
    CAST(("h"."nIp" / 256 )& 255 ) AS VARCHAR(4))  || '.'  ||

    /* adresse IP de l'appareil sur lequel l'événement s'est produit */
    CAST(("h"."nIp" )& 255 ) AS VARCHAR(4))
  )  AS "strIp"
FROM "v_akpub_ev_event"  AS "e"
  INNER JOIN  "v_akpub_host"  AS "h" ON "h"."nId" = "e"."nHostId"
WHERE "e"."tmRiseTime" >= NOW() AT TIME ZONE 'utc'  + make_interval(days => CAST(-7  AS INT))
ORDER BY "e"."tmRiseTime" DESC ;
```

Exemple pour MySQL ou MariaDB :

```
SELECT

  /* identificateur d'événement */
  `e`.`nId`,

  /* heure de l'événement */
  `e`.`tmRiseTime`,

  /* nom interne du type d'événement */
  `e`.`strEventType`,

  /* nom de l'événement affiché */
  `e`.`wstrEventTypeDisplayName`,

  /* description de l'événement affichée */
  `e`.`wstrDescription`,

  /* nom du groupe d'appareils */
  `e`.`wstrGroupName`,

  /* nom de l'appareil affiché sur lequel l'événement s'est produit */
  `h`.`wstrDisplayName`,
  CONCAT(
    LEFT(CAST(((`h`.`nIp`  DIV  1677721) & 255) AS CHAR), 4), '.',
    LEFT(CAST(((`h`.`nIp`  DIV  65536) & 255) AS CHAR), 4), '.',
    LEFT(CAST(((`h`.`nIp`  DIV  256) & 255) AS CHAR), 4), '.',

    /* adresse IP de l'appareil sur lequel l'événement s'est produit */
    LEFT(CAST(((`h`.`nIp`) & 255) AS CHAR), 4)
  )  AS `strIp`
FROM `v_akpub_ev_event`  AS `e`
  INNER JOIN  `v_akpub_host`  AS `h` ON `h`.`nId` = `e`.`nHostId`
WHERE `e`.`tmRiseTime` >= ADDDATE( UTC_TIMESTAMP( ) , INTERVAL -7  DAY)
ORDER BY `e`.`tmRiseTime` DESC ;
```

Consultation du nom de la base de données de Kaspersky Security Center

Pour accéder à la base de données Kaspersky Security Center à l'aide des outils d'administration de base de données SQL Server, MySQL ou MariaDB, vous devez connaître le nom de la base de données, afin de pouvoir vous y connecter sans l'éditeur de scripts SQL.

Pour consulter le nom de la base de données de Kaspersky Security Center, procédez comme suit :

1. Dans le menu principal, cliquez sur l'icône des paramètres ( ) en regard du nom du Serveur d'administration requis.

   La fenêtre des propriétés du Serveur d'administration s'ouvre.

2. Sous l'onglet **Général**, sélectionnez la section **Détails sur la base de données utilisée**.

Le nom de la base de données est indiqué dans le champ **Nom de la base de données**. Utilisez ce nom de base de données pour vous connecter à la base de données et pour l'invoquer dans vos requêtes SQL.

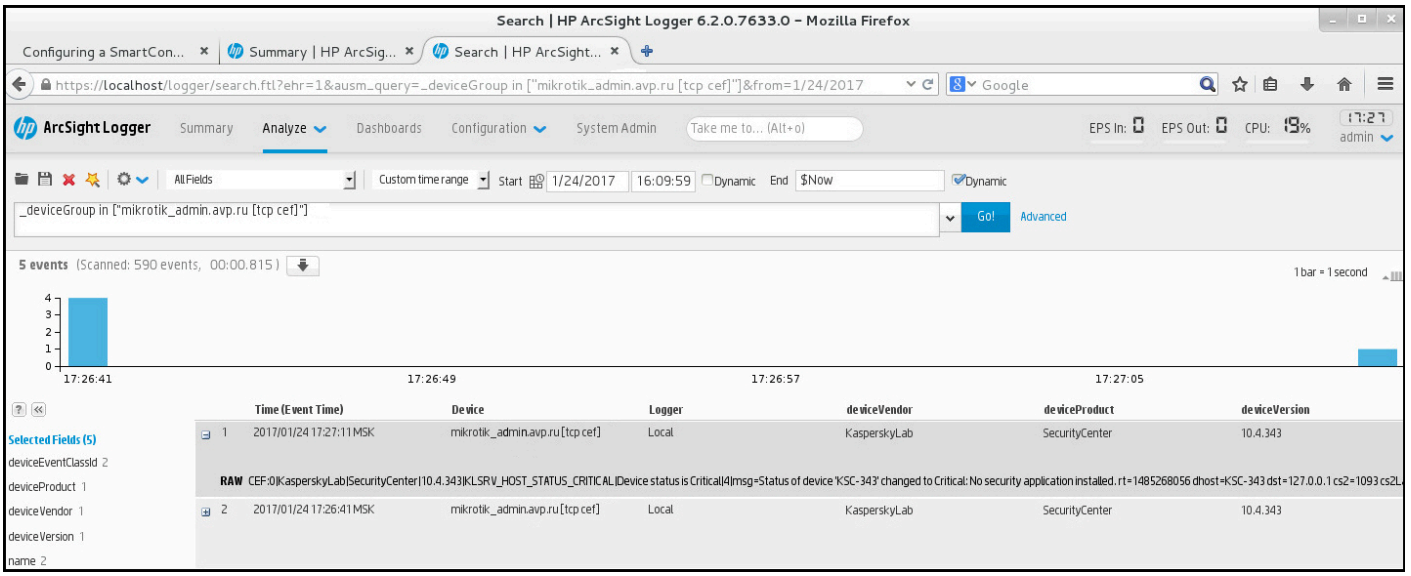
Consultation des résultats de l'exportation

Vous pouvez voir si l'exportation a réussi. Pour cela, vérifiez si le système SIEM a reçu les messages contenant les événements à exporter.

Si les événements envoyés par Kaspersky Security Center ont été reçus et correctement interprétés par le système SIEM, cela signifie que la configuration des deux côtés est correcte. Dans le cas contraire, vérifiez et le cas échéant, modifiez les paramètres de Kaspersky Security Center et du système SIEM.

Vous trouverez ci-après un exemple d'événements exportés dans le système ArcSight. Par exemple, le premier événement est un événement critique du Serveur d'administration : " *État de l'appareil Critique* ".

L'affichage des événements exportés varie en fonction du système SIEM utilisé.



Exemple d'événements

Utilisation de Kaspersky Security Center Web Console dans le Cloud

Cette section fournit des informations sur les fonctionnalités de Kaspersky Security Center Web Console relatives au déploiement et à la maintenance de Kaspersky Security Center dans les environnements cloud comme Amazon Web Services, Microsoft Azure ou Google Cloud.

Pour travailler dans un environnement Cloud, vous avez besoin d'une licence spéciale. Si vous ne disposez pas d'une telle licence, les éléments d'interface liés aux appareils Cloud ne sont pas affichés.

Configuration pour une utilisation dans le Cloud dans Kaspersky Security Center Web Console

Pour configurer Kaspersky Security Center à l'aide de l'Assistant de configuration pour une utilisation dans le Cloud, vous devez disposer des éléments suivants :

- Les informations d'identification particulières pour un environnement cloud :
  - Un rôle IAM qui a reçu l'autorisation de sonder le segment dans le Cloud ou un compte utilisateur IAM qui a reçu l'autorisation de sonder le segment dans le Cloud (pour une utilisation avec Amazon Web Services)
  - Un ID de l'application Azure, un mot de passe et un abonnement (pour une utilisation avec Microsoft Azure)
  - Adresse email du client Google, ID du projet et clé privée (pour une utilisation avec Google Cloud)
- Paquets d'installation :
  - Agent d'administration pour Windows
  - Agent d'administration pour Linux
  - Kaspersky Endpoint Security for Linux
- Plug-in Internet pour Kaspersky Endpoint Security for Linux
- Au moins un des éléments suivants :
  - Paquet d'installation et plug-in Internet pour Kaspersky Endpoint Security for Windows (recommandé)
  - Paquet d'installation et plug-in Internet pour Kaspersky Security for Windows Server

L'Assistant de configuration pour une utilisation dans le Cloud démarre automatiquement à la première connexion via la Console d'administration au Serveur d'administration si vous déployez Kaspersky Security Center depuis une image AMI prête. Vous pouvez aussi lancer l'Assistant manuellement à tout moment.

Pour lancer l'Assistant de configuration pour une utilisation dans le Cloud manuellement, procédez comme suit :

Dans le menu principal, accédez à **Découverte et déploiement** → **Déploiement et attribution** → **Configurer l'environnement cloud**.

L'Assistant démarre.

Une session de travail moyenne pour la configuration d'un environnement cloud dure environ 15 minutes.

Étape 1. Vérification des plug-ins et des paquets d'installation requis

Cette étape ne s'affiche pas si vous disposez de tous les plug-ins Internet et paquets d'installation requis répertoriés ci-dessous.

Pour configurer un environnement cloud, vous devez disposer des modules suivants :

- Paquets d'installation :
  - Agent d'administration pour Windows
  - Agent d'administration pour Linux
  - Kaspersky Endpoint Security for Linux
- Plug-in Internet pour Kaspersky Endpoint Security for Linux
- Au moins un des éléments suivants :
  - Paquet d'installation et plug-in Internet pour Kaspersky Endpoint Security for Windows (recommandé)
  - Paquet d'installation et plug-in Internet pour Kaspersky Security for Windows Server

    Nous vous recommandons d'utiliser Kaspersky Endpoint Security for Windows au lieu de Kaspersky Security for Windows Server.

Kaspersky Security Center détecte automatiquement les modules dont vous disposez déjà et répertorie uniquement ceux qui manquent. Téléchargez les modules répertoriés en cliquant sur le bouton **Sélectionner les applications à télécharger**, puis en sélectionnant les plug-ins et les paquets d'installation requis. Après avoir téléchargé un module, vous pouvez utiliser le bouton **Actualiser** pour mettre à jour la liste des modules manquants.

Étape 2. Licence de l'application

Cette étape ne s'affiche que si vous utilisez une image AMI selon le principe BYOL et que vous n'avez pas activé l'application avec une licence Kaspersky Security for Virtualization ou une licence Kaspersky Hybrid Cloud Security.

Indiquez la clé de licence et cliquez sur **Suivant** pour continuer.

La clé de licence est ajoutée au stockage du Serveur d'administration.

Si vous exécutez de nouveau l'Assistant, cette étape ne s'affiche pas.

Étape 3. Sélection de l'environnement cloud et de l'autorisation

Cette section présente les fonctionnalités applicables uniquement à Kaspersky Security Center 12.1 ou version ultérieure.

Définissez les paramètres suivants :

- **Environnement cloud**

  Sélectionnez le Cloud dans lequel vous déployez Kaspersky Security Center : AWS, Azure ou Google Cloud.

  Si vous prévoyez de travailler avec plusieurs environnements cloud, sélectionnez un environnement, puis exécutez de nouveau l'Assistant.

- **Nom de la connexion**

  Saisissez un nom pour la connexion. Le nom ne peut pas contenir plus de 256 caractères. Seuls les caractères Unicode sont admis.

  Ce nom servira aussi pour le groupe d'administration des appareils dans le cloud.

  Si vous prévoyez de travailler avec plusieurs environnements Cloud, vous pourriez inclure le nom de l'environnement dans le nom de la connexion, par exemple, " Segment Azure ", " Segment AWS " ou " Segment Google ".

Entrez vos informations d'identification pour recevoir l'autorisation dans l'environnement cloud que vous avez indiqué.

AWS

Si vous avez sélectionné AWS comme le type de segment dans le Cloud, vous avez besoin d'un rôle IAM ou d'une clé d'accès AWS IAM pour sonder davantage le segment dans le Cloud.

- **Rôle AWS IAM attribué à une instance EC2**

  Sélectionnez cette option si vous disposez d'un rôle IAM avec les droits requis pour le Serveur d'administration.

- **Utilisateur AWS IAM**

  Sélectionnez cette option si vous disposez d'une clé d'accès AWS IAM. Entrez vos données clés :

  - **ID de la clé d'accès**

    L'ID de clé d'accès IAM est une suite de caractères alphanumériques. Vous avez reçu l'ID de clé lors de la création du compte utilisateur IAM.

    Ce champ est accessible si vous avez opté pour l'autorisation à l'aide d'une clé d'accès AWS IAM et non pas d'un rôle IAM.

  - **Clé secrète**

    La clé secrète que vous avez reçue avec l'ID de clé d'accès quand vous avez créé le compte utilisateur IAM.

    Les caractères de la clé secrète s'affichent sous la forme d'astérisques. Après que vous avez commencé à saisir la clé secrète, le bouton **Afficher** apparaît. Cliquez sur ce bouton pendant le temps qu'il vous faut pour consulter les caractères saisis.

    Ce champ est accessible si vous avez opté pour l'autorisation à l'aide d'une clé d'accès AWS IAM et non pas d'un rôle IAM.

    Pour afficher les caractères que vous avez entrés, cliquez sur le bouton **Afficher** et maintenez-le enfoncé.

Azure

Si vous avez choisi Azure comme le type de segment dans le Cloud, configurez les paramètres suivants de la connexion qui interviendra à l'avenir dans le sondage des segments dans le Cloud :

- **ID de l'application Azure**

  Vous avez créé cet identifiant de l'application sur le portail Azure.

  Vous pouvez fournir un identifiant de l'application Azure pour le sondage et d'autres fins. Si vous souhaitez sonder un autre segment Azure, il faut d'abord supprimer la connexion Azure existante.

- **ID de l'abonnement Azure**

  Vous avez créé l'abonnement sur le portail Azure.

- **Mot de passe de l'application Azure**

  Vous avez obtenu le mot de passe de l'identifiant de l'application quand vous avez créé celui-ci.

  Les caractères de la mot de passe s'affichent sous la forme d'astérisques. Après que vous avez commencé à saisir le mot de passe, le bouton **Afficher** apparaît. Maintenez ce bouton enfoncé pour voir les caractères saisis.

  Pour afficher les caractères que vous avez entrés, cliquez sur le bouton **Afficher** et maintenez-le enfoncé.

- **Nom du compte du stockage Azure**

  Vous avez créé le nom du Compte du stockage Azure pour utiliser Kaspersky Security Center.

- **Clé d'accès au stockage Azure**

  Vous avez reçu un mot de passe (une clé) lorsque vous avez créé le compte du stockage Azure pour utiliser Kaspersky Security Center.

  La clé est disponible dans la section « Aperçu du compte du stockage Azure », dans la sous-section « Clés ».

  Pour afficher les caractères que vous avez entrés, cliquez sur le bouton **Afficher** et maintenez-le enfoncé.

Google Cloud

Si vous avez choisi Google Cloud comme le type de segment dans le Cloud, configurez les paramètres suivants de la connexion qui interviendra à l'avenir dans le sondage segments dans le Cloud :

- **Adresse email du client**

  L'email client est l'adresse email que vous avez utilisée pour enregistrer votre projet sur Google Cloud.

- **Identifiant du projet**

  L'identifiant du projet est l'identifiant que vous avez reçu lors de l'enregistrement de votre projet sur Google Cloud.

- **Clé privée**

  La clé privée est la séquence de caractères que vous avez reçue comme clé privée lors de l'enregistrement de votre projet sur Google Cloud. Envisagez de copier et coller cette séquence pour éviter les erreurs.

  Pour afficher les caractères que vous avez entrés, cliquez sur le bouton **Afficher** et maintenez-le enfoncé.

La connexion que vous avez définie est enregistrée dans les paramètres de l'application.

L'Assistant de configuration pour une utilisation dans le Cloud vous permet de définir un seul segment. Par la suite, vous pouvez indiquer d'autres connexions pour l'administration d'autres segments dans le Cloud.

Cliquez sur **Suivant** pour continuer.

Étape 4. Sondage des segments, configuration de la synchronisation avec le Cloud et sélection des actions ultérieures

Cette étape marque le début du sondage des segments dans le Cloud et la création automatique d'un groupe d'administration spécial pour les appareils Cloud. Les appareils trouvés lors du sondage sont placés dans ce groupe. C'est ici aussi que vous allez programmer le sondage du segment dans le cloud (par défaut, toutes les 5 minutes ; vous pouvez modifier ce paramètre ultérieurement).

La règle de déplacement automatique **Synchronisation avec Cloud** est créée à cette étape. À chaque analyse ultérieur du réseau Cloud, les appareils virtuels détectés sont déplacés dans le sous-groupe correspondant au sein du groupe **Appareils administrés\Cloud**.

Configurez les paramètres suivants :

- **Synchroniser les groupes d'administration avec la structure cloud**

  Quand cette option est activée, le groupe **Cloud** est créé automatiquement dans le groupe **Appareils administrés** et la Recherche d'appareils dans le Cloud démarre. Les machines virtuelles détectées à chaque analyse du réseau Cloud sont déplacées dans le groupe Cloud. La structure des sous-groupes d'administration au sein de ce groupe correspond à la structure de votre segment dans le Cloud (dans AWS, les zones d'accessibilité et les groupes de déplacement ne sont pas représentés dans la structure dans Azure, les sous-réseaux ne sont pas représentés dans la structure). Les appareils qui ne sont pas identifiés en tant qu'instances dans le Cloud se trouvent dans le groupe **Appareils non définis**. Cette structure de groupes permet d'installer les applications antivirus sur les instances à l'aide des tâches d'installation de groupe et de configurer de différentes stratégies pour différents groupes.

  Quand l'option est désactivée, le groupe **Cloud** est aussi créé et une recherche d'appareil est lancée toutefois, les sous-groupes qui correspondent à la structure du segment dans le Cloud ne sont pas créés au sein du groupe. Toutes les instances détectées se trouvent dans le groupe d'administration **Cloud** et s'affichent dans une liste commune. Si lors de l'utilisation de Kaspersky Security Center, vous devez effectuer une synchronisation, vous pourrez modifier les propriétés de la règle **Synchronisation avec Cloud** et la forcer. Le forcement de la règle reconstruit la structure des groupes à l'intérieur du groupe Cloud de manière à ce qu'elle corresponde à la structure de votre segment dans le Cloud.

  Cette option est Inactif par défaut.

- **Déployer la protection**

  Quand cette option est sélectionnée, l'Assistant crée une tâche d'installation d'applications de sécurité sur les instances. La fin de l'assistant est automatiquement suivie du lancement de l'assistant de déploiement de la protection sur vos segments dans le Cloud, et vous pouvez installer sur celles-ci l'Agent d'administration et les applications de sécurité.

  Kaspersky Security Center peut réaliser le déploiement à l'aide de ses propres outils. Si vous n'avez pas les permissions pour installer les applications sur les instances EC2 ou les machines virtuelles Azure, vous pouvez configurer la tâche **Installation à distance** manuellement et précisez un compte disposant des permissions requises. Dans ce cas, la tâche Installation à distance ne fonctionnera pas pour les appareils détectés par l'API d'AWS ou Azure. Cette tâche fonctionne uniquement pour les appareils détectés à l'aide du sondage Active Directory, du sondage des domaines Windows ou du sondage des plages IP.

  Si cette option n'est pas sélectionnée, l'Assistant de déploiement de la protection ne démarre pas et la création des tâches d'installation des applications de sécurité sur les instances n'a pas lieu. Vous pouvez réaliser ces deux opérations manuellement plus tard.

Si vous sélectionnez l'option Déployer la protection, la section **Redémarrage des appareils** devient accessible. Dans cette section, vous devez choisir ce qu'il faut faire lorsque le système d'exploitation d'un appareil cible doit être redémarré. Sélectionnez s'il faut ou non redémarrer l'appareil si le système d'exploitation doit être redémarré pendant l'installation des applications :

- **Ne pas redémarrer**

  Si cette option a été sélectionnée, l'appareil ne sera pas redémarré après l'installation de l'application de sécurité.

- **Redémarrer**

  Si cette option a été sélectionnée, l'appareil sera redémarré après l'installation de l'application de sécurité.

Cliquez sur **Suivant** pour continuer.

Pour Google Cloud, vous ne pouvez effectuer de déploiement qu'avec les outils natifs de Kaspersky Security Center. Si vous avez sélectionné Google Cloud, l'option **Déployer la protection** n'est pas disponible.

Étape 5. Sélection de l'application pour laquelle créer une stratégie et des tâches

Cette étape s'affiche uniquement si vous disposez de paquets d'installation et de plug-ins pour Kaspersky Endpoint Security for Windows et Kaspersky Security for Windows Server. Si vous disposez d'un plug-in et d'un paquet d'installation pour une seule de ces applications, cette étape est ignorée et Kaspersky Security Center crée une stratégie et des tâches pour l'application existante.

Sélectionnez une application pour laquelle vous souhaitez créer une stratégie et des tâches :

- Kaspersky Endpoint Security for Windows
- Kaspersky Security for Windows Server

Étape 6. Configuration de Kaspersky Security Network pour Kaspersky Security Center

Indiquez les paramètres du transfert des informations sur le fonctionnement de Kaspersky Security Center dans la base de connaissances de Kaspersky Security Network (KSN). Sélectionnez l'une des options ci-dessous :

- **J'accepte les termes du Kaspersky Security Network**

  Kaspersky Security Center et les applications administrées installées sur les appareils client transfèrent automatiquement les détails de leurs opérations à Kaspersky Security Network. La coopération avec Kaspersky Security Network garantit une mise à jour plus rapide des bases de données sur les virus et les menaces, ce qui améliore la vitesse de réaction face aux menaces naissantes.

- **Je refuse les termes du Kaspersky Security Network**

  Kaspersky Security Center et les applications administrées ne fourniront aucune information à Kaspersky Security Network.

  Si vous sélectionnez cette option, l'utilisation de Kaspersky Security Network sera désactivée.

Kaspersky recommande la participation au Kaspersky Security Network.

Les accords KSN pour les applications administrées peuvent également être affichés. Si vous acceptez d'utiliser Kaspersky Security Network, l'application administrée enverra des données à Kaspersky. Si vous n'acceptez pas de participer à Kaspersky Security Network, l'application administrée n'enverra aucune donnée à Kaspersky. (Vous pouvez modifier ce paramètre ultérieurement dans la stratégie de l'application.)

Cliquez sur **Suivant** pour continuer.

Étape 7. Création d'une configuration initiale de protection

Vous pouvez consulter une liste de stratégies et de tâches créées.

Attendez la fin de la création des stratégies et des tâches, puis cliquez sur **Suivant** pour continuer. Sur la dernière page de l'assistant, cliquez sur le bouton **Terminer** pour quitter.

Sondage de segments du réseau via Kaspersky Security Center Web Console

Le Serveur d'administration reçoit les informations sur la structure du réseau (et sur les appareils qui en font partie) au cours des sondages réguliers des segments dans le Cloud à l'aide des outils de l'API d'AWS, de l'API d'Azure et de l'API de Google. Sur la base des informations obtenues, Kaspersky Security Center met à jour le contenu des dossiers Appareils non définis et Appareils administrés. Si vous avez configuré le déplacement automatique des appareils dans les groupes d'administration, les appareils détectés sont inclus dans les groupes d'administration.

Pour que le Serveur d'administration puisse sonder les segments dans le Cloud, vous devez posséder les privilèges correspondants fournis avec un rôle IAM ou le compte utilisateur IAM (dans AWS) ou avec l'ID de l'application et le mot de passe (dans Azure) ou avec un email client de Google, un identifiant de projet Google et une clé privée (dans Google Cloud).

Vous pouvez ajouter et supprimer des connexions, ainsi que configurer une programmation du sondage pour chaque segment dans le Cloud.

Ajout de connexions pour le sondage des segments dans le Cloud

Pour ajouter une connexion pour le sondage des segments dans le Cloud à la liste des connexions disponibles, procédez comme suit :

1. Dans le menu principal, accédez à **Découverte et déploiement** → **Découverte** → **Cloud**.
2. Dans la fenêtre qui s'ouvre, cliquez sur **Propriétés**.
3. Dans la fenêtre **Paramètres** qui s'ouvre, cliquez sur **Ajouter**.

   La fenêtre **Paramètres du segment dans le cloud** s'ouvre.
4. Définissez le nom de l'environnement Cloud de la connexion qui interviendra à l'avenir dans le sondage des segments dans le Cloud :

   - Environnement cloud

     Sélectionnez le Cloud dans lequel vous déployez Kaspersky Security Center : AWS, Azure ou Google Cloud.

     Si vous prévoyez de travailler avec plusieurs environnements cloud, sélectionnez un environnement, puis exécutez de nouveau l'Assistant.

   - Nom de la connexion

     Saisissez un nom pour la connexion. Le nom ne peut pas contenir plus de 256 caractères. Seuls les caractères Unicode sont admis.

     Ce nom servira aussi pour le groupe d'administration des appareils dans le cloud.

     Si vous prévoyez de travailler avec plusieurs environnements Cloud, vous pourriez inclure le nom de l'environnement dans le nom de la connexion, par exemple, " Segment Azure ", " Segment AWS " ou " Segment Google ".

5. Entrez vos informations d'identification pour recevoir l'autorisation dans l'environnement cloud que vous avez indiqué.

- Si vous avez sélectionné AWS, spécifiez les paramètres suivants :

  - **Utiliser le rôle IAM AWS**

    Sélectionnez cette option, si vous avez déjà créé un rôle IAM pour l'utilisation du Serveur d'administration avec les services AWS.

  - **Identifiants du compte utilisateur IAM AWS**

    Choisissez cette option, si vous avez un compte utilisateur IAM doté des privilèges requis et si vous pouvez saisir l'identifiant de la clé et la clé secrète.

    Si vous avez indiqué que vous avez Identifiants du compte utilisateur IAM AWS, définissez les éléments suivants :

    - **ID de la clé d'accès**

      L'ID de clé d'accès IAM est une suite de caractères alphanumériques. Vous avez reçu l'ID de clé lors de la création du compte utilisateur IAM.

      Ce champ est accessible si vous avez opté pour l'autorisation à l'aide d'une clé d'accès AWS IAM et non pas d'un rôle IAM.

    - **Clé secrète**

      La clé secrète que vous avez reçue avec l'ID de clé d'accès quand vous avez créé le compte utilisateur IAM.

      Les caractères de la clé secrète s'affichent sous la forme d'astérisques. Après que vous avez commencé à saisir la clé secrète, le bouton **Afficher** apparaît. Cliquez sur ce bouton pendant le temps qu'il vous faut pour consulter les caractères saisis.

      Ce champ est accessible si vous avez opté pour l'autorisation à l'aide d'une clé d'accès AWS IAM et non pas d'un rôle IAM.

    Pour afficher les caractères que vous avez entrés, cliquez sur le bouton **Afficher** et maintenez-le enfoncé.

- Si vous avez sélectionné Azure, spécifiez les paramètres suivants :

  - **ID de l'application Azure**

    Vous avez créé cet identifiant de l'application sur le portail Azure.

    Vous pouvez fournir un identifiant de l'application Azure pour le sondage et d'autres fins. Si vous souhaitez sonder un autre segment Azure, il faut d'abord supprimer la connexion Azure existante.

  - **ID de l'abonnement Azure**

    Vous avez créé l'abonnement sur le portail Azure.

- **Mot de passe de l'application Azure**

  Vous avez obtenu le mot de passe de l'identifiant de l'application quand vous avez créé celui-ci.

  Les caractères de la mot de passe s'affichent sous la forme d'astérisques. Après que vous avez commencé à saisir le mot de passe, le bouton **Afficher** apparaît. Maintenez ce bouton enfoncé pour voir les caractères saisis.

  Pour afficher les caractères que vous avez entrés, cliquez sur le bouton **Afficher** et maintenez-le enfoncé.

- **Nom du compte du stockage Azure**

  Vous avez créé le nom du Compte du stockage Azure pour utiliser Kaspersky Security Center.

- **Clé d'accès du stockage Azure**

  Vous avez reçu un mot de passe (une clé) lorsque vous avez créé le compte du stockage Azure pour utiliser Kaspersky Security Center.

  La clé est disponible dans la section « Aperçu du compte du stockage Azure », dans la sous-section « Clés ».

  Pour afficher les caractères que vous avez entrés, cliquez sur le bouton **Afficher** et maintenez-le enfoncé.

Si vous avez sélectionné Google Cloud, spécifiez les paramètres suivants :

- **Adresse email du client**

  L'email client est l'adresse email que vous avez utilisée pour enregistrer votre projet sur Google Cloud.

- **Identifiant du projet**

  L'identifiant du projet est l'identifiant que vous avez reçu lors de l'enregistrement de votre projet sur Google Cloud.

- **Clé privée**

  La clé privée est la séquence de caractères que vous avez reçue comme clé privée lors de l'enregistrement de votre projet sur Google Cloud. Envisagez de copier et coller cette séquence pour éviter les erreurs.

  Pour afficher les caractères que vous avez entrés, cliquez sur le bouton **Afficher** et maintenez-le enfoncé.

6. Si vous le souhaitez, cliquez sur **Planifier le sondage** et modifiez les paramètres par défaut.

La connexion est enregistrée dans les paramètres de l'application.

Après le premier sondage du nouveau segment dans le Cloud, le sous-groupe qui correspond à ce segment apparaît dans le groupe d'administration **Appareils administrés\Cloud**.

Si vous utilisez des identifiants incorrects, aucune instance ne sera détectée lors du sondage des segments dans le Cloud et le nouveau sous-groupe n'apparaîtra pas dans le groupe d'administration **Appareils administrés\Cloud**.

Suppression d'une connexion pour le sondage des segments dans le Cloud

Si vous n'avez plus besoin de sonder un segment dans le Cloud en particulier, vous pouvez supprimer la connexion qui correspond à celui-ci dans la liste des connexions disponibles. Vous pouvez également supprimer la connexion si, par exemple, les droits de sondage du segment dans le Cloud ont été transmis à un autre utilisateur utilisant d'autres informations d'identification.

Pour supprimer une connexion, procédez comme suit :

1. Dans le menu principal, accédez à **Découverte et déploiement → Découverte → Cloud**.
2. Dans la fenêtre qui s'ouvre, cliquez sur **Propriétés**.
3. Dans la fenêtre **Paramètres** qui s'ouvre, cliquez sur le nom du segment que vous souhaitez supprimer.
4. Cliquez sur **Supprimer**.
5. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **OK** pour confirmer votre choix.

   La connexion est supprimée. Les appareils du segment dans le Cloud correspondant à cette connexion sont automatiquement supprimés des groupes d'administration.

Configuration de la programmation du sondage via Kaspersky Security Center Web Console

Le sondage du segment dans le Cloud est programmé. Vous pouvez définir la fréquence du sondage.

La fréquence de sondage est automatiquement définie sur 5 minutes dans les paramètres de configuration de l'environnement cloud. Vous pouvez modifier cette valeur à tout moment. Toutefois, il est déconseillé de réaliser un sondage à une fréquence supérieure à 5 minutes, car cela pourrait provoquer des erreurs dans le fonctionnement de l'API.

Pour configurer la programmation du sondage du segment dans le Cloud, procédez comme suit :

1. Dans le menu principal, accédez à **Découverte et déploiement → Découverte → Cloud**.
2. Dans la fenêtre qui s'ouvre, cliquez sur **Propriétés**.
3. Dans la fenêtre **Paramètres** qui s'ouvre, cliquez sur le nom du segment pour lequel vous souhaitez configurer une programmation de sondage.

   Cela ouvre la fenêtre **Paramètres du segment dans le cloud**.

4. Dans la fenêtre **Paramètres du segment dans le cloud**, cliquez sur le bouton **Planifier le sondage**.

   Cette opération permet d'ouvrir la fenêtre **Programmation**.

5. Dans la fenêtre **Programmation**, définissez les paramètres suivants :

- **Lancement planifié**

  Options de programmation du sondage :

  - **Tous les N jours**

    Le sondage s'exécute régulièrement, selon l'intervalle défini en jours, à partir de la date et heure définis.

    Le sondage s'exécute par défaut chaque jour, à partir de la date et de l'heure actuelle du système.

  - Toutes les N minutes

    Le sondage s'exécute régulièrement, selon l'intervalle défini en minutes, à partir de l'heure définie.

    Le sondage s'exécute par défaut toutes les cinq minutes, à partir de l'heure actuelle du système.

  - Par jours de la semaine

    Le sondage s'exécute régulièrement les jours définis de la semaine, à l'heure indiquée.

    Par défaut, le sondage s'exécute chaque vendredi à 18h00.

  - Chaque mois, les jours indiqués des semaines sélectionnées

    Le sondage s'exécute régulièrement les jours définis de chaque mois, à l'heure indiquée.

    Par défaut, aucun jour du mois n'est sélectionné. L'heure de lancement par défaut est 18h00.

- **Intervalle de démarrage**

  Définissez la valeur de N (pour les minutes ou les jours).

- **À partir de**

  Déterminez quand vous souhaitez commencer le premier sondage.

- **Lancer les tâches non exécutées**

  Si le Serveur d'administration est éteint ou s'il n'est pas disponible au moment auquel le sondage a été programmé, le Serveur d'administrateur peut soit lancer le sondage immédiatement après que le Serveur d'administration a été allumé ou attendre la prochaine programmation du sondage.

  Si cette option est activée, le Serveur d'administration lance le sondage directement après qu'il a été allumé.

  Si cette option est désactivée, le Serveur d'administration attend la prochaine programmation du sondage.

  Cette option est activée par défaut.

6. Enregistrez les modifications.

La programmation du sondage pour le segment est configurée et enregistrée.

Affichage des résultats du sondage des segments dans le Cloud via Kaspersky Security Center Web Console

Vous pouvez afficher les résultats du sondage des segments dans le Cloud, c'est-à-dire afficher la liste des appareils dans le Cloud administrés par le Serveur d'administration.

Pour afficher les résultats du sondage des segments dans le Cloud,

Dans le menu principal, accédez à **Découverte et déploiement** → **Découverte** → **Cloud**.

Cette action permet d'afficher les segments dans le Cloud disponibles pour le sondage.

Affichage des propriétés des appareils du Cloud via Kaspersky Security Center Web Console

Vous pouvez afficher les propriétés de chaque appareil du Cloud.

Pour afficher les propriétés d'un appareil du Cloud, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Appareils administrés**.
2. Cliquez sur le nom de l'appareil dont vous souhaitez voir les propriétés.

   La fenêtre des propriétés s'ouvre et la section **Général** est sélectionnée.
3. Si vous souhaitez afficher les propriétés propres aux appareils du Cloud, sélectionnez la section **Système** dans la fenêtre des propriétés.

   Les propriétés sont affichées en fonction de la plateforme Cloud de l'appareil.

   Pour les appareils dans AWS, les propriétés suivantes sont affichées :

   - **Appareil découvert à l'aide de l'API** (valeur : **AWS**)
   - **Région Cloud**
   - **Cloud VPC**
   - **Zone de disponibilité du cloud**
   - **Sous-réseau du cloud**
   - **Groupe de placement Cloud** (cette unité n'est affichée que si l'instance appartient à un groupe de placement ; dans le cas contraire, elle n'est pas affichée)

   Pour les appareils dans Azure, les propriétés suivantes sont affichées :

   - **Appareil découvert à l'aide de l'API** (valeur : **Microsoft Azure**)
   - **Région Cloud**
   - **Sous-réseau Cloud**

   Pour les appareils dans Google Cloud, les propriétés suivantes sont affichées :

   - **Appareil découvert à l'aide de l'API** (valeur : **Google Cloud**)
   - **Région Cloud**
   - **Cloud VPC**
   - **Zone de disponibilité du cloud**
   - **Sous-réseau du cloud**

Synchronisation avec le Cloud : Configuration de la règle de déplacement

Pendant l'utilisation de la Configuration de l'environnement cloud, la règle Synchronisation avec Cloud est créée automatiquement. La règle permet de déplacer automatiquement les appareils trouvés à chaque sondage à partir du groupe Appareils non définis vers le groupe Appareils administrés\Cloud pour que ces appareils soient accessibles pour l'administration centralisée. La règle par défaut est activée une fois créée. Vous pouvez désactiver, modifier ou forcer une règle à tout moment.

Pour modifier les propriétés de la règle Synchronisation avec Cloud et / ou forcer une règle, procédez comme suit :

1. Dans le menu principal, accédez à **Découverte et déploiement** → **Déploiement et attribution** → **Règles de déplacement**.

   Cette action permet d'ouvrir la liste des règles de déplacement.

2. Dans la liste des règles de déplacement, sélectionnez **Synchronisation avec le cloud**.

   Cette action permet d'ouvrir la fenêtre des propriétés de la règle.

3. Si nécessaire, sous l'onglet **Conditions de la règle**, puis sous l'onglet **Segments dans le cloud**, définissez les paramètres suivants :

- **L'appareil se trouve dans un segment dans le cloud**

  La règle s'applique uniquement aux appareils qui se trouvent dans le segment dans le Cloud sélectionné. Si la case est décochée, la règle s'applique à tous les appareils trouvés.

  Cette option est sélectionnée par défaut.

- **Inclure les objets enfants**

  Si la case est cochée, cette règle exécutée pour tous les appareils du segment choisi et dans toutes les sous-sections du Cloud. Dans le cas contraire, la règle s'applique uniquement aux appareils qui se trouvent dans le segment racine.

  Cette option est sélectionnée par défaut.

- **Déplacer les appareils des objets enfants vers les sous-groupes correspondants**

  Si la case est Activé, les appareils des objets enfants sont déplacés dans les sous-groupes correspondant à leur structure.

  Si l'option est désactivée, les appareils des objets enfants sont déplacés dans la racine du sous-groupe AWS sans décomposition en sous-groupes.

  Cette option est activée par défaut.

- **Créer les sous-groupes correspondant aux conteneurs des appareils récemment détectés**

  Quand cette option est activée, quand la structure du groupe **Appareils administrés\Cloud** ne contient aucun sous-groupe correspondant à la section qui contient l'appareil, Kaspersky Security Center crée ces sous-groupes. Par exemple, si un nouveau sous-réseau est découvert pendant la Recherche d'appareils, un nouveau groupe portant le même nom est créé dans le groupe **Appareils administrés\Cloud**.

  Si cette option est désactivée, Kaspersky Security Center ne crée aucun nouveau sous-groupe. Par exemple, si un nouveau sous-réseau est découvert lors du sondage du réseau, un nouveau groupe portant le même nom ne sera pas créé dans le groupe **Appareils administrés\Cloud** et les appareils qui se trouve dans ce sous-réseau seront déplacés vers le groupe **Appareils administrés\Cloud**.

  Cette option est activée par défaut.

- **Supprimer les sous-groupes n'ayant pas de correspondance dans les segments dans le cloud**

  Si cette option est activée, l'application supprime du groupe Cloud tous les sous-groupes qui ne correspondent à aucun objet dans le cloud.

  Si cette option est désactivée, les sous-groupes qui ne correspondent à aucun objet dans le Cloud sont conservés.

  Cette option est activée par défaut.

Si vous avez activé l'option **Synchroniser les groupes d'administration avec la structure cloud** lors de l'utilisation de la Configuration de l'environnement cloud, la règle **Synchronisation avec le cloud** est créée et les options **Créer les sous-groupes correspondant aux conteneurs des appareils récemment détectés** et **Supprimer les sous-groupes n'ayant pas de correspondance dans les segments dans le cloud** sont activées.

Si vous n'avez pas activé l'option **Synchroniser les groupes d'administration avec la structure cloud**, la règle **Synchronisation avec le cloud** est créée et ces options sont désactivées (décochées). Si votre travail avec Kaspersky Security Center nécessite que la structure des sous-groupes du sous-groupe **Appareils administrés\Cloud** corresponde à la structure des segments dans le Cloud, activez les options **Créer les sous-groupes correspondant aux conteneurs des appareils récemment détectés** et **Supprimer les sous-groupes n'ayant pas de correspondance dans les segments dans le cloud** dans les propriétés de la règle, puis appliquez la règle.

4. Sélectionnez la valeur dans la liste déroulante **Appareil découvert à l'aide de l'API** :

   - **Non**. L'appareil n'est pas détecté à l'aide de l'API AWS, Azure ou Google, c'est-à-dire qu'il se trouve soit en dehors de l'environnement Cloud, soit dans l'environnement Cloud, mais il ne peut pas être détecté en utilisant une API pour une raison ou une autre.

   - **AWS**. L'appareil est détecté via l'utilisation de l'API AWS, autrement dit, l'appareil est bel et bien dans le cloud AWS.

   - **Azure**. L'appareil a été détecté via l'utilisation de l'API Azure, autrement dit, l'appareil est bel et bien dans le cloud Azure.

   - **Google Cloud**. L'appareil a été détecté via l'utilisation de l'API Google, autrement dit, l'appareil est bel et bien dans le cloud Google.

   - Pas de valeur. Le critère n'est pas appliqué.

5. En cas de besoin, configurez d'autres propriétés de la règle dans les autres sections.

La règle de déplacement est configurée.

Installation à distance d'applications sur les machines virtuelles Azure

Vous devez posséder une licence valide afin de pouvoir installer les applications sur les machines virtuelles Microsoft Azure.

Kaspersky Security Center prend en charge les scénarios suivants :

- Un appareil client est découvert par le biais d'une API Azure ; l'installation est également réalisée par le biais d'une API. L'utilisation de l'API Azure signifie que vous ne pouvez installer que les applications suivantes :

  - Kaspersky Endpoint Security for Linux

  - Kaspersky Endpoint Security for Windows

  - Kaspersky Security for Windows Server

- Un appareil client est découvert au moyen de l'API Azure ; l'installation est effectuée au moyen d'un point de distribution ou, s'il n'y a pas de point de distribution, manuellement, à l'aide de paquets d'installation autonomes. Vous pouvez ainsi installer n'importe quelle application prise en charge par Kaspersky Security Center.

Pour créer une tâche d'installation à distance de l'application sur les machines virtuelles Azure :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Tâches**.
2. Cliquez sur **Ajouter**.

   Ceci permet de lancer l'assistant de création d'une tâche.
3. Suivez les instructions de l'assistant :

   a. Sélectionnez **Installation à distance d'une application** comme type de tâche.

   b. Sur la page **Paquets d'installation**, sélectionnez **Installation à distance par l'API Microsoft Azure**.

   c. Lorsque vous sélectionnez le compte pour accéder aux appareils, utilisez un compte Azure existant ou cliquez sur **Ajouter** et saisissez les identifiants de votre compte Azure :

   - **Nom du compte Azure**

     Saisissez n'importe quel nom pour les identifiants que vous précisez. Ce nom s'affichera dans la liste des comptes pour l'exécution de la tâche.

   - **ID de l'application Azure**

     Vous avez créé cet identifiant de l'application sur le portail Azure.

     Vous pouvez fournir un identifiant de l'application Azure pour le sondage et d'autres fins. Si vous souhaitez sonder un autre segment Azure, il faut d'abord supprimer la connexion Azure existante.

   - **Mot de passe de l'application Azure**

     Vous avez obtenu le mot de passe de l'identifiant de l'application quand vous avez créé celui-ci.

     Les caractères de la mot de passe s'affichent sous la forme d'astérisques. Après que vous avez commencé à saisir le mot de passe, le bouton **Afficher** apparaît. Maintenez ce bouton enfoncé pour voir les caractères saisis.

   d. Sélectionnez les appareils concernés dans le groupe **Appareils administrés\Cloud**.

Quand l'assistant a terminé, la tâche d'installation à distance de l'application apparaît dans la liste des tâches.

Création d'une tâche de sauvegarde des données du Serveur d'administration à l'aide d'un SGBD dans le Cloud

Les tâches de sauvegarde sont des tâches du Serveur d'administration. Vous créez une tâche de sauvegarde si vous souhaitez utiliser un SGBD situé dans un environnement Cloud (AWS ou Azure).

Pour créer une tâche de copie de sauvegarde des données du Serveur d'administration, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Tâches**.
2. Cliquez sur **Ajouter**.

   Ceci permet de lancer l'Assistant de création d'une tâche.

3. Sur la première page de l'Assistant, dans la liste **Application**, sélectionnez **Kaspersky Security Center 15.1**, et dans la liste **Type de tâche**, sélectionnez **Sauvegarde des données du Serveur d'administration**.

4. Sur la page correspondante de l'Assistant, définissez les informations suivantes :

   - Si vous utilisez une base de données dans AWS :

     - **Nom du compartiment S3**

       Le nom du compartiment S3 que vous avez créé pour la Sauvegarde.

     - **ID de clé d'accès**

       Vous avez reçu l'ID de clé (séquence de caractères alphanumériques) lorsque vous avez créé le compte utilisateur IAM pour travailler avec l'instance de stockage du seau S3.

       Le champ est disponible si vous avez sélectionné la base de données RDS sur un seau S3.

     - **Clé secrète**

       La clé secrète que vous avez reçue avec l'ID de clé d'accès quand vous avez créé le compte utilisateur IAM.

       Les caractères de la clé secrète s'affichent sous la forme d'astérisques. Après que vous avez commencé à saisir la clé secrète, le bouton **Afficher** apparaît. Cliquez sur ce bouton pendant le temps qu'il vous faut pour consulter les caractères saisis.

       Ce champ est accessible si vous avez opté pour l'autorisation à l'aide d'une clé d'accès AWS IAM et non pas d'un rôle IAM.

   - Si vous utilisez une base de données dans Microsoft Azure :

     - **Nom du compte du stockage Azure**

       Vous avez créé le nom du Compte du stockage Azure pour utiliser Kaspersky Security Center.

     - **Identifiant de l'abonnement Azure**

       Vous avez créé l'abonnement sur le portail Azure.

     - **Mot de passe Azure**

       Vous avez obtenu le mot de passe de l'ID de l'application quand vous avez créé celui-ci.

       Les caractères de la mot de passe s'affichent sous la forme d'astérisques. Après que vous avez commencé à saisir le mot de passe, le bouton **Afficher** apparaît. Maintenez ce bouton enfoncé pour voir les caractères saisis.

     - **ID de l'application Azure**

Vous avez créé cet identifiant de l'application sur le portail Azure.

Vous pouvez fournir un identifiant de l'application Azure pour le sondage et d'autres fins. Si vous souhaitez sonder un autre segment Azure, il faut d'abord supprimer la connexion Azure existante.

- **Nom du serveur SQL Azure**

  Le nom et le groupe de ressources sont disponibles dans les propriétés du Serveur Azure SQL

- **Groupe de ressources du serveur SQL Azure**

  Le nom et le groupe de ressources sont disponibles dans les propriétés du Serveur Azure SQL

- **Clé d'accès au stockage Azure**

  Disponible dans les propriétés de votre compte de stockage, dans la sections Clés d'accès. Vous pouvez utiliser n'importe quelle clé (clé1 ou clé2).

La tâche est créée et s'affiche dans la liste des tâches. Si vous activez l'option **Ouvrir les détails de la tâche à la fin de la création**, vous pouvez modifier les paramètres par défaut de la tâche immédiatement après la création de celle-ci. Si vous n'activez pas cette tâche, la tâche est créée selon les paramètres par défaut. Vous pourrez modifier ces paramètres par défaut plus tard, à tout moment.

Diagnostic à distance des appareils clients

Vous pouvez utiliser les diagnostics à distance pour l'exécution à distance des opérations suivantes sur des appareils clients Windows et Linux :

- Activation et désactivation du traçage, modification du niveau de traçage et téléchargement du fichier de traçage
- Téléchargement des informations relatives au système et des paramètres des applications
- Téléchargement des journaux des événements
- Génération d'un fichier dump pour une application
- Lancement du diagnostic et téléchargement des rapports du diagnostic
- Lancement, arrêt ou relancement des applications

Vous pouvez utiliser les journaux des événements et les rapports de diagnostic téléchargés depuis un appareil client pour résoudre vous-même un problème. Si vous contactez le Support Technique de Kaspersky, un expert du Support Technique peut également vous demander de télécharger les fichiers de traçage, les fichiers de vidage, les journaux des événements et les rapports de diagnostic d'un appareil client pour que Kaspersky puisse réaliser une analyse plus poussée.

Ouverture de la fenêtre de diagnostic à distance

Pour effectuer des diagnostics à distance sur des appareils clients Windows et Linux, vous devez d'abord ouvrir la fenêtre de diagnostics à distance.

Pour ouvrir la fenêtre de diagnostic à distance, procédez comme suit :

1. Pour sélectionner l'appareil pour lequel vous souhaitez ouvrir la fenêtre de diagnostic à distance, réalisez une des actions suivantes :

   - Si l'appareil appartient à un groupe d'administration, dans le menu principale, accédez à **Ressources (Appareils)** → **Appareils administrés**.

   - Si l'appareil appartient au groupe Appareils non définis, dans le menu principal, accédez à **Découverte et déploiement** → **Appareils non définis**.

2. Cliquez sur le nom de l'appareil concerné.

3. Dans la fenêtre des propriétés de l'appareil qui s'ouvre, sélectionnez l'onglet **Avancé**.

4. Dans la fenêtre qui s'ouvre, cliquez sur **Diagnostic à distance**.

   Cette action permet d'ouvrir la fenêtre **Diagnostic à distance** d'un appareil client. Si la connexion entre le Serveur d'administration et l'appareil client n'est pas établie, le message d'erreur s'affiche.

Alternativement, si vous avez besoin d'obtenir simultanément toutes les informations de diagnostic sur un appareil client Linux, vous pouvez exécuter le script collect.sh sur cet appareil.

Activation et désactivation du traçage pour les applications

Vous pouvez activer et désactiver le traçage pour les applications, y compris le traçage Xperf.

Activation et désactivation du traçage

Pour activer ou désactiver le traçage sur un appareil distant :

1. Ouvrez la fenêtre de diagnostic à distance d'un l'appareil client.

2. Dans la fenêtre de diagnostic à distance, sélectionnez l'onglet **Applications Kaspersky**.

   Dans la section **Administration des applications**, la liste des applications Kaspersky installées sur l'appareil s'affiche.

3. Dans la liste des applications, sélectionnez l'application pour laquelle vous souhaitez activer ou désactiver le traçage.

   La liste des options de diagnostic à distance s'ouvre.

4. Si vous souhaitez activer le traçage, procédez comme suit :

   a. Dans la section **Traçage**, cliquez sur **Activer le traçage**.

   b. Dans la fenêtre **Modifier le niveau de traçage** qui s'ouvre, nous conseillons de conserver les valeurs par défaut pour les paramètres. Le cas échéant, un expert du Support Technique vous guidera au cours du processus de configuration. Les paramètres suivants sont disponibles :

   - **Niveau de traçage**

     Le niveau de traçage définit le volume de détails repris dans le fichier de traçage.

   - **Traçage sur la base d'une rotation**

     L'application écrase les informations de traçage afin d'empêcher l'augmentation excessive de la taille du fichier de traçage. Indiquez le nombre maximal de fichiers à utiliser pour stocker les informations de traçage ainsi que la taille maximale de chaque fichier. Quand le nombre maximum de fichiers de traçage de la taille maximale est atteint, le fichier de traçage le plus ancien est supprimé afin de pouvoir écrire un nouveau fichier de traçage.

     Ce paramètre est disponible uniquement pour Kaspersky Endpoint Security.

   c. Cliquez sur **Enregistrer**.

   Le traçage est activé pour l'application sélectionnée. Dans certains cas, pour activer le traçage de l'application de sécurité, il faut relancer cette application et sa tâche.

   Sur les appareils clients basés sur Linux, le suivi du module Programme de mise à jour de l'Agent d'administration est réglementé par les paramètres de l'Agent d'administration. Par conséquent, les options **Activer le traçage** et **Modifier le niveau de traçage** sont désactivées pour ce module sur les appareils clients exécutant Linux.

5. Si vous souhaitez désactiver le traçage pour l'application sélectionnée, cliquez sur le bouton **Désactiver le traçage**.

   Le traçage est désactivé pour l'application sélectionnée.

Activation du traçage Xperf

Pour Kaspersky Endpoint Security, un expert du Support Technique peut vous demander d'activer le traçage Xperf pour les informations relatives aux performances du système.

Pour activer et configurer le traçage Xperf ou le désactiver, procédez comme suit :

1. Ouvrez la fenêtre de diagnostic à distance d'un l'appareil client.

2. Dans la fenêtre de diagnostic à distance, sélectionnez l'onglet **Applications Kaspersky**.

   Dans la section **Administration des applications**, la liste des applications Kaspersky installées sur l'appareil s'affiche.

3. Dans la liste des applications, sélectionnez Kaspersky Endpoint Security for Windows.

   La liste des options de diagnostic à distance pour Kaspersky Endpoint Security for Windows s'affiche.

4. Dans la section **Traçage Xpref**, cliquez sur **Activer le traçage Xperf**.

   Si le traçage Xperf est déjà activé, le bouton **Désactiver le traçage Xperf** s'affiche à la place. Cliquez sur ce bouton si vous souhaitez désactiver le traçage Xperf pour Kaspersky Endpoint Security for Windows.

5. Dans la fenêtre **Modifier le niveau de traçage Xperf** qui s'ouvre, en fonction de la demande de l'expert du Support Technique, réalisez les opérations suivantes :

   a. Sélectionnez l'un des niveaux de traçage suivants :

   - **Niveau faible**

     Un fichier de traçage de ce genre contient le minimum d'informations sur le système.

     Cette option est sélectionnée par défaut.

   - **Niveau profond**

     Un fichier de traçage de ce type contient plus de détails que les fichiers de traçage du niveau *Clair* et qui peut être sollicité par les experts du Support Technique lorsqu'un fichier de traçage du niveau *Clair* ne suffit pas à évaluer les performances. Le fichier de traçage *Profond* contient les informations techniques relatives au système, dont les informations relatives au matériel, au système d'exploitation, à la liste des processus et des applications lancés et arrêtés, aux événements utilisés pour l'évaluation des performants et aux événements de l'outil d'évaluation du système Windows.

   b. Sélectionnez l'une des types de traçage Xperf suivants :

   - **Type élémentaire**

     Les informations de traçage sont obtenues pendant le fonctionnement de l'application Kaspersky Endpoint Security.

     Cette option est sélectionnée par défaut.

   - **Type au redémarrage**

     Les informations de traçage sont reçues au du démarrage du système d'exploitation sur l'appareil administré. Ce type de traçage est efficace lorsque le problème qui affecte les performances du système se produit après que l'appareil est allumé et avant le démarrage de Kaspersky Endpoint Security.

   Vous pourriez également être invité à activer l'option **Taille du fichier de rotation, en Mo** pour empêcher l'augmentation excessive de la taille du fichier de traçage. Définissez ensuite la taille maximale de chaque fichier de traçage. Quand le fichier atteint la taille maximale, les informations de traçage les plus anciennes sont écrasées par les nouvelles.

   c. Définissez la taille du fichier de rotation.

   d. Cliquez sur **Enregistrer**.

   Le traçage Xperf est activé et configuré.

6. Si vous souhaitez désactiver le traçage Xperf pour Kaspersky Endpoint Security for Windows, cliquez sur **Désactiver le traçage Xperf** dans la section **Traçage Xpref**.

   Le traçage Xperf est désactivé.

Téléchargement des fichiers de traçage d'une application

Pour télécharger un fichier de traçage depuis une application :

1. Ouvrez la fenêtre de diagnostic à distance d'un l'appareil client.
2. Dans la fenêtre de diagnostic à distance, sélectionnez l'onglet **Applications Kaspersky**.

   Dans la section **Administration des applications**, la liste des applications Kaspersky installées sur l'appareil s'affiche.
3. Dans la liste des applications, sélectionnez l'application pour laquelle vous souhaitez télécharger un fichier de traçage.
4. Dans la section **Traçage**, cliquez sur le bouton **Fichiers de traçage**.

   Cette action permet d'ouvrir la fenêtre **Journaux de traçage des appareils**, où une liste des fichiers de traçage s'affiche.
5. Dans la liste des fichiers de traçage, sélectionnez le fichier que vous souhaitez télécharger.
6. Exécutez une des actions suivantes :

   - Téléchargez le fichier sélectionné en cliquant sur **Télécharger**. Vous pouvez sélectionner un ou plusieurs fichiers à télécharger.
   - Téléchargez une partie du fichier sélectionné :

     a. Cliquez sur **Télécharger une partie**.

     Il est impossible de télécharger des parties de plusieurs fichiers à la fois. Si vous sélectionnez plusieurs fichiers de traçage, le bouton **Télécharger une partie** est désactivé.

     b. Dans la fenêtre qui s'ouvre, indiquez le nom et la partie de fichier à télécharger, en fonction de vos besoins.

     Pour les appareils basés sur Linux, la modification du nom de la partie du fichier n'est pas disponible.

     c. Cliquez sur **Télécharger**.

Le fichier sélectionné, ou une partie de celui-ci, est téléchargé à l'emplacement que vous définissez.

Suppression de fichiers de traçage

Vous pouvez supprimer les fichiers de traçage qui ne sont plus nécessaires.

Pour supprimer un fichier de traçage, procédez comme suit :

1. Ouvrez la fenêtre de diagnostic à distance d'un l'appareil client.
2. Dans la fenêtre de diagnostic à distance qui s'ouvre, sélectionnez l'onglet **Journaux des événements**.

3. Dans la section **Fichiers de traçage**, cliquez sur **Journaux du service Windows Update** ou **Journaux d'installation à distance**, en fonction des fichiers de traçage que vous souhaitez supprimer.

   > Le lien **Journaux du service Windows Update** est disponible uniquement pour les appareils clients Windows.

   Cette action permet d'ouvrir la fenêtre **Journaux de traçage des appareils**, où une liste des fichiers de traçage s'affiche.

4. Dans la liste des fichiers de traçage, sélectionnez un ou plusieurs fichiers que vous souhaitez supprimer.

5. Cliquez sur le bouton **Supprimer**.

Les fichiers de traçage sélectionnés sont supprimés.

Téléchargement des paramètres de l'application

Pour télécharger les paramètres des applications à partir d'un appareil client, procédez comme suit :

1. Ouvrez la fenêtre de diagnostic à distance d'un l'appareil client.

2. Dans la fenêtre de diagnostic à distance, sélectionnez l'onglet **Applications Kaspersky**.

3. Dans la section **Paramètres de l'application**, cliquez sur le bouton **Télécharger** pour télécharger les informations relatives aux paramètres des applications installées sur l'appareil client.

L'archive ZIP contenant les informations est téléchargée à l'emplacement indiqué.

Téléchargement des journaux des événements

Pour télécharger le journal des événements depuis l'appareil distant, procédez comme suit :

1. Ouvrez la fenêtre de diagnostic à distance d'un l'appareil client.

2. Dans la fenêtre de diagnostic à distance, sous l'onglet **Journaux des événements**, cliquez sur **Tous les journaux des appareils**.

3. Dans la fenêtre **Tous les journaux des appareils**, sélectionnez un ou plusieurs journaux pertinents.

4. Exécutez une des actions suivantes :

   - Téléchargez le journal sélectionné en cliquant sur **Télécharger le fichier entier**.

   - Téléchargez une partie du journal sélectionné :

     a. Cliquez sur **Télécharger une partie**.

     Il est impossible de télécharger des parties de plusieurs journaux à la fois. Si vous sélectionnez plusieurs journaux d'événements, le bouton **Télécharger une partie** sera désactivé.

     b. Dans la fenêtre qui s'ouvre, indiquez le nom et la partie du journal à télécharger, en fonction de vos besoins.

     Pour les appareils basés sur Linux, la modification du nom de la partie du journal n'est pas disponible.

     c. Cliquez sur **Télécharger**.

Le journal des événements sélectionné, ou une partie de celui-ci, est téléchargé à l'emplacement spécifié.

Lancement, arrêt, relancement de l'application

Vous pouvez lancer, arrêter et relancer des applications sur un appareil client.

Pour lancer, arrêter ou relancer une application, procédez comme suit :

1. Ouvrez la fenêtre de diagnostic à distance d'un l'appareil client.

2. Dans la fenêtre de diagnostic à distance, sélectionnez l'onglet **Applications Kaspersky**.

   Dans la section **Administration des applications**, la liste des applications Kaspersky installées sur l'appareil s'affiche.

3. Dans la liste des applications, sélectionnez l'application que vous souhaitez lancer, arrêter ou relancer.

4. Sélectionnez une action en cliquant sur l'un des boutons suivants :

   - **Arrêter l'application**

     Ce bouton n'est accessible que si l'application est en cours d'exécution.

   - **Relancer l'application**

     Ce bouton n'est accessible que si l'application est en cours d'exécution.

   - **Lancer l'application**

     Ce bouton n'est accessible que si l'application n'est pas en cours d'exécution.

Selon l'action sélectionnée, l'application nécessaire sera lancée, arrêtée ou relancée sur l'appareil client.

Si vous redémarrez l'Agent d'administration, un message s'affiche indiquant que la connexion actuelle de l'appareil au Serveur d'administration sera interrompue.

Exécuter le diagnostic à distance de l'Agent d'administration de Kaspersky Security Center et télécharger les résultats

Pour lancer le diagnostic de l'Agent d'administration de Kaspersky Security Center sur un appareil à distance et télécharger les résultats, procédez comme suit :

1. Ouvrez la fenêtre de diagnostic à distance d'un l'appareil client.
2. Dans la fenêtre de diagnostic à distance, sélectionnez l'onglet **Applications Kaspersky**.

   Dans la section **Administration des applications**, la liste des applications Kaspersky installées sur l'appareil s'affiche.
3. Dans la liste des applications, sélectionnez **Agent d'administration de Kaspersky Security Center**.

   La liste des options de diagnostic à distance s'ouvre.
4. Dans la section **Rapport de diagnostic**, cliquez sur le bouton **Poser le diagnostic**.

   Cette action permet de lancer le processus de diagnostic à distance et de générer un rapport de diagnostic. Le processus de diagnostic est terminé, le bouton **Télécharger le rapport des diagnostics** devient accessible.
5. Cliquez sur le bouton **Télécharger le rapport des diagnostics** pour télécharger le rapport.

Le rapport est téléchargé à l'emplacement indiqué.

Exécution d'une application sur un appareil client

Vous devrez peut-être exécuter une application sur l'appareil client si un expert du Support technique de Kaspersky vous le demande. Vous n'avez pas besoin d'installer l'application sur cet appareil.

Pour exécuter une application sur l'appareil client, procédez comme suit :

1. Ouvrez la fenêtre de diagnostic à distance d'un l'appareil client.
2. Dans la fenêtre de diagnostic à distance, sélectionnez l'onglet **Exécution d'une application à distance**.
3. Dans le groupe **Fichiers de l'application**, cliquez sur le bouton **Parcourir** afin de sélectionner une archive ZIP contenant l'application que vous souhaitez exécuter sur l'appareil client.

   L'archive ZIP doit inclure le dossier des utilitaires. Ce dossier contient le fichier exécutable qui sera lancé sur un appareil distant.

   Vous pouvez spécifier le nom du fichier exécutable et les arguments de la ligne de commande, si nécessaire. Pour ce faire, remplissez les champs **Fichier exécutable dans une archive à exécuter sur un appareil distant** et **Arguments de la ligne de commande**.
4. Cliquez sur le bouton **Charger et exécuter** pour lancer l'application indiquée sur l'appareil client.
5. Suivez les instructions d'un expert de l'assistance Kaspersky.

Génération d'un fichier dump pour une application

Le fichier de vidage de l'application vous permet de consulter les paramètres de l'application exécutée sur l'appareil client à un moment donné. Ce fichier contient également des informations sur les modules chargés pour une application.

L'obtention de fichiers de vidage à partir d'appareils Linux n'est pas prise en charge.

L'utilitaire kldumper est utilisé pour obtenir les fichiers de vidage via le diagnostic à distance. Cet utilitaire est conçu pour obtenir les fichiers de vidage des processus des applications Kaspersky à la demande des experts du Support technique. Vous trouverez plus de détails sur les exigences relatives à l'utilisation de l'utilitaire kldumper dans la Base de connaissances de Kaspersky Security Center.

Pour créer un fichier de vidage pour une application :

1. Ouvrez la fenêtre de diagnostic à distance d'un l'appareil client.
2. Dans la fenêtre de diagnostic à distance, sélectionnez l'onglet **Exécution d'une application à distance**.
3. Dans la section **Génération du fichier dump du processus**, indiquez le fichier exécutable de l'application pour lequel vous souhaitez générer le fichier dump.
4. Cliquez sur le bouton **Télécharger le fichier dump**.

   Les archives avec le fichier de vidage de l'application sont téléchargées.

   Si l'application indiquée n'est pas exécutée sur l'appareil client, le dossier « result » contenu dans l'archive téléchargée sera vide.

   Si l'application indiquée fonctionne, mais que le téléchargement échoue avec une erreur ou que le dossier « result » est vide dans l'archive téléchargée, consultez la Base de connaissances de Kaspersky Security Center.

Exécution de diagnostics à distance sur un appareil client basé sur Linux

Kaspersky Security Center vous permet de télécharger les informations de diagnostic de base à partir d'un appareil client. Vous pouvez également obtenir les informations de diagnostic sur un appareil basé sur Linux à l'aide du script collect.sh de Kaspersky. Ce script est exécuté sur l'appareil client Linux qui doit être diagnostiqué, puis génère un fichier contenant les informations de diagnostic, les informations système sur cet appareil, les fichiers de traçage des applications, les journaux de l'appareil et un fichier de vidage pour les applications terminées en urgence.

Nous vous recommandons d'utiliser le script collect.sh pour obtenir simultanément toutes les informations de diagnostic sur l'appareil client Linux. Si vous téléchargez les informations de diagnostic à distance via Kaspersky Security Center, vous devrez parcourir toutes les sections de l'interface de diagnostic à distance. De plus, les informations de diagnostic d'un appareil basé sur Linux ne seront probablement pas obtenues dans leur intégralité.

Si vous devez envoyer le fichier généré avec les informations de diagnostic au support technique de Kaspersky, supprimez toutes les informations confidentielles avant d'envoyer le fichier.

Pour télécharger les informations de diagnostic à partir d'un appareil client Linux à l'aide du script collect.sh :

1. Téléchargez le script collect.sh emballé dans l'archive collect.tar.gz.
2. Copiez l'archive téléchargée sur l'appareil client Linux qui doit être diagnostiqué.
3. Exécutez la commande suivante pour décompresser l'archive collect.tar.gz :

   ```
   # tar -xzf collect.tar.gz
   ```

4. Exécutez la commande suivante pour spécifier les droits d'exécution du script :

   ```
   # chmod +x collect.sh
   ```

5. Exécutez le script collect.sh en utilisant un compte disposant de droits d'administrateur :

   ```
   # ./collect.sh
   ```

Un fichier contenant les informations de diagnostic est généré et enregistré dans le dossier /tmp/$HOST_NAME-collect.tar.gz.

Téléchargement et suppression de fichiers de la Quarantaine et de la Sauvegarde

Cette section explique comment télécharger et supprimer des fichiers de la Quarantaine et de la Sauvegarde dans Kaspersky Security Center Web Console.

Téléchargement de fichiers à partir de la Quarantaine et de la Sauvegarde

Vous ne pouvez télécharger des fichiers depuis la Quarantaine et la Sauvegarde que si l'une des deux conditions est remplie : l'option **Maintenir la connexion au Serveur &d'administration** est activée dans les paramètres de l'appareil ou une passerelle de connexion est en cours d'utilisation. Dans le cas contraire, il n'est pas possible d'effectuer de téléchargement.

Pour enregistrer une copie du fichier de la quarantaine ou du dossier de sauvegarde sur le disque dur, procédez comme suit :

1. Exécutez une des actions suivantes :

   - Si vous souhaitez enregistrer une copie du fichier en quarantaine, dans le menu principal, accédez à **Opérations → Stockages → Quarantaine**.

   - Si vous souhaitez enregistrer une copie du fichier du dossier de sauvegarde, dans le menu principal, accédez à **Opérations → Stockages → Sauvegarde**.

2. Dans la fenêtre qui s'ouvre, sélectionnez un fichier que vous souhaitez télécharger et cliquez sur **Télécharger**.

   Le téléchargement démarre. Une copie du fichier qui avait été placé en quarantaine sur l'appareil client est enregistrée dans le dossier indiqué.

Modification de la langue de l'interface de Kaspersky Security Center Web Console

Vous pouvez sélectionner la langue de l'interface de Kaspersky Security Center Web Console.

Pour modifier la langue d'interface, procédez comme suit :

1. Dans le menu principal, accédez à **Paramètres → Langue**.

2. Sélectionnez une des langues de localisation prises en charge.

Guide de référence de l'API

Ce guide de référence de Kaspersky Security Center OpenAPI est conçu pour vous aider dans les tâches suivantes :

- Automatisation et personnalisation. À l'aide de la Console d'administration, vous pouvez automatiser les tâches que vous ne souhaitez peut-être pas gérer manuellement. Vous pouvez également implémenter des scénarios personnalisés qui ne sont pas encore pris en charge dans la Console d'administration. Par exemple, en tant qu'administrateur, vous pouvez utiliser Kaspersky Security Center OpenAPI pour créer et exécuter des scripts qui faciliteront le développement de la structure des groupes d'administration et maintiendront cette structure à jour.

- Développement personnalisé. Par exemple, vous pouvez développer une autre Console d'administration basée sur MMC pour vos clients qui permet d'effectuer un ensemble limité d'actions.

Dans le guide de référence OpenAPI, vous pouvez utiliser le champ de recherche situé dans la partie droite de l'écran pour localiser les informations dont vous avez besoin.

GUIDE DE RÉFÉRENCE OPENAPI

Exemples de scripts

Le guide de référence OpenAPI contient des exemples de scripts Python répertoriés dans le tableau ci-dessous. Les exemples montrent comment vous pouvez appeler les méthodes OpenAPI et accomplir automatiquement différentes tâches pour protéger votre réseau, par exemple, créer une hiérarchie " principale/secondaire ", exécuter des tâches dans Kaspersky Security Center ou affecter des points de distribution. Vous pouvez exécuter les exemples tels quels ou créer vos propres scripts sur la base des exemples.

Pour appeler les méthodes OpenAPI et exécuter des scripts, procédez comme suit :

1. Téléchargez l'archive KlAkOAPI.tar.gz. Cette archive comprend le paquet KlAkOAPI et des exemples (vous pouvez les copier à partir de l'archive ou du guide de référence OpenAPI). L'archive KlAkOAPI.tar.gz se trouve également dans le dossier d'installation de Kaspersky Security Center.

2. Installez le paquet KlAkOAPI depuis l'archive KlAkOAPI.tar.gz sur l'appareil sur lequel le Serveur d'administration est installé.

   Vous pouvez appeler les méthodes OpenAPI, exécuter les exemples et vos propres scripts uniquement sur les appareils sur lesquels le Serveur d'administration et le paquet KlAkOAPI sont installés.

Correspondance entre les scénarios utilisateur et les exemples de méthodes de Kaspersky Security Center OpenAPI

Exemple	Objectif de l'exemple	Scénario
Journal KlAkParams	Vous pouvez extraire et traiter les données en utilisant la structure de données `KlAkParams`. L'exemple montre comment utiliser cette structure de données. L'exemple de sortie peut être présent de différentes manières. Vous pouvez obtenir les données pour envoyer une méthode HTTP ou les utiliser dans votre code.	Surveillance et rapports
Créer et supprimer une hiérarchie primaire/secondaire	Vous pouvez ajouter un Serveur d'administration secondaire et établir une hiérarchie de type " principal/secondaire ". Vous pouvez également déconnecter le Serveur d'administration secondaire de la hiérarchie.	• Création d'une hiérarchie des Serveurs d'administration : ajout d'un Serveur d'administration secondaire • Suppression d'une hiérarchie des Serveurs d'administration
Créer la hiérarchie de groupe avec une structure basée sur l'unité Active Directory	Vous pouvez sonder l'unité Active Directory et former une hiérarchie de groupes d'appareil découverts.	Création des groupes d'administration
Créer la hiérarchie de groupe avec une structure basée sur l'unité Active Directory mise en cache	Vous pouvez former une hiérarchie des groupes d'appareils administrés en fonction de l'unité Active Directory sondé précédemment. Si de nouveaux appareils apparaissent dans Active Directory après le dernier sondage, ils ne sont pas ajoutés au groupe parce qu'ils ne figurent pas dans les résultats enregistrés du sondage.	Création des groupes d'administration
Télécharger les fichiers avec la liste des réseaux via la passerelle de connexion vers l'appareil spécifié	Vous pouvez vous connecter à l'Agent d'administration sur l'appareil nécessaire à l'aide d'une passerelle de connexion, puis téléchargez un fichier contenant la liste des réseaux sur votre appareil.	Réglage des points de distribution et des passerelles de connexion
Installez une clé de licence stockée dans le stockage principal du Serveur d'administration sur les Serveurs d'administration secondaires	Vous pouvez vous connecter au Serveur d'administration primaire, télécharger une clé de licence requise à partir de celui-ci et transmettre cette clé à tous les Serveurs d'administration secondaires inclus dans une hiérarchie.	Licence des applications administrées
Créer un rapport des droits d'utilisateur effectifs	Vous pouvez créer les rapports différents. Par exemple, vous pouvez générer le rapport des droits d'utilisateur effectifs en utilisant cet exemple. Ce rapport décrit les droits dont dispose un utilisateur, en fonction de son groupe et de son rôle. Vous pouvez télécharger le rapport au format HTML, PDF ou Excel.	Génération et affichage d'un rapport
Lancer une tâche pour un appareil	Vous pouvez vous connecter à l'Agent d'administration sur l'appareil nécessaire à l'aide d'une passerelle de connexion, puis exécuter la tâche nécessaire.	Lancer une tâche manuellement

Exemple	Objectif de l'exemple	Scénario
Créer des sous-réseaux IP reposant sur Active Directory Site and Services	Vous pouvez créer un sous-réseau IP basé sur l'unité Active Directory que vous utilisez. L'exemple lance le sondage de la plage d'adresses IP spécifiée et supprime les sous-réseaux découverts pour éviter leur conflit avec un nouveau sous-réseau. Par conséquent, n'exécutez pas cet exemple sur le réseau où il est important d'enregistrer les sous-réseaux. Après le sondage, l'exemple fait référence à Active Directory, examine chaque appareil qu'il contient et crée le sous-réseau IP. Pour ce faire, l'exemple utilise les masques et les adresses IP de tous les appareils.	Configuration de la protection réseau
Enregistrer les points de distribution pour les appareils d'un groupe	Vous pouvez affecter des appareils administrés en tant que points de distribution (anciennement appelés agents de mise à jour).	Mise à jour des bases de données et des applications Kaspersky
Énumérer tous les groupes	Vous pouvez effectuer diverses actions avec les groupes d'administration : L'exemple montre comment procéder : • Obtenir un identifiant du groupe racine "Appareils administrés" • Se déplacer dans la hiérarchie du groupe • Récupérer la hiérarchie complète et développée des groupes, ainsi que leurs noms et leur imbrication	Configuration du Serveur d'administration
Énumérer les tâches, interroger les statistiques des tâches et exécuter une tâche	Vous pouvez découvrir les informations suivantes : • Historique de progression des tâches • État actuel de la tâche • Nombre de tâches dans différents états Vous pouvez également exécuter une tâche. Par défaut, l'exemple exécute une tâche après avoir généré des statistiques.	Suivi et affichage des comptes rendus d'activité des tâches
Créer et exécuter une tâche	Vous pouvez créer une tâche. Spécifiez dans l'exemple les paramètres suivants de la tâche : • Type • Méthode d'exécution • Nom • Groupe d'appareils pour lequel la tâche sera utilisée Par défaut, l'exemple crée une tâche avec le type "Afficher un message". Vous pouvez exécuter cette tâche pour tous les appareils administrés du Serveur d'administration. Si nécessaire, vous pouvez spécifier vos propres paramètres de la tâche.	Création d'une tâche
Énumérer les clés de licence	Vous pouvez obtenir une liste de toutes les clés de licence actives pour les applications Kaspersky installées sur les appareils administrés du Serveur d'administration. La liste contient des données détaillées sur chaque clé de licence, telles que le nom, le type ou la date d'expiration.	Consultation des informations sur les clés de licence utilisées
Créer et trouver un utilisateur interne	Vous pouvez créer un compte pour les travaux ultérieurs.	Sélection du compte utilisateur pour lancer le Serveur d'administration
Créer une catégorie personnalisée	Vous pouvez créer la catégorie d'application avec les paramètres nécessaires.	Création d'une catégorie d'applications enrichie manuellement
Énumérer les utilisateurs à l'aide de SrvView	Vous pouvez utiliser la catégorie SrvView pour demander des informations détaillées depuis le Serveur d'administration. Par exemple, vous pouvez obtenir une liste d'utilisateurs en utilisant cet exemple.	Administration des comptes utilisateurs

Applications interagissant avec Kaspersky Security Center via OpenAPI

Certaines applications interagissent avec Kaspersky Security Center via OpenAPI. De telles applications incluent, par exemple, Kaspersky Anti Targeted Attack Platform ou Kaspersky Security for Virtualization. Il peut également s'agir d'une application cliente personnalisée que vous avez développée sur la base d'OpenAPI.

Les applications interagissant avec Kaspersky Security Center via OpenAPI se connectent au Serveur d'administration. Si vous avez configuré une liste d'autorisations d'adresses IP pour la connexion au Serveur d'administration, ajoutez les adresses IP des appareils sur lesquels sont installées les applications utilisant Kaspersky Security Center OpenAPI. Pour savoir si l'application que vous utilisez fonctionne par OpenAPI, consultez l'Aide de cette application.

Meilleures pratiques pour les prestataires de services

Cette section fournit les informations relatives à la configuration et à l'utilisation de Kaspersky Security Center.

Elle contient des recommandations sur le déploiement, la configuration et l'utilisation de l'application, ainsi que les solutions pour résoudre les problèmes les plus fréquents qui surviennent pendant le fonctionnement de l'application.

Planification du déploiement de Kaspersky Security Center

Lors de la planification du déploiement des modules de Kaspersky Security Center dans le réseau de l'entreprise, il faut prendre en considération les facteurs suivants :

- Nombre total d'appareils
- Nombre de clients MSP

Un Serveur d'administration peut servir un maximum de 100 000 appareils. Si le total des appareils sur le réseau d'une entreprise est supérieur à 100 000, il faut installer chez les fournisseurs de service plusieurs Serveurs d'administration regroupés dans une hiérarchie pour simplifier l'administration centralisée.

Il est possible de créer un maximum de 500 serveurs virtuels sur un Serveur d'administration et par conséquent, il faut prévoir un Serveur d'administration distinct par groupe de 500 clients MSP.

Lors de la planification du déploiement, il faut examiner la nécessité d'attribuer au Serveur d'administration un certificat spécial X.509. L'attribution d'un certificat X.509 au Serveur d'administration peut se justifier dans les cas suivants (liste non-exhaustive) :

- Pour inspecter le trafic SSL à l'aide d'un proxy de terminaison SSL termination proxy ou pour utiliser un proxy inverse
- Pour attribuer les valeurs souhaitées des champs du certificat
- Pour garantir la robustesse souhaitée du chiffrement du certificat

Octroi de l'accès au Serveur d'administration via Internet

Pour que les appareils installés sur le réseau du client puissent contacter le Serveur d'administration via Internet, les ports suivants du Serveur d'administration doivent être accessibles :

- 13000 TCP : port TLS du Serveur d'administration, ce port est réservé à la connexion des Agents d'administration du réseau du client
- 8061 TCP : port HTTPS, utilisé pour la publication des paquets autonomes à l'aide des outils de la Console d'administration
- 8060 TCP : port HTTP, utilisé pour la publication des paquets autonomes à l'aide des outils de la Console d'administration
- 13292 TCP : ce port TLS est requis uniquement s'il faut administrer des appareils mobiles

Si vous devez fournir aux clients les options de base d'administration du réseau via Kaspersky Security Center Web Console, vous devez également ouvrir le port 8080 TCP (port HTTPS) de Kaspersky Security Center Web Console.

Configuration typique de Kaspersky Security Center

Un ou plusieurs Serveurs d'administration se trouvent sur les serveurs MSP. La quantité de Serveurs peut être choisie en fonction de la présence de matériel accessible, ainsi qu'en fonction du nombre de clients MSP à servir ou du total d'appareils administrés.

Un Serveur d'administration peut servir jusqu'à 100 000 appareils. Il faut prendre en considération la possibilité d'augmenter la quantité d'appareils administrés dans un proche avenir : il peut être souhaitable de connecter un peu moins d'appareils à un Serveur d'administration.

Il est possible de créer un maximum de 500 serveurs virtuels sur un Serveur d'administration et par conséquent, il faut prévoir un Serveur d'administration distinct par groupe de 500 clients MSP.

S'il existe plusieurs Serveurs, il est conseillé de les regrouper dans une hiérarchie. L'existence d'une hiérarchie de Serveurs d'administration permet d'éviter le dédoublement de stratégies et de tâches, de travailler avec tous les appareils administrés comme s'ils étaient administrés par un seul Serveur d'administration : exécuter la recherche d'appareils, créer des sélections d'appareils, créer des rapports.

Il faut désigner un ou plusieurs points de distribution sur chaque Serveur virtuel qui correspond à un client MSP. Si la communication entre les clients MSP et le Serveur d'administration s'opère via Internet, il peut être utile de créer pour les points de distribution une tâche *Télécharger les mises à jour sur les stockages des points de distribution* afin que les points de distribution téléchargent la mise à jour non pas depuis le Serveur d'administration, mais directement depuis les serveurs de Kaspersky.

Si une partie des appareils du réseau du client MSP ne dispose pas d'un accès direct à Internet, les points de distribution doivent être placés en mode de passerelle (Connection Gateway). Dans ce cas, les Agents d'administration sur les appareils sur le réseau du client MSP se connectent (pour la synchronisation) au Serveur d'administration non pas directement, mais via la passerelle.

Dans la mesure où le Serveur d'administration ne peut pas sonder le réseau du client MSP, il est préférable de confier cette fonction à un point de distribution.

Le Serveur d'administration ne peut pas envoyer les notifications sur le port 15000 UDP aux appareils administrés situés au-delà du NAT sur le réseau du client MSP. Pour résoudre ce problème, il est conseillé d'activer le mode de maintien de la connexion au Serveur d'administration dans les propriétés des appareils qui sont des points de distribution et qui fonctionnent en mode de passerelle (Connection Gateway) (case **Maintenir la connexion au Serveur d'administration**). Le mode de maintien de la connexion est accessible si le total des points de distribution n'est pas supérieur à 300.

À propos des points de distribution

Un appareil avec l'Agent d'administration installé peut servir de point de distribution. Dans ce mode, l'Agent d'administration peut exercer les fonctions suivantes :

- Transférer des fichiers vers des appareils clients, notamment :
  - Mises à jour des bases de données et des modules logiciels de Kaspersky

    Les mises à jour peuvent être obtenues à partir du Serveur d'administration ou des serveurs de mise à jour de Kaspersky. Dans ce cas, il faut créer la tâche *Télécharger les mises à jour sur les stockages des points de distribution* pour l'appareil qui fait office de point de distribution.
  - Mises à jour du logiciel tiers
  - Paquets d'installation
  - Mises à jour Windows lorsque vous utilisez le Serveur d'administration comme serveur WSUS
- Installer le logiciel sur d'autres appareils, y compris exécuter le déploiement initial des Agents d'administration sur les appareils.
- Sonder le réseau dans le but de détecter de nouveaux appareils et de mettre à jour les informations sur les appareils détectés. Un point de distribution peut exécuter les mêmes méthodes de recherche d'appareils que le Serveur d'administration.

Le déploiement de points de distribution sur le réseau de l'entreprise poursuit les buts suivants :

- Diminuer la charge du Serveur d'administration au cas où la source des mises à jour est le Serveur d'administration.
- Optimiser le trafic Internet, car, dans ce cas, chaque appareil du réseau du client MSP n'a pas besoin de contacter les serveurs de Kaspersky ni le Serveur d'administration pour les mises à jour.
- Accorder au Serveur d'administration l'accès aux appareils au-delà du NAT (par rapport au Serveur d'administration) du réseau du client MSP permet à ce Serveur de réaliser les opérations suivantes :
  - Envoyer des notifications aux appareils via UDP sur le réseau IPv4 ou IPv6
  - Sonder le réseau IPv4 ou IPv6
  - Exécuter le déploiement initial
  - Fonctionnement en tant que serveur push

Un point de distribution est assigné au groupe d'administration. Dans ce cas, la zone d'action du point de distribution reprend les appareils situés dans ce groupe d'administration et l'ensemble de ses sous-groupes. L'appareil qui fait office de point de distribution ne doit pas se trouver obligatoirement dans le groupe d'administration auquel il est attribué.

Vous pouvez faire fonctionner un point de distribution comme une passerelle de connexion. Dans ce cas, les appareils qui se trouvent dans la zone d'action de ce point de distribution se connectent au Serveur d'administration non pas directement, mais via la passerelle. Vous pouvez utiliser ce mode dans les cas où il est impossible d'établir une connexion directe entre les appareils hébergeant l'Agent d'administration et un Serveur d'administration.

Les appareils fonctionnant comme points de distribution doivent être protégés, y compris physiquement contre tout accès non autorisé.

Hiérarchie des Serveurs d'administration

Il peut y avoir plus d'un Serveur d'administration par MSP. L'administration de plusieurs serveurs hétérogènes n'est pas pratique et pour cette raison, il est utile de les regrouper dans une hiérarchie. La configuration " primaire/secondaire " entre deux Serveurs d'administration offre les possibilités suivantes :

- Le Serveur d'administration secondaire hérite des stratégies et des tâches du Serveur d'administration principal, les paramètres en double sont supprimés.
- Les sélections d'appareils sur le Serveur d'administration principal peuvent reprendre des appareils de Serveurs d'administration secondaires.
- Les rapports relatifs au Serveur d'administration principal peuvent comprendre des données (y compris des données détaillées) des Serveurs d'administration secondaires.

Le Serveur d'administration principal reçoit uniquement les données des Serveurs d'administration secondaires non virtuels qui respectent les options répertoriées ci-dessus. Cette restriction ne s'applique pas aux Serveurs d'administration virtuels qui partagent la base de données avec leur Serveur d'administration principal.

Serveurs d'administration virtuels

Il est possible de créer dans un Serveur d'administration physique plusieurs Serveurs d'administration virtuels dans une multitude de Serveurs secondaires semblables. Par rapport au modèle de partage de l'accès qui repose sur des listes de contrôle de l'accès (ACL), le modèle des Serveurs d'administration virtuels est plus pratique et permet une isolation plus poussée. Outre la structure propre des groupes d'administration pour les appareils administrés avec les stratégies et les tâches, chaque Serveur d'administration virtuel possède également son propre groupe d'appareils non définis, ses propres sélections de rapports, ses sélections d'appareils et d'événements, ses paquets d'installation, ses règles de déplacement des appareils, etc. Pour obtenir l'isolement maximal des clients MSP entre eux, il est conseillé d'utiliser la fonction des Serveurs d'administration virtuels. De plus, la création d'un Serveur d'administration virtuel pour chaque client MSP permet d'offrir aux clients des possibilités de base en matière d'administration de son réseau à l'aide de Kaspersky Security Center Web Console.

Les Serveurs d'administration virtuels ressemblent en de nombreux points aux Serveurs d'administration secondaires, mais ils possèdent les différences suivantes :

- Le Serveur d'administration virtuel ne possède pas la plupart des paramètres globaux, ni ses propres ports TCP.
- Le Serveur d'administration virtuel ne peut pas avoir de serveurs secondaires.

- Le Serveur d'administration virtuel ne peut pas avoir ses propres serveurs virtuels.
- le Serveur d'administration physique présente les appareils, les groupes, les événements et les objets des appareils administrés (éléments de la quarantaine, registre des applications, etc.) de l'ensemble de ses Serveurs virtuels.
- Le Serveur d'administration virtuel peut analyser le réseau uniquement à l'aide des points de distribution qui y sont connectés.

Administration des appareils mobiles dotés de Kaspersky Endpoint Security for Android

L'administration des appareils mobiles dotés de Kaspersky Endpoint Security for Android™ (ci-après les appareils KES) s'opère via le Serveur d'administration. Kaspersky Security Center est compatible avec les fonctions suivantes d'administration des appareils KES :

- utilisation des appareils mobiles comme des appareil clients :
  - appartenance aux groupes d'administration
  - Surveillance, par exemple concernant l'affichage des statuts, des événements et des rapports
  - modification des paramètres locaux et désignation de stratégies pour l'application Kaspersky Endpoint Security for Android
- envoi centralisé de commandes
- installation à distance de paquets des applications mobiles.

Le Serveur d'administration gère les appareils KES via TLS, port TCP 13292.

Déploiement et configuration initiale

Kaspersky Security Center est une application distribuée. Kaspersky Security Center contient les applications suivantes :

- Le Serveur d'administration est le module central responsable de l'administration des appareils de l'entreprise et de la conservation des données dans le SGBD.
- La Console d'administration est l'outil principal de l'administrateur. La Console d'administration est livrée avec le Serveur d'administration, mais peut être également installée séparément sur un ou plusieurs appareils de l'administrateur.
- Kaspersky Security Center Web Console : l'interface Internet du Serveur d'administration qui permet de réaliser les tâches les plus simples. Vous pouvez installer ce composant sur tout appareil conforme aux critères de Configuration matérielle et logicielle requise.
- L'Agent d'administration intervient dans l'administration de l'application de sécurité installée sur l'appareil, ainsi que dans l'obtention d'informations sur l'appareil. Les Agents d'administration s'installent sur les appareils de l'entreprise.

Le déploiement de Kaspersky Security Center dans le réseau de l'entreprise se réalise comme suit :

- Installation du Serveur d'administration
- Installation de Kaspersky Security Center Web Console
- Installation de la Console d'administration sur l'appareil de l'administrateur
- Installation de l'Agent d'administration et de l'application de sécurité sur les appareils de l'organisation

Recommandations d'installation du Serveur d'administration

Cette section contient des recommandations sur l'installation du Serveur d'administration. La section contient aussi des scénarios d'utilisation du dossier partagé sur l'appareil doté du Serveur d'administration en vue du déploiement de l'Agent d'administration sur les appareils clients.

Création des comptes utilisateurs pour les services du Serveur d'administration sur un cluster haute disponibilité

Par défaut, le programme d'installation crée lui-même des comptes utilisateurs sans privilèges pour les services du Serveur d'administration. Ce comportement est parfaitement adapté à l'installation du Serveur d'administration sur un appareil normal.

Cependant, en cas d'installation du Serveur d'administration sur un cluster haute disponibilité, il faut procéder différemment :

1. Créer des comptes utilisateurs de domaine sans privilèges pour les services du Serveur d'administration et les ajouter au groupe de sécurité de domaine global KLAdmins.
2. Définir dans le programme d'installation du Serveur d'administration les comptes utilisateurs de domaine créés.

Choix d'un SGBD

Au moment de choisir un SGBD qui va être utilisé par le Serveur d'administration, il faut tenir compte du nombre d'appareils desservis par le Serveur d'administration.

Le tableau suivant répertorie les options de SGBD valides, ainsi que les recommandations et restrictions relatives à leur utilisation.

SGBD	Recommandations et restrictions
SQL Server Express Edition 2016 et suivante	Utilisez ce SGBD si vous prévoyez d'utiliser un seul Serveur d'administration pour moins de 10 000 appareils. Il est recommandé de désactiver la tâche Inventaire des logiciels et de désactiver (dans les paramètres de stratégie Kaspersky Endpoint Security) les notifications du Serveur d'administration sur les applications lancées. Vous pouvez limiter le nombre d'événements dans le stockage d'événements pour éviter un débordement de base de données. Pour plus de détails, reportez-vous à la section suivante : Calcul de l'espace disponible dans la base de données. L'utilisation conjointe du SGBD Server Express Edition par le Serveur d'administration et une autre application est strictement interdite. La base de données Microsoft SQL Express n'est pas prise en charge pour la tâche **Synchronisation des mises à jour Windows Update**.
SQL Server Edition local, différent d'Express. 2016 et suivante	Pas de restrictions.
SQL Server Edition distant, différent d'Express, 2016 et suivante	Valide uniquement si les deux appareils se trouvent dans le même domaine Windows® ; si les domaines diffèrent, il faut établir une relation de confiance bilatérale entre eux.
MySQL 5.5, 5.6 ou 5.7 local ou distant (les versions MySQL 5.5.1, 5.5.2, 5.5.3, 5.5.4 et 5.5.5 ne sont plus prises en charge)	Utilisez ce SGBD si vous prévoyez d'utiliser un seul Serveur d'administration pour moins de 10 000 appareils. Il est recommandé de désactiver la tâche Inventaire des logiciels et de désactiver (dans les paramètres de stratégie Kaspersky Endpoint Security) les notifications du Serveur d'administration sur les applications lancées. Pour plus de détails, reportez-vous à la section suivante : Calcul de l'espace disponible dans la base de données.
MySQL local ou distant 8.0.20 ou version ultérieure	Utilisez ce SGBD si vous prévoyez d'utiliser un seul Serveur d'administration pour moins de 50 000 appareils. Il est recommandé de désactiver la tâche Inventaire des logiciels et de désactiver (dans les paramètres de stratégie Kaspersky Endpoint Security) les notifications du Serveur d'administration sur les applications lancées. Pour plus de détails, reportez-vous à la section suivante : Calcul de l'espace disponible dans la base de données.
MariaDB locale ou distante (voir les versions prises en charge)	Utilisez ce SGBD si vous prévoyez d'utiliser un seul Serveur d'administration pour moins de 20 000 appareils. Il est recommandé de désactiver la tâche Inventaire des logiciels et de désactiver (dans les paramètres de stratégie Kaspersky Endpoint Security) les notifications du Serveur d'administration sur les applications lancées. Pour plus de détails, reportez-vous à la section suivante : Calcul de l'espace disponible dans la base de données.
PostgreSQL, Postgres Pro (cf. les versions compatibles)	Utilisez l'un de ces SGBD si vous prévoyez d'utiliser un seul Serveur d'administration pour moins de 50 000 appareils. Il est recommandé de désactiver la tâche Inventaire des logiciels et de désactiver (dans les paramètres de stratégie Kaspersky Endpoint Security) les notifications du Serveur d'administration sur les applications lancées. Pour plus de détails, reportez-vous à la section suivante : Calcul de l'espace disponible dans la base de données.

Si vous utilisez un SGBD PostgreSQL, MariaDB ou MySQL, l'onglet **Événements** peut afficher une liste incomplète des événements pour l'appareil client sélectionné. Cette situation se produit lorsque le SGBD stocke un très grand nombre d'événements. Vous pouvez augmenter le nombre d'événements affichés d'une des manières suivantes :

- Suppression des événements inutiles.
- Réduction de la durée de conservation des événements inutiles.

Pour consulter la liste complète des événements enregistrés sur le Serveur d'administration pour l'appareil, accédez à Rapports.

Si vous utilisez SQL Server 2019 en tant que SGBD et vous n'avez pas de correctif cumulatif CU12 ou ultérieur, vous devez effectuer les opérations suivantes après d'installer Kaspersky Security Center :

1. Connectez-vous à SQL Server à l'aide de SQL Management Studio.
2. Exécutez les commandes suivantes (si vous avez choisi un nom différent pour la base de données, utilisez ce nom au lieu de KAV) :

   ```
   USE KAV
   GO
   ALTER DATABASE SCOPED CONFIGURATION SET TSQL_SCALAR_UDF_INLINING = OFF
   GO
   ```

3. Redémarrez le service SQL Server 2019.

Sinon, l'utilisation de SQL Server 2019 peut entraîner des erreurs, telles que « la mémoire système est insuffisante dans le pool de ressources 'interne' pour exécuter cette requête ».

Indication de l'adresse du Serveur d'administration

Lors de l'installation du Serveur d'administration, il faut indiquer l'adresse externe du Serveur d'administration. Cette adresse est utilisée par défaut lors de la création des paquets d'installation de l'Agent d'administration. L'adresse du Serveur d'administration peut être modifiée par la suite à l'aide des outils de la Console d'administration, toutefois dans ce cas elle n'est pas modifiée automatiquement dans les paquets d'installation de l'Agent d'administration déjà créés.

Configuration de la protection sur le réseau d'une entreprise cliente

Après la fin de l'installation du Serveur d'administration, la Console d'administration, qui permet de réaliser la configuration initiale à l'aide d'un Assistant, démarre. L'Assistant de configuration initiale de l'application crée dans le groupe d'administration racine les stratégies et tâches suivantes :

- La stratégie de Kaspersky Endpoint Security
- La tâche de groupe de mise à jour de Kaspersky Endpoint Security
- La tâche de groupe d'analyse de l'appareil de Kaspersky Endpoint Security
- La stratégie de l'Agent d'administration
- La tâche de recherche de vulnérabilités (tâche de l'Agent d'administration)
- La tâche de l'installation des mises à jour et de correction des vulnérabilités (tâche de l'Agent d'administration)

Les stratégies et les tâches adoptent les paramètres par défaut qui ne sont pas forcément parfaits ou adaptés à la société en question. C'est pourquoi il faut consulter les propriétés des objets créés et, le cas échéant, introduire des modifications manuellement.

Cette section fournit des informations sur la configuration manuelle des stratégies, des tâches et d'autres paramètres du Serveur d'administration ainsi que des informations sur les points de distribution, l'élaboration de la structure des groupes d'administration, sur les hiérarchies de tâches et sur d'autres paramètres.

Configuration manuelle d'une stratégie de Kaspersky Endpoint Security

Cette section fournit des recommandations sur la configuration de la stratégie de Kaspersky Endpoint Security créée par l'Assistant de configuration initiale de l'application. Vous pouvez effectuer la configuration dans la fenêtre des propriétés de la stratégie.

En cas de modification d'un paramètre, il convient de cliquer sur le bouton avec le cadenas au-dessus du paramètre pour que la valeur du paramètre soit appliquée sur le poste de travail.

Configuration de la stratégie dans la section Protection avancée

Pour obtenir une description complète des paramètres dans cette section, veuillez consulter la documentation de Kaspersky Endpoint Security for Windows.

Dans la section **Protection avancée**, vous pouvez configurer l'utilisation de Kaspersky Security Network pour Kaspersky Endpoint Security for Windows. Vous pouvez également configurer les modules de Kaspersky Endpoint Security for Windows, tels que Détection comportementale, Protection contre les exploits, Prévention des intrusions et Réparation des actions malicieuses.

Dans la sous-section **Kaspersky Security Network**, nous vous recommandons d'activer l'option **Kaspersky Security Network**. L'utilisation de cette option aide à rediffuser et optimiser le trafic sur le réseau. Si l'option **Kaspersky Security Network** est désactivée, vous pouvez activer l'utilisation directe des serveurs KSN.

Configuration de la stratégie dans la section Protection principale

Pour obtenir une description complète des paramètres dans cette section, veuillez consulter la documentation de Kaspersky Endpoint Security for Windows.

Dans la section **Protection principale** de la fenêtre des propriétés de la stratégie, nous vous recommandons de définir des paramètres supplémentaires dans les sous-sections **Pare-feu** et **Protection contre les fichiers malicieux**.

La sous-section **Pare-feu** contient les paramètres qui vous permettent de contrôler l'activité réseau des applications sur les appareils clients. Un appareil client utilise un réseau auquel l'un des états suivants est attribué : public, local ou de confiance. Selon l'état du réseau, Kaspersky Endpoint Security peut autoriser ou interdire l'activité réseau sur un appareil. Lorsque vous ajoutez un nouveau réseau à votre organisation, vous devez lui attribuer un état de réseau approprié. Par exemple, si l'appareil client est un ordinateur portable, nous recommandons que cet appareil utilise le réseau public ou de confiance, car l'ordinateur portable n'est pas toujours connecté au réseau local. Dans la sous-section **Pare-feu**, vous pouvez vérifier si vous avez correctement attribué des états aux réseaux utilisés dans votre organisation.

Pour vérifier la liste des réseaux, procédez comme suit :

1. Dans les propriétés de la stratégie, accédez à **Protection principale → Pare-feu**.
2. Dans le groupe **Réseaux disponibles**, cliquez sur le bouton **Paramètres**.
3. Dans la fenêtre **Pare-feu** qui s'ouvre, accédez à l'onglet **Réseaux** pour consulter la liste des réseaux.

La sous-section **Protection contre les fichiers malicieux** permet de désactiver l'analyse des disques réseau. L'analyse des disques réseau peut placer une charge importante sur les disques réseau. Il est préférable de réaliser l'analyse directement sur les serveurs de fichiers.

Pour désactiver l'analyse des disques réseau, procédez comme suit :

1. Dans les propriétés de la stratégie, accédez à **Protection principale → Protection contre les fichiers malicieux**.
2. Dans le groupe **Niveau de sécurité**, cliquez sur le bouton **Paramètres**.
3. Dans la fenêtre **Protection contre les fichiers malicieux** qui s'ouvre, accédez à l'onglet **Général** et décochez la case **Tous les disques réseau**.

Configuration de la stratégie dans la section Paramètres généraux

Pour obtenir la description complète des paramètres dans cette section, veuillez consulter la documentation de Kaspersky Endpoint Security.

Ci-après, les actions de configuration avancée que nous vous recommandons d'effectuer dans la fenêtre des propriétés de la stratégie de Kaspersky Endpoint Security, dans la section **Paramètres généraux**.

Section Paramètres généraux, sous-section Rapports et stockage

Dans la section **Transfert des données vers le Serveur d'administration**, veuillez cocher la case **À propos des applications lancées**. Si cette case est cochée, la base de données du Serveur d'administration enregistre les informations relatives à toutes les versions de tous les modules logiciels sur les appareils dans le réseau. Les informations indiquées peuvent prendre un espace considérable dans la base de données de Kaspersky Security Center (des dizaines de gigaoctets). Par conséquent, si la case **À propos des applications lancées** est toujours cochée dans la stratégie de niveau supérieur, elle doit être décochée.

Section Paramètres généraux, sous-section Interface

Si la protection contre les menaces du réseau de l'entreprise doit être gérée en mode centralisé via la Console d'administration, il faut désactiver l'affichage de l'interface utilisateur de Kaspersky Endpoint Security sur les postes de travail (en décochant la case **Afficher l'interface de l'application** dans la section **Interaction avec l'utilisateur**) et activez la protection par mot de passe (en cochant la case **Activer la protection par mot de passe** dans la section **Protection par mot de passe**).

Configuration de la stratégie dans la section Configuration d'événement

Il faut désactiver, dans la section **Configuration de l'événement**, la conservation de tous les événements sur le Serveur d'administration, à l'exception des événements ci-après :

- Sous l'onglet **Critique** :
  - *Le lancement automatique de l'application est désactivé*
  - *Accès interdit*
  - *Le lancement de l'application est interdit*
  - *Désinfection impossible*
  - *Contrat de licence utilisateur final violé*
  - *Impossible de charger le module de chiffrement*
  - *Impossible de lancer deux tâches simultanément*
  - *Une menace active a été détectée. Il faut lancer la procédure de désinfection avancée*
  - *Une attaque réseau a été détectée*
  - *Certains modules n'ont pas été mis à jour*
  - *Erreur d'activation*
  - *Erreur d'activation du mode portable*
  - *Erreur d'interaction avec Kaspersky Security Center*
  - *Erreur de désactivation du mode portable*
  - *Erreur de modification de la sélection de modules de l'application*
  - *Erreur d'application des règles de chiffrement/déchiffrement des fichiers*
  - *La stratégie ne peut pas être appliquée*
  - *Le processus est terminé*
  - *L'activité réseau est interdite*
- Dans l'onglet **Erreur de fonctionnement** : *Erreur dans les paramètres de la tâche. Les paramètres ne sont pas appliqués*

- Sous l'onglet **Avertissement** :
  - *L'Autodéfense de l'application est désactivée*
  - *La clé de réserve est incorrecte*
  - *L'utilisateur a refusé la stratégie de chiffrement*
- Sous l'onglet **Information** : *Le lancement de l'application est interdit en mode test*

Configuration manuelle d'une tâche de groupe de mise à jour de Kaspersky Endpoint Security

Si le Serveur d'administration est la source des mises à jour, pour les tâches de groupe de mise à jour de Kaspersky Endpoint Security, la programmation optimale et recommandée est **Lors du téléchargement des mises à jour dans le stockage** si la case **Utiliser un délai aléatoire automatique pour le démarrage des tâches** est cochée.

Si une tâche de téléchargement des mises à jour dans le stockage depuis les serveurs de Kaspersky est créée sur chaque point de distribution, la solution optimale recommandée pour la tâche de groupe de mise à jour de Kaspersky Endpoint Security est la planification périodique. Dans ce cas, la valeur de l'intervalle aléatoire doit être réglée sur 1 heure.

Configuration manuelle d'une tâche de groupe d'analyse de l'appareil de Kaspersky Endpoint Security

L'Assistant de configuration initiale de l'application crée la tâche de groupe d'analyse d'un appareil. La programmation par défaut de la tâche est **Lancer tous les vendredi à 19:00** avec allocation aléatoire automatique et la case **Lancer les tâches non exécutées** est décochée.

Cela signifie que si les appareils de la société sont désactivés le vendredi à 18h30, la tâche d'analyse de l'appareil ne sera jamais lancée. Il faut configurer une programmation optimale de cette tâche sur la base du règlement de travail adopté par la société.

Planification de la tâche Recherche de vulnérabilités et des mises à jour requises

L'Assistant de configuration initiale de l'application crée une tâche *Recherche de vulnérabilités et de mises à jour requises* pour l'Agent d'administration. Par défaut, la programmation choisie pour cette tâche est **Lancer tous les mardi à 19:00** avec randomisation automatique et la case **Lancer les tâches non exécutées** est cochée.

Si le règlement de travail de la société prévoit la désactivation des appareils à ce moment, la tâche *Recherche de vulnérabilités et de mises à jour requises* est lancée après l'activation de l'appareil (le mercredi matin). Ce comportement est à éviter car la recherche de vulnérabilités peut augmenter la charge sur le processeur et le sous-système de disque de l'appareil. Vous devez configurer une programmation optimale de cette tâche sur la base du règlement de travail adopté par l'entreprise.

Configuration manuelle d'une tâche de groupe d'installation des mises à jour et de correction des vulnérabilités

L'Assistant de configuration initiale de l'application crée une tâche de groupe d'installation des mises à jour et de recherche de vulnérabilités pour l'Agent d'administration. Par défaut, le lancement de la tâche est prévu chaque jour à 1:00 avec allocation aléatoire automatique, et l'option **Lancer les tâches non exécutées** n'est pas activée.

Si le règlement de travail de la société prévoit la désactivation des appareils pendant la nuit, la tâche d'installation des mises à jour ne sera jamais exécutée. Il faut définir le calendrier optimum de la tâche de recherche de vulnérabilités sur la base du règlement de travail en vigueur dans la société. De plus, il ne faut pas oublier que l'installation des mises à jour peut requérir le redémarrage de l'appareil.

Élaboration de la structure de groupes d'administration et désignation des points de distribution

La structure des groupes d'administration dans Kaspersky Security Center exerce les fonctions suivantes :

- Désignation de la zone d'action des stratégies.

  Il existe une autre méthode d'application des paramètres nécessaires sur les appareils : le recours aux profils de stratégie. Dans ce cas, la zone d'action des stratégies est définie, par exemple, à l'aide de tags, de l'emplacement des appareils dans les sous-divisions Active Directory et de l'appartenance aux groupes de sécurité Active Directory.

- Désignation de la zone d'action des tâches de groupe.

  Il y existe une méthode de désignation de la zone d'action des tâches de groupe qui ne repose pas sur la hiérarchie des groupes d'administration : l'utilisation de tâche pour des sélections d'appareils et des ensembles d'appareils.

- Désignation des privilèges d'accès aux appareils et aux Serveurs d'administration secondaires et virtuels.

- Ceci assigne les points de distribution.

Lors de la mise en place de la structure de groupes d'administration, il faut prendre en considération la topologie du réseau de l'entreprise pour garantir la désignation optimale des points de distribution. La distribution optimale des points de distribution permet de diminuer le trafic réseau à l'intérieur du réseau de l'entreprise.

En fonction de la structure organisationnelle du client MSP et de la topologie des réseaux, les configurations typiques suivantes de structure des groupes d'administration existent :

- Un bureau

- Plusieurs petits bureaux isolés

Configuration standard d'un client MSP : un bureau

Dans la configuration typique " un bureau ", tous les appareils se trouvent sur le réseau de l'entreprise et se " voient ". Le réseau de l'entreprise peut comprendre plusieurs " parties " mises en évidence (des réseaux ou des segments de réseau) et reliées par des canaux étroits.

Les moyens suivants de construction de la structure de groupes d'administration existent :

- Construction de la structure des groupes d'administration en tenant compte de la topologie du réseau. La structure des groupes d'administration ne doit pas obligatoirement refléter exactement la topologie du réseau. Il suffit que quelques groupes d'administration correspondent à des parties du réseau mises en évidence. Les points de distribution peuvent être désignés automatiquement ou manuellement.

- Construction de la structure des groupes d'administration qui ne reflète pas la topologie du réseau. Dans ce cas, il faut désactiver la désignation automatique des points de distribution et désigner dans chaque partie du réseau mise en évidence un ou plusieurs appareils en tant que points de distribution sur le groupe d'administration racine, par exemple, sur le groupe **Appareils administrés**. Tous les points de distribution se trouvent au même niveau et possèdent la même zone d'action, à savoir tous les appareils du réseau de l'entreprise. Chaque Agent d'administration se connecte dans ce cas au point de distribution qui possède l'itinéraire le plus court. L'utilitaire tracert permet de définir l'itinéraire d'accès au point de distribution.

Configuration standard d'un client MSP : plusieurs petits bureaux isolés

Cette configuration typique correspond à plusieurs petits bureaux distants, potentiellement connectés au siège principal via Internet. Chacun de ces bureaux distants se trouve au-delà du NAT. Autrement dit, la connexion d'un bureau distant à un autre est impossible. Ils sont isolés.

La configuration doit absolument se refléter dans la structure des groupes d'administration : pour chacun des bureaux distants. il faut créer un groupe d'administration distinct (les groupes **Bureau 1**, **Bureau 2** sur l'illustration ci-après).

Bureaux distants affichés dans la structure des groupes d'administration

Sur chaque groupe d'administration correspondant à un bureau, il faut désigner un ou plusieurs points de distribution. Les points de distribution doivent être des appareils du bureau distant dotés d'espace suffisant sur le disque. Ainsi, les appareils qui se trouvent par exemple dans le groupe **Bureau 1** vont contacter les points de distribution assignés au groupe d'administration **Bureau 1**.

Si certains utilisateurs se déplacent d'un bureau à l'autre avec des ordinateurs portables, il faut sélectionner dans chaque bureau distant, en plus des points de distribution cités ci-dessus, deux ou plusieurs appareils et les assigner comme points de distribution pour le groupe d'administration de niveau supérieur (le groupe **Groupe racine pour les bureaux** dans l'illustration ci-dessus).

Exemple : Par exemple, voici un ordinateur portable qui se trouve dans le groupe d'administration **Bureau 1**, mais qui est déplacé physiquement dans le bureau qui correspond au groupe **Bureau 2**. Après le déplacement, l'Agent d'administration sur l'ordinateur portable tente de contacter les points de distribution assignés au groupe **Bureau 1**, mais ceux-ci ne sont pas accessibles. Alors l'Agent d'administration commence à contacter les points de distribution désignés pour le groupe **Groupe racine pour les bureaux**. Étant donné que les bureaux distants sont isolés les uns des autres, seules les requêtes d'accès aux points de distribution assignés au groupe d'administration **Groupe racine pour les bureaux** aboutissent lorsque l'Agent d'administration tente d'accéder aux points de distribution dans le groupe **Bureau 2**. Autrement dit, l'ordinateur portable demeure dans le groupe d'administration qui correspond à son bureau d'origine, mais il utilise malgré tout le point de distribution du bureau où il se trouve physiquement à l'heure actuelle.

Hiérarchie des stratégies, utilisation des profils de stratégie

Cette section contient des informations sur les particularités de l'application de stratégies aux appareils dans les groupes d'administration. Cette section fournit également des informations sur les profils de stratégie.

Hiérarchie des stratégies

Dans Kaspersky Security Center, les stratégies servent à appliquer un ensemble de valeurs de paramètres identiques à plusieurs appareils. Par exemple, la zone d'action de la stratégie de l'application A définie pour le groupe G reprend les appareils administrés dotés de l'application A et situés dans le groupe d'administration G et l'ensemble de ses sous-groupes, à l'exception des sous-groupes dans les propriétés desquels la case **Hériter du groupe parent** est décochée.

La stratégie se distingue des paramètres locaux par la présence de cadenas (🔒) en regard des paramètres qu'elle contient. Un cadenas fermé dans les propriétés de la stratégie signifie que le paramètre (ou le groupe de paramètres) correspondant doit, premièrement, être utilisé dans la composition des paramètres effectifs et, deuxièmement, être inscrit dans la stratégie de niveau inférieur.

La définition des paramètres actifs sur l'appareil peut être représentée de la manière suivante : les valeurs des paramètres sans " cadenas " sont tirées de la stratégie, elles sont écrasées par les valeurs des paramètres locaux, puis les valeurs récupérées sont écrasées par les valeurs des paramètres avec cadenas extraites de la stratégie.

Les stratégies d'une même application agissent les unes sur les autres en fonction de la hiérarchie des groupes d'administration : les paramètres avec cadenas fermé de la stratégie supérieure sont appliqués aux paramètres du même nom de la stratégie inférieure.

Il existe un type particulier de stratégie : la stratégie pour les utilisateurs itinérants. Cette stratégie entre en vigueur sur l'appareil quand celui-ci passe au mode de l'utilisateur autonome. Les stratégies pour les utilisateurs autonomes n'agissent pas sur les autres stratégies selon la hiérarchie des groupes d'administration.

Profils de stratégie

Dans de nombreux cas, l'application de stratégies à des appareils sur la seule base de la hiérarchie des groupes d'administration n'est pas pratique. La nécessité de créer plusieurs copies de stratégies, qui se distinguent par un ou deux paramètres, dans différents groupes d'administration peut se présenter, avec la synchronisation manuelle ultérieure du contenu de ces stratégies.

Pour éviter ce type de problèmes, Kaspersky Security Center prend en charge les *profils de stratégie*. Un profil de stratégie est un sous-ensemble nommé de paramètres de stratégie. Ce sous-ensemble est diffusé sur les appareils avec la stratégie et vient compléter la stratégie quand une condition définie, la *condition d'activation du profil*, est remplie. Les profils contiennent uniquement les paramètres qui se distinguent de la stratégie " de base " en vigueur sur l'appareil client (ordinateur, appareil mobile). Quand le profil est activé, les paramètres de la stratégie en vigueur sur l'appareil avant l'activation du profil sont modifiés. Ces paramètres prennent alors les valeurs reprises dans le profil.

Les profils de stratégie possèdent maintenant les restrictions suivantes :

- Une stratégie ne peut pas compter plus de 100 profils.
- Un profil de stratégie ne peut pas contenir d'autres profils.
- Un profil de stratégie ne peut pas contenir des paramètres de notification.

Composition d'un profil

Un profil de stratégie contient les parties suivantes :

- Nom. Les profils qui portent le même nom agissent les uns sur les autres selon la hiérarchie des groupes d'administration avec des règles générales.
- Sous-ensemble de paramètres d'une stratégie. À la différence d'une stratégie qui contient tous les paramètres, un profil reprend uniquement les paramètres qui sont vraiment nécessaires (le cadenas est activé).
- La condition d'activation est une expression logique avec les propriétés de l'appareil. Le profil est actif (complète la stratégie) uniquement quand la condition d'activation du profil se vérifie. Dans les autres cas, le profil est inactif et est ignoré. Les propriétés suivantes de l'appareil peuvent intervenir dans l'expression logique :
  - état du mode de l'utilisateur autonome ;
  - propriétés de l'environnement réseau : nom de la règle active de connexion de l'Agent d'administration ;
  - présence ou absence sur l'appareil des tags indiqués ;
  - emplacement de l'appareil dans les sous-divisions Active Directory : explicite (l'appareil se trouve directement dans la sous-division indiquée) ou implicite (l'appareil se trouve dans la sous-division qui se trouve à l'intérieur de la sous-division indiquée à n'importe quel niveau d'imbrication) ;
  - appartenance de l'appareil au groupe de sécurité Active Directory (explicite ou implicite) ;
  - appartenance du propriétaire de l'appareil au groupe de sécurité Active Directory (explicite ou implicite).
- Case de désactivation du profil. Les profils désactivés sont toujours ignorés, les conditions d'activation ne sont pas vérifiées.
- Priorité du profil. Les conditions d'activation des profils sont indépendantes, c'est pourquoi plusieurs profils peuvent s'activer simultanément. Si les profils actifs contiennent les ensembles de paramètres qui ne se recoupent pas, aucun problème ne se présente. Mais si deux profils actifs contiennent des valeurs différentes pour un même paramètre, il y a une ambiguïté. L'ambiguïté se résout à l'aide des priorités des profils : la valeur adoptée dans ce cas est celle du profil qui affiche la priorité supérieure (le profil qui se trouve plus haut dans la liste des profils).

Comportement des profils dans le cadre de l'action des stratégies les unes sur les autres selon la hiérarchie

Les profils homonymes sont rassemblés selon les règles du groupement de stratégies. Les profils de stratégie supérieure ont une priorité supérieure à celle des profils de la stratégie inférieure. Si la modification des paramètres est interdite (cadenas activé) dans la stratégie supérieure, la stratégie inférieure utilise les conditions d'activation de la stratégie supérieure. Si la modification des paramètres est autorisée dans la stratégie supérieure, ce sont les conditions d'activation du profil de stratégie inférieure qui sont utilisées.

Puisque le profil de stratégie peut contenir la propriété **Appareil en mode déconnecté** dans la condition de l'activation, les profils remplacent complètement la fonction des stratégies pour les utilisateurs itinérants qui ne va plus être prise en charge à l'avenir.

La stratégie pour les utilisateurs itinérants peut contenir des profils, mais l'activation de ses profils ne peut pas se produire avant que l'appareil ne passe au mode de l'utilisateur autonome.

Tâches

Kaspersky Security Center gère le fonctionnement des protection applications Kaspersky installées sur les appareils par la création et l'exécution des *tâches*. Les tâches permettent d'exécuter l'installation, le lancement et l'arrêt des applications, l'analyse des fichiers, la mise à jour des bases de données et des modules des applications, les autres actions avec les applications.

Des tâches pour une application définie peuvent être créées uniquement si le plug-in d'administration pour cette application est installé.

Les tâches peuvent être exécutées sur le Sur le Serveur d'administration et sur les appareils.

Tâches exécutées sur le Serveur d'administration :

- Diffusion automatique des rapports
- Téléchargement des mises à jour dans le stockage du Serveur d'administration
- Sauvegarde des données du Serveur d'administration
- Maintenance de la base de données
- Synchronisation de Windows Update
- Création du paquet d'installation sur la base de l'image du système d'exploitation de l'appareil de référence

Les types de tâche suivants sont réalisés sur les appareils :

- *Tâches* exécutées sur un appareil particulier

  Les tâches locales peuvent être modifiées non seulement par l'administrateur via la Console d'administration, mais aussi par l'utilisateur de l'appareil distant (par exemple, dans l'interface de l'application de sécurité). Si la tâche locale a été modifiée simultanément par l'administrateur et l'utilisateur sur l'appareil administré, ce sont les modifications introduites par l'administrateur qui sont retenues car elles ont une priorité supérieure.

- *Tâches de groupe* : tâches qui sont réalisées sur tous les appareils d'un groupe particulier

  Sauf indication contraire dans les propriétés de la tâche, une tâche de groupe peut également avoir un impact sur les sous-groupes du groupe sélectionné. Une tâche de groupe agit aussi (de manière facultative) sur les appareils connectés aux Serveurs d'administration virtuels et secondaires placés dans ce groupe et ses sous-groupes.

- *Tâches* — Tâches exécutées sur les appareils un ensemble de peu importe leur inclusion dans les groupes d'administration.

Pour chaque application vous pouvez créer n'importe quel nombre de tâches de groupe, de tâches globales et des tâches locales.

Vous pouvez modifier les paramètres des tâches en l'exécution des tâches, copier, exporter ou importer, ainsi que supprimer les Tâches.

Les tâches ne sont lancées sur un appareil que lorsque l'application pour laquelle les tâches ont été créées est lancée.

Les résultats des tâches sont enregistrés dans les journaux des événements Microsoft Windows et Kaspersky Security Center d'une manière centralisée sur le Serveur d'administration et d'une manière locale sur chaque appareil.

N'incluez pas de données confidentielles dans les paramètres des tâches. Par exemple, le mot de passe de l'administrateur de domaine.

Règles de déplacement des appareils

Il est utile d'automatiser le placement des appareils dans des groupes d'administration sur le serveur virtuel qui correspond au client MSP à l'aide de *règles de déplacement des appareils*. Une règle de déplacement contient trois parties principales : le nom, la condition d'exécution (l'expression logique sur les attributs de l'appareil) et le groupe d'administration cible. La règle déplace l'appareil dans le groupe d'administration cible si les attributs de l'appareils répondent à la condition d'exécution de la règle.

Les règles de déplacement des appareils ont des priorités. Le Serveur d'administration analyse les attributs de l'appareil pour voir s'ils sont conformes à la condition d'exécution de chaque règle, selon la priorité décroissante des règles. Si les attributs de l'appareil satisfont à la condition d'exécution de la règle, l'appareil est déplacé vers le groupe cible et le traitement des règles pour cet appareil cesse. Si les attributs de l'appareil satisfont directement à plusieurs règles, l'appareil est placé dans le groupe cible de la règle qui affiche la priorité la plus élevée (la règle qui figure plus haut dans la liste).

Les règles de déplacement des appareils peuvent être créées de manière implicite. Par exemple, les propriétés d'un paquet ou d'une tâche d'installation à distance peuvent contenir un groupe d'administration qui va accueillir un appareil après l'installation sur celui-ci d'un Agent d'administration. De même, l'administrateur de Kaspersky Security Center peut créer des règles de déplacement de manière explicite dans la liste des règles de déplacement. La liste se trouve dans la Console d'administration, dans les propriétés du groupe **Appareils non définis**.

La règle de déplacement par défaut est prévue pour le déplacement initial et ponctuel des appareils dans les groupes d'administration. La règle déplace une seule fois les appareils qui se trouvent dans le groupe **Appareils non définis**. Si l'appareil a déjà été déplacé une fois par cette règle, celle-ci ne le déplacera pas à nouveau, même si l'appareil est replacé manuellement dans le groupe **Appareils non définis**. C'est le moyen recommandé pour l'utilisation des règles de déplacement.

Il est possible de déplacer des appareils qui se trouvent déjà dans des groupes d'administration. Pour cela, il faut décocher la case **Déplacer uniquement les appareils non inclus dans un groupe d'administration** dans les propriétés de la règle.

La présence de règles de déplacement qui agissent sur des appareils qui figurent déjà dans des groupes d'administration augmente sensiblement la charge sur le Serveur d'administration.

Il est possible de créer une règle de déplacement qui peut agir à plusieurs reprises sur le même appareil.

Il est vivement conseillé d'éviter d'adopter une démarche de manipulation des appareils administrés dans le cadre de laquelle le même appareil est déplacé à plusieurs reprises d'un groupe vers un autre, par exemple pour appliquer une stratégie particulière à l'appareil, pour lancer une tâche de groupe spéciale ou réaliser une mise à jour depuis un point de distribution défini.

Ces scénarios ne sont pas pris en charge car ils ne sont pas efficaces en termes de charge sur le Serveur d'administration et de trafic réseau. De plus, ils sont en contradiction avec les modèles de fonctionnement de Kaspersky Security Center (surtout au niveau des privilèges d'accès, des événements et des rapports). Il faut trouver une autre solution, par exemple utiliser des profils de stratégies, des tâches pour des sélections d'appareils, désigner des agents de mises à Réseau conformément à la méthode, etc.

Catégorisation du logiciel

La méthode principale pour contrôler le lancement des applications repose sur les *catégories de Kaspersky* (ci-après, les *catégories KL*). Les catégories KL simplifient la tâche de l'administrateur de Kaspersky Security Center au niveau de la maintenance des catégories d'applications et réduisent le volume de trafic transmis aux appareils administrés.

Créez des catégories utilisateur uniquement pour les applications qui ne correspondent à aucune des catégories KL (par exemple une application développée sur mesure). Les catégories utilisateur sont créées sur la base d'un paquet d'installation (MSI) ou sur la base du dossier contenant les paquets d'installation.

S'il existe une grande collection à enrichir de logiciels qui ne sont pas classés selon les catégories KL, il peut être utile de créer une catégorie mise à jour automatiquement. Cette catégorie s'enrichit automatiquement des sommes de contrôle des fichiers exécutable lors de la modification du dossier contenant les distributions.

Ne créez pas des catégories d'applications mises à jour automatiquement pour les dossiers Mes documents, %windir%, %ProgramFiles% et %ProgramFiles(x86)%. Les fichiers dans ces dossiers changent souvent, ce qui augmente la charge sur le Serveur d'administration et le trafic dans le réseau. Il faut créer un dossier séparé contenant la collection de logiciels et l'enrichir de temps à autre.

À propos des applications multilocataires

Kaspersky Security Center permet aux administrateurs de fournisseurs de services et aux administrateurs de locataires d'utiliser des applications de Kaspersky qui prennent en charge plusieurs entités. Après l'installation d'une application Kaspersky multilocataires dans l'infrastructure d'un fournisseur de services, les locataires peuvent commencer à utiliser l'application.

Pour séparer les tâches et les stratégies liées à différents locataires, vous devez créer un Serveur d'administration virtuel dédié dans Kaspersky Security Center pour chaque locataire. Toutes les tâches et stratégies des applications multilocataires exécutées pour un locataire doivent être créées pour le groupe d'administration des appareils administrés du Serveur d'administration virtuel correspondant à ce locataire. Les tâches créées pour les groupes d'administration associés au Serveur d'administration principal n'affectent pas les appareils des locataires.

Contrairement aux administrateurs de fournisseur de services, un administrateur de locataire peut créer et afficher des tâches et des stratégies d'application uniquement pour les appareils du locataire concerné. Les ensembles de tâches et les paramètres de stratégie disponibles pour les administrateurs de fournisseur de services et les administrateurs de locataire sont différents. Certaines tâches et certains paramètres de stratégie ne sont pas disponibles pour les administrateurs de locataire.

Dans une structure hiérarchique de locataire, les stratégies créées pour les applications multilocataires sont héritées des groupes d'administration de niveau inférieur ainsi que des groupes d'administration de niveau supérieur : la stratégie est propagée à tous les appareils clients appartenant au locataire.

Copie de sauvegarde et restauration des paramètres du Serveur d'administration

La tâche de sauvegarde et l'utilitaire klbackup permettent de réaliser une sauvegarde des paramètres du Serveur d'administration et des bases de données qu'il utilise. La copie de sauvegarde reprend tous les paramètres principaux et les objets du Serveur d'administration : les certificats du Serveur d'administration, les clés principales de chiffrement des disques des appareils administrés, les clés pour les licences, la structure des groupes d'administration avec tout le contenu, les tâches, les stratégies, etc. La copie de sauvegarde permet de restaurer le fonctionnement du Serveur d'administration très rapidement : d'une dizaine de minutes à deux heures.

En l'absence d'une copie de sauvegarde, un échec peut provoquer la perte irréversible des certificats et de tous les paramètres du Serveur d'administration. Il faudrait alors configurer à nouveau Kaspersky Security Center et réaliser à nouveau le déploiement initial de l'Agent d'administration sur le réseau de l'organisation. De plus, les clés principales du chiffrement des disques des appareils administrés seraient également perdues, ce qui pose un risque de perte irréversible des données chiffrées sur les appareils dotés de Kaspersky Endpoint Security. Par conséquent, ne négligez pas les sauvegardes régulières du Serveur d'administration à l'aide de la tâche de sauvegarde standard.

L'Assistant de configuration initiale de l'application crée la tâche de sauvegarde des paramètres du Serveur d'administration avec le lancement quotidien à 4h00 du matin. Les copies de sauvegarde sont enregistrées par défaut dans le dossier %ALLUSERSPROFILE%\Application Data\KasperskySC.

Si vous utilisez une instance de Microsoft SQL Server installée sur un autre appareil en guise de SGBD, il faut modifier la tâche de sauvegarde : indiquer en tant que dossier d'enregistrement des copies de sauvegarde le chemin UNC, accessible en écriture, au service du Serveur d'administration et au service SQL Server. Cette exigence spéciale est le résultat des particularités de la sauvegarde dans le SGBD Microsoft SQL Server.

Si vous utilisez à titre de SGBD une instance locale de Microsoft SQL Server, il est recommandé d'enregistrer aussi les copies de sauvegarde sur un lecteur distinct afin de les protéger contre un endommagement simultané avec le Serveur d'administration.

Puisque la copie de sauvegarde contient d'importantes données, la tâche de sauvegarde et l'utilitaire klbackup prévoient la protection des copies de sauvegarde par mot de passe. Par défaut, aucun mot de passe n'est défini lors de la création de la tâche de sauvegarde. Vous devez spécifier un mot de passe dans les propriétés de la tâche de sauvegarde. Le non-respect de cette exigence signifie que les clés des certificats du Serveur d'administration, les clés pour les licences et la clé principale du chiffrement des disques des appareils administrés ne sont pas chiffrées.

Outre les sauvegardes régulières, il faut aussi créer une copie de sauvegarde avant toute modification importante, notamment avant la mise à jour du Serveur d'administration jusqu'à version la plus récente et avant l'installation des correctifs du Serveur d'administration.

Si vous utilisez Microsoft SQL Server en tant que SGBD, vous pouvez réduire la taille des copies de sauvegarde. Pour ce faire, activez l'option **Compresser la sauvegarde** dans les paramètres de SQL Server.

La restauration au départ d'une copie de sauvegarde s'opère via l'utilitaire klbackup sur l'instance opérationnelle du Serveur d'administration opérationnel qui vient d'être installé et dont la version est identique à la version du Serveur pour lequel la copie de sauvegarde avait été créée (ou plus récente).

L'instance du Serveur d'administration sur lequel la restauration a lieu doit utiliser un SGBD du même type (par exemple, le même SQL Server ou MariaDB) de la même version ou d'une version plus récente. La version du Serveur d'administration peut être la même (avec un correctif semblable ou plus récent) ou plus récente.

Cette section décrit les scénarios typiques de restauration des paramètres et des objets du Serveur d'administration.

Panne de l'appareil doté du Serveur d'administration

Si l'appareil doté du Serveur d'administration tombe en panne après la défaillance, il est recommandé d'exécuter les actions suivantes :

- Attribuer la même adresse au nouveau Serveur d'administration : le nom NetBIOS, nom de domaine complet, IP statique, en fonction de ce qui avait été défini lors du déploiement des Agents d'administration.
- Installer le Serveur d'administration avec un SGBD du même type, de la même version ou d'une version plus récente. Il est possible d'installer la même version du Serveur avec le même correctif ou un correctif plus récent, ou une version plus récente. Après l'installation, il n'est pas nécessaire d'exécuter la configuration initiale à l'aide de l'Assistant.
- Dans le menu **Démarrer**, lancez l'utilitaire klbackup et réalisez la restauration.

Endommagement des paramètres du Serveur d'administration ou de la base de données

Si le Serveur d'administration est devenu inopérationnel suite à l'endommagement des paramètres ou de la base de données (par exemple, à cause d'une panne d'alimentation), il est conseillé de suivre le scénario de restauration suivant :

1. Lancer l'analyse du système de fichiers sur l'appareil concerné.
2. Désinstaller la version inopérationnelle du Serveur d'administration.
3. Installer à nouveau le Serveur d'administration avec la SGBD du même type et de version identique ou plus récente. Il est possible d'installer la même version du Serveur avec le même correctif ou un correctif plus récent, ou une version plus récente. Après l'installation, il n'est pas nécessaire d'exécuter la configuration initiale à l'aide de l'Assistant.
4. Depuis le menu **Démarrer**, lancez l'utilitaire de la copie de sauvegarde klbackup et réalisez la restauration.

Il est inadmissible de restaurer le Serveur d'administration à l'aide d'une méthode autre que l'utilitaire standard klbackup.

Tous les cas de restauration du Serveur d'administration à l'aide d'un logiciel tiers entraînent toujours une perte de synchronisation des données sur les nœuds de l'application distribuée Kaspersky Security Center et par conséquent, un mauvais fonctionnement de l'application.

Déploiement de l'Agent d'administration et de l'application de sécurité

Pour administrer les appareils de l'entreprise, il faut installer l'Agent d'administration sur les appareils. Le déploiement de l'application distribuée Kaspersky Security Center sur les appareils de l'entreprise commence d'habitude par l'installation de l'Agent d'administration sur ceux-ci.

Sous Microsoft Windows XP, un Agent d'administration peut ne pas effectuer correctement les opérations suivantes : télécharger les mises à jour directement à partir des serveurs de Kaspersky (comme point de distribution) ; fonctionner comme proxy KSN (comme point de distribution) et détecter les vulnérabilités tierces (si la gestion des vulnérabilités et des correctifs est utilisée).

Déploiement initial

Si un Agent d'administration est déjà installé sur l'appareil, l'installation à distance des applications sur celui-ci se réalise à l'aide de l'Agent d'administration en question. Dans ce cas, le paquet de distribution de l'application à installer avec les paramètres d'installation définis par l'administrateur se réalise via les canaux de communication entre les Agents d'administration et le Serveur d'administration. Pour transférer le paquet de distribution, vous pouvez utiliser des centres intermédiaires de diffusion sous la forme de points de distribution, d'une diffusion multicast, etc. Les informations détaillées sur l'installation des applications sur les appareils administrés déjà dotés de l'Agent d'administration sont reprises dans cette section.

L'installation initiale de l'Agent d'administration sur des appareils Microsoft Windows peut être réalisée d'une des manières suivantes :

- A l'aide d'outils tiers d'installation à distance d'applications.
- A l'aide du mécanisme des stratégies de groupe Microsoft Windows avec les outils standard d'administration des stratégies de groupe Microsoft Windows.
- De manière forcée, à l'aide des options correspondantes dans la tâche d'installation à distance des applications de Kaspersky Security Center.
- Via l'envoi aux utilisateurs des appareils de liens vers les paquets autonomes créés par Kaspersky Security Center. Les paquets autonomes sont des modules exécutables qui contiennent la distribution des applications sélectionnés avec les paramètres configurés.
- Manuellement, en lançant les programmes d'installation sur les appareils.

Sur les plateformes qui diffèrent de Microsoft Windows, l'installation initiale de l'Agent d'administration sur les appareils administrés doit s'opérer à l'aide des outils tiers disponibles ou manuellement via l'envoi à l'utilisateur d'une archive contenant un paquet de distribution préalablement configuré. La mise à jour de l'Agent d'administration jusqu'à la nouvelle version et l'installation d'autres applications de Kaspersky sur ces plateformes peuvent être réalisées à l'aide de tâches d'installation à distance des applications, en utilisant les Agents d'administration qui se trouvent déjà sur les appareils. Dans ce cas, l'installation se déroule comme l'installation sur la plateforme Microsoft Windows.

Lors de la sélection des méthodes et des stratégies de déploiement des applications sur le réseau administré, il faut prendre en considération une série de facteurs (liste non exhaustive) :

- Configuration du réseau d'entreprise
- Nombre total d'appareils
- Présence de domaines Windows sur le réseau administré, possibilité de modifier les stratégies de groupe Active Directory dans ces domaines
- Valeur du ou des comptes utilisateur dotés des autorisations d'administrateur local sur les appareils où il faut réaliser le déploiement initial des applications de Kaspersky (à savoir la disponibilité d'un compte utilisateur de domaine avec des autorisations d'administrateur local, ou la présence de comptes utilisateurs locaux unifiés avec autorisations d'administrateur sur ces appareils)
- Caractère de la communication et bande passante des canaux réseau entre le Serveur d'administration et les réseaux de clients MSP et la largeur de la bande passant des canaux au sein de ces réseaux
- Paramètres de sécurité adoptés, au moment du début du déploiement, sur les appareils distants (plus particulièrement l'utilisation d'UAC et du mode Simple Stockage de fichiers)

Configuration des paramètres des programmes d'installation

Avant de procéder au déploiement des applications de Kaspersky dans le réseau, il faut définir les paramètres de l'installation, à savoir ces paramètres qui sont définis au cours de l'installation de l'application. Lors de l'installation de l'Agent d'administration, il faut définir au moins l'adresse pour la connexion au Serveur d'administration, paramètres proxy et, si possible, certains paramètres avancés. En fonction du mode d'installation choisi, les paramètres peuvent être définis de différentes façons. Dans le cas le plus simple (installation manuelle interactive sur l'appareil sélectionné), vous pouvez définir les paramètres requis via l'interface utilisateur du programme d'installation car dans certains cas, le déploiement initial peut même être réalisé via l'envoi aux utilisateurs de liens vers le paquet de distribution de l'Agent d'administration avec indication des paramètres (adresses du Serveur d'administration, etc.) que l'utilisateur va devoir saisir dans l'interface du programme d'installation.

Ce mode de configuration des paramètres est déconseillé dans la pratique en raison de son aspect peu convivial pour les utilisateurs et du risque élevé d'erreur lors de la définition manuelle des valeurs des paramètres. Il ne convient pas non plus à l'installation en mode silencieux des applications sur des groupes d'appareils. Dans un cas typique, l'administrateur doit définir centralement les valeurs des paramètres qui peuvent être utilisés par la suite pour la création des paquets d'installation autonomes. Les paquets autonomes sont des archives autoextractibles des distributions dont les paramètres ont été définis par un administrateur. Les paquets autonomes peuvent être disposés sur les ressources auxquelles les utilisateurs finaux peuvent accéder pour télécharger du contenu (par exemple, le Serveur Web de Kaspersky Security Center) et pour l'installation en mode silencieux sur les appareils sélectionnés du réseau.

Paquets d'installation

La méthode principale de configuration des paramètres d'installation des applications est universelle et convient à tous les moyens d'installation des applications : aussi bien via les outils de Kaspersky Security Center qu'à l'aide de la majorité des outils tiers. Ce moyen prévoit la création dans Kaspersky Security Center des paquets d'installation des applications.

Les paquets d'installation sont créés selon un des moyens suivants :

- Automatiquement au départ des distributions indiquées sur la base des *descripteurs* repris dans leur composition (fichiers portant l'extension kud contenant les règles de l'installation, l'analyse du résultat et d'autres informations).

- Au départ des fichiers exécutables des programmes d'installation ou des programmes d'installation au format Microsoft Windows Installer (MSI), pour les applications standard ou prises en charge.

Les paquets d'installation créés sont organisés hiérarchiquement sous forme de dossiers avec des sous-dossiers et des fichiers. Outre le paquet de distribution original, le paquet d'installation contient également des paramètres modifiés (y compris les paramètres du programme d'installation et la règle du traitement de situations, comme la nécessité du redémarrage du système d'exploitation pour terminer l'installation), ainsi que de petits modules auxiliaires.

Vous pouvez définir les valeurs des paramètres de l'installation propres à l'app concrète prise en charge dans l'interface utilisateur de la Console d'administration lors de la création du paquet d'installation (plus de paramètres encore peuvent être configurés dans les propriétés d'un paquet d'installation déjà créé). En cas d'installation à distance des applications via les outils de Kaspersky Security Center, les paquets d'installation sont remis aux appareils ciblés de telle sorte que le programme d'installation de l'application offre l'accès à tous les paramètres définis par l'administrateur disponibles pour cette application. En cas d'utilisation d'outils tiers pour installer des applications de Kaspersky, il suffit de garantir l'accès sur l'appareil ciblé à l'ensemble du paquet d'installation, à savoir la disponibilité du paquet de distribution et ses paramètres. Les paquets d'installation sont créés et conservés par Kaspersky Security Center dans un sous-dossier dédié du dossier des données partagées.

N'indiquez pas dans les paramètres des paquets d'installation les données des comptes utilisateur privilégiés.

Pour obtenir des instructions sur l'utilisation de cette méthode de configuration pour les applications de Kaspersky avant le déploiement via des outils tiers, consultez la section " Déploiement à l'aide du mécanisme des stratégies de groupe Microsoft Windows ".

Directement après l'installation de Kaspersky Security Center, plusieurs paquets d'installation, prêts à l'emploi, sont créés automatiquement. Il s'agit entre autres de paquets de l'Agent d'administration et de l'application de sécurité pour la plateforme Microsoft Windows.

L'utilisation des paquets d'installation pour le déploiement d'applications sur le réseau du client MSP implique dans de nombreux cas la création de paquets d'installation sur les serveurs virtuels qui correspondent aux clients MSP. La création de paquets d'installation sur les Serveurs virtuels permet d'utiliser différents paramètres d'installation dans les paquets d'installation destinés à différents clients MSP. Dans le premier exemple, ceci s'impose principalement dans les paquets d'installation de l'Agent d'administration, car les Agents d'administration déployés sur les réseaux de différents clients MSP utilisent différentes adresses de connexion au Serveur d'administration. Plus particulièrement, l'adresse est déterminée par le serveur virtuel auquel l'agent d'administration se connecte.

Outre la possibilité de créer des paquets d'installation directement sur le Serveur d'administration virtuel, le mode principal d'utilisation des paquets d'installation sur les Serveurs d'administration virtuels est la " diffusion " des paquets d'installation depuis le Serveur d'administration principal vers les serveurs virtuels. La tâche correspondante du Serveur d'administration permet de diffuser les paquets d'installation sélectionnés ou tous les paquets d'installation sur les Serveurs d'administration virtuels sélectionnés (y compris tous les serveurs qui appartiennent au groupe d'administration sélectionné). De même, lors de la création d'un Serveur d'administration virtuel, vous pouvez sélectionner la liste des paquets d'installation du Serveur d'administration principal. Les paquets sélectionnés sont diffusés directement sur le Serveur d'administration virtuel qui a été à nouveau créé.

Lors de la diffusion d'un paquet d'installation, seule une partie de son contenu est copiée. Seuls les fichiers des paramètres propres à ce Serveur d'administration virtuel sont stockés dans le stockage de fichiers qui correspond au paquet d'installation diffusé sur le serveur Virtuel. La partie principale non modifiée du paquet d'installation (y compris le paquet de distribution de l'app à installer) est enregistrée uniquement dans le stockage du Serveur d'administration principal. Cela permet d'augmenter sensiblement les performances du système et de réduire le volume d'espace disque requis. Lors de l'utilisation de paquets d'installation distribués sur des Serveurs d'administration virtuels (à savoir, lors de l'utilisation des tâches d'installation à distance ou lors de la création de paquets d'installation autonomes), on observe l'ajout des données du paquet d'installation original du Serveur d'administration principal des fichiers contenant les paramètres qui correspondent au paquet diffusé sur le Serveur d'administration virtuel.

Malgré le fait que la clé de licence pour une application peut être définie dans les propriétés du paquet d'installation, il vaut mieux ne pas utiliser ce mode de diffusion des licences en raison de l'accessibilité en lecture des fichiers qui se trouvent dans le répertoire. Il faut utiliser des clés de licence diffusées automatiquement ou les tâches pour l'installation des clés de licence.

Propriétés MSI et fichiers de transformation

Une autre manière configurer les paramètres de l'installation sur la plateforme Windows consiste à désigner les propriétés MSI et les fichiers de transformation. Ce mode peut être utilisé lors de l'installation à l'aide d'outils tiers axés sur le fonctionnement avec des programmes d'installation au format Microsoft Installer, ainsi que lors de l'installation via des stratégies de groupe Windows à l'aide des outils standard de Microsoft ou d'autres outils tiers qui fonctionnent avec les stratégies de groupe Windows.

Déploiement à l'aide d'outils tiers d'installation à distance d'applications

Si l'entreprise possède d'autres moyens quelconque d'installation à distance des applications (par exemple, Microsoft System Center), il est conseillé de réaliser le déploiement initial à l'aide de ces outils.

Procédez comme suit :

- Sélectionner la méthode de configuration des paramètres d'installation la mieux adaptée à l'outil de déploiement utilisé.
- Définir le mécanisme de synchronisation entre la modification des paramètres des paquets d'installation dans l'interface de la Console d'administration et l'utilisation des outils tiers de déploiement des applications choisis depuis les données des paquets d'installation.

Informations générales sur les tâches d'installation à distance des applications de Kaspersky Security Center

Kaspersky Security Center propose différents mécanismes d'installation à distance des apps sous la forme de tâches d'installation à distance des apps. Il est possible de créer une tâche d'installation à distance aussi bien pour un groupe d'administration indiqué que pour un ensemble d'appareils ou pour une sélection d'appareils (ces tâches apparaissent dans la Console d'administration, dans le dossier **Tâches**). Lors de la création de la tâche, vous pouvez choisir les paquets d'installation (de l'Agent d'administration et/ou d'une autre application) qui peuvent être installés à l'aide de cette tâche ainsi que définir plusieurs paramètres qui définissent le mode d'installation à distance.

Les tâches pour les groupes d'administration agissent non seulement sur les appareils affectés à un groupe spécifique, mais également sur tous les appareils de l'ensemble des sous-groupes de ce groupe d'administration. Si le paramètre correspondant est activé dans les paramètres de la tâche, la tâche s'applique aux appareils des Serveurs d'administration secondaires situés dans ce groupe ou dans ses sous-groupes.

Les tâches pour 'ensemble d'appareils mettent à jour la liste des appareils clients à chaque lancement, conformément à la composition de la sélection d'appareils au lancement de la tâche. Si la sélection d'appareils contient des appareils connectés à des Serveurs d'administration secondaires, la tâche est également lancée sur ces appareils.

Pour garantir le fonctionnement de la tâche d'installation à distance sur les appareils connectés à des Serveurs d'administration secondaires, il faut d'abord diffuser les paquets d'installation utilisés par la tâche aux Serveurs d'administration secondaires correspondant à l'aide d'une tâche de diffusion.

Déploiement à l'aide du mécanisme des stratégies de groupe Microsoft Windows

Il est conseillé de réaliser le déploiement initial des Agents d'administration à l'aide des stratégies de groupe Microsoft Windows quand les conditions suivantes sont remplies :

- Les appareils sont les membres du domaine Active Directory.
- Autorisation de l'accès au contrôleur de domaine avec les privilèges d'administrateur qui permettent de créer et de modifier des stratégies de groupe Active Directory.
- Possibilité de transfert des paquets d'installation configurés dans le réseau des appareils administrés (dans le dossier partagé accessible en écriture pour tous les appareils).
- Le plan de déploiement permet d'attendre le redémarrage standard des appareils avant le début du déploiement sur ceux ci des Agent d'administration ou la stratégie de groupe Windows peut être imposée aux appareils.

L'essence de ce mode de déploiement est la suivante :

- Le paquet de distribution de l'application au format Microsoft Installer (paquet MSI) se place dans le dossier partagé (le dossier accessible en lecture aux comptes utilisateurs LocalSystem des appareils).
- Dans la stratégie de groupe Active Directory, l'objet d'installation est créé pour le paquet de distribution.

- La zone d'action de l'installation est définie en indiquant l'organisation unitaire et/ou le groupe de sécurité qui contient le ou les appareil(s) cible(s).

- Lorsque l'appareil entre à nouveau dans le domaine (avant l'entrée des utilisateurs de l'appareil dans le système), la recherche de la présence de l'application requise parmi les applications installées a lieu. Si l'application est absente, le paquet de distribution est téléchargé depuis la ressource définie dans la stratégie, puis l'installation a lieu.

Un des avantages de ce mode de déploiement est le fait que les applications désignées sont installées sur les appareils lors du chargement du système d'exploitation avant l'entrée de l'utilisateur dans le système. Même si l'utilisateur doté des privilèges requis supprime l'application, celle-ci est à nouveau installée au prochain chargement du système d'exploitation. Ce mode de déploiement présente toutefois un inconvénient : les modifications introduites par l'administrateur dans la stratégie de groupe entrent en vigueur uniquement après le redémarrage des appareils (sans l'application des moyens complémentaires).

Les stratégies de groupe permettent d'installer l'Agent d'administration ainsi que d'autres applications dont les programmes d'installation possèdent le format Windows Installer.

> L'installation de l'Agent d'administration à partir du paquet MSI n'est possible qu'en mode silencieux, l'installation interactive à partir du paquet MSI n'est pas prise en charge.

Si vous choisissez ce mode de déploiement, il faut, entre autres, évaluer la charge sur la ressource fichier d'où les fichiers seront copiés vers les dans le appareils au moment de l'application des stratégies de groupe Windows. Vous devez également choisir la méthode de remise du paquet d'installation configuré à cette ressource ainsi que la méthode de synchronisation des modifications pertinentes dans ses paramètres.

Utilisation des stratégies Microsoft Windows avec l'aide de la tâche d'installation à distance des applications de Kaspersky Security Center

Ce mode de déploiement est possible uniquement si le contrôleur de domaine auquel appartiennent les appareils est accessible depuis l'appareil sur lequel le Serveur d'administration est installé et si les appareils ont un accès en lecture au dossier partagé du Serveur d'administration (dans lequel se trouvent les paquets d'installation). C'est pourquoi ce mode de déploiement n'est pas envisagé dans le cadre de MSP.

Installation indépendante d'applications à l'aide de stratégies Microsoft Windows

L'administrateur peut créer lui-même dans la stratégie de groupe Windows les objets nécessaires à l'installation. Dans ce cas, il faut placer les paquets sur un serveur de fichiers distinct et y faire référence.

Les scénarios d'installation suivants sont possible :

- L'administrateur crée le paquet d'installation et configure ses propriétés dans la Console d'administration. Ensuite, l'administrateur copie l'ensemble du sous-dossier EXEC de ce paquet dans le dossier partagé de Kaspersky Security Center et le colle dans le dossier sur une ressource fichiers spéciale de l'entreprise. L'objet de la stratégie de groupe fait référence au fichier MSI de ce paquet configuré qui se trouve dans le sous-dossier sur une ressource fichier spéciale de l'entreprise.

- L'administrateur charge le paquet de distribution de l'application (y compris la distribution de l'Agent d'administration) depuis Internet et la place sur la ressource fichier spéciale de l'entreprise. L'objet de la stratégie de groupe fait référence au fichier MSI de ce paquet configuré qui se trouve dans le sous-dossier sur une ressource fichier spéciale de l'entreprise. La configuration des paramètres de l'installation s'opère via la configuration des propriétés MSI ou via la configuration des fichiers de transformation MST.

Déploiement forcé à l'aide d'une tâche d'installation à distance des applications de Kaspersky Security Center

Pour réaliser le déploiement initial de l'Agent d'administration ou d'autres applications, vous pouvez forcer l'installation des paquets d'installation sélectionnés à l'aide de la tâche d'installation à distance de Kaspersky Security Center, à condition que chaque appareil dispose d'un ou plusieurs comptes utilisateurs avec des droits d'administrateur local.

L'installation forcée peut être utilisée notamment dans le cas où le Serveur d'administration n'a pas d'accès direct aux appareils : par exemple, les appareils se trouvent sur des réseaux isolés ou bien ils se trouvent sur un réseau local, mais le Serveur d'administration se trouve dans la zone démilitarisée.

Lors du déploiement initial, l'Agent d'administration n'est pas installé. Par conséquent, dans les paramètres de la tâche d'installation à distance, il n'est pas possible de sélectionner la distribution des fichiers nécessaires à l'installation de l'application à l'aide de l'Agent d'administration. Vous pouvez uniquement choisir de distribuer des fichiers en utilisant les ressources du système d'exploitation par l'intermédiaire du Serveur d'administration ou des points de distribution.

Le service du Serveur d'administration doit être exécuté sous un compte disposant de privilèges d'administrateur sur les appareils cibles. Vous pouvez également désigner un compte ayant accès au partage admin$ dans les paramètres de la tâche d'installation à distance.

Par défaut, la tâche d'installation à distance se connecte aux appareils à l'aide des identifiants du compte sous lequel le Serveur d'administration est exécuté, c'est-à-dire le compte permettant d'accéder au partage admin$. Vous devez définir ce compte dans les paramètres de la tâche d'installation à distance uniquement si l'Agent d'administration n'est pas installé sur les appareils cibles.
Lors de la création de la tâche d'installation à distance à exécuter sur des appareils basés sur Linux, vous devez toujours définir un compte pour la création d'une connexion SSH.

Les appareils peuvent être désignés explicitement (via une liste) soit via la sélection du groupe d'administration de Kaspersky Security Center auquel ils appartiennent, soit via la création d'une sélection d'appareils selon une condition définie. Le début de l'installation est défini par la programmation de la tâche. Si le paramètre **Lancer les tâches non exécutées** est activé dans les propriétés de la tâche, la tâche peut être exécutée directement après l'activation des appareils ou lors de leur transfert dans le groupe d'administration cible.

L'installation forcée implique la remise des paquets d'installation aux appareils cibles, suivie de la copie des fichiers sur la ressource d'administration admin$ de chacun des appareils et l'enregistrement à distance sur ceux-ci des services auxiliaires. La remise des paquets d'installation sur les appareils cibles s'opère à l'aide de la fonction de Kaspersky Security Center chargée de l'interaction sur le réseau. Les conditions suivantes doivent être remplies :

- Les appareils cibles sont accessibles du côté du Serveur d'administration ou du point de distribution.
- La résolution des noms pour les appareils fonctionne correctement sur le réseau.
- Les ressources d'administration partagées admin$ ne sont pas désactivées sur les appareils administrés.

- Les services système suivants sont exécutés sur les appareils cibles :
  - Server (LanmanServer)

    Par défaut, ce service est exécuté.
  - DCOM Server Process Launcher (DcomLaunch)
  - RPC Endpoint Mapper (RpcEptMapper)
  - Remote Procedure Call (RpcSs)
- Le port TCP 445 est ouvert sur les appareils cibles pour permettre l'accès à distance via les outils Windows.

  > Les protocoles TCP 139, UDP 137 et UDP 138 sont utilisés par des protocoles plus anciens et ne sont plus nécessaires pour les applications actuelles.

  Les ports d'accès dynamiques sortants doivent être autorisés sur le pare-feu pour les connexions du Serveur d'administration et des points de distribution vers les appareils cibles.
- Les paramètres de sécurité de la stratégie de domaine Active Directory sont autorisés à assurer le fonctionnement du protocole NTLM lors du déploiement de l'Agent d'administration.
- Sur les appareils cibles exécutant Microsoft Windows XP, le mode Simple File Sharing est désactivé.
- Sur les appareils cibles, le modèle d'accès partagé et de sécurité est défini sur *Habituel – les utilisateurs locaux s'authentifient comme eux-mêmes*. Il ne peut en aucun cas être défini sur *Invité – les utilisateurs locaux s'authentifient en tant qu'invité*.
- Les appareils appartiennent au domaine ou des comptes utilisateurs unifiés avec privilèges d'administration sont créés au préalable sur les appareils.

> Pour réussir le déploiement de l'Agent d'administration ou d'autres applications sur un appareil qui n'est pas joint à un domaine Active Directory Windows Server 2003 ou une version ultérieure, vous devez désactiver le contrôle de compte d'utilisateur à distance sur cet appareil. Le contrôle de compte d'utilisateur à distance est l'une des raisons qui empêche les comptes d'administration locaux d'accéder à admin$, ce qui est nécessaire pour le déploiement forcé de l'Agent d'administration ou d'autres applications. La désactivation du contrôle de compte d'utilisateur à distance n'affecte pas le contrôle de compte d'utilisateur local.

Lors de l'installation sur de nouveaux appareils qui ne figurent pas encore dans les groupe d'administration de Kaspersky Security Center, il est possible de définir dans les propriétés de la tâche d'installation à distance le groupe d'administration dans lequel les appareils vont être placés à l'issue de l'installation de l'Agent d'administration sur ces appareils.

> Lors de la création de la tâche de groupe, il ne faut pas oublier que la tâche de groupe agit sur les appareils de tous les sous-groupes du groupe sélectionné. C'est la raison pour laquelle il n'est pas nécessaire de duplique les tâches d'installation dans les sous-groupes.

L'installation automatique est un moyen simplifié de créer des tâches pour l'installation forcée d'applications. Pour cela, il faut sélectionner dans la liste des paquets d'installation des propriétés du groupe d'administration les paquets à installer sur les appareils de ce groupe. Au final, les paquets d'installation sélectionnés sont installés automatiquement sur tous les appareils de ce groupe et de ses sous-groupes. La période pendant laquelle les paquets sont installés dépend de la bande passe du réseau et du total d'appareils dans le réseau.

Pour réduire la charge sur le Serveur d'administration lors de la propagation des paquets d'installation sur les appareils, vous pouvez sélectionner l'installation via les points de distribution dans la tâche d'installation. Il ne faut pas oublier que ce mode d'installation génère une charge sensible sur les appareils désignés comme points de distribution. C'est la raison pour laquelle il est recommandé de sélectionner des appareils conformes aux exigences des points de distribution. Si vous utilisez des points de distribution, vous devez vous assurer qu'ils sont présents dans chacun des sous-réseaux isolés hébergeant des appareils cibles.

L'utilisation de points de distribution en guise de centres locaux d'installation peut être pratique notamment pour les installations sur des appareils dans des sous-réseaux connectés au Serveur d'administration via un canal de communication étroit alors qu'il existe un canal large entre les appareils au sein du sous-réseau.

Il faut que l'espace disponible dans la section contenant le dossier %ALLUSERSPROFILE %\Application Data\KasperskyLab\adminkit soit plusieurs fois supérieur au volume total des paquets de distribution des applications à installer.

Lancement de paquets autonomes créés par Kaspersky Security Center

Les méthodes décrites ci-dessus pour le déploiement initial de l'Agent d'administration et des applications ne sont pas toujours applicables en raison de l'impossibilité de remplir toutes les conditions requises. Dans ce cas, il est possible de créer un seul fichier exécutable au départ des paquets d'installations préparés par l'administrateur et dotés des paramètres requis pour l'installation à l'aide des outils de Kaspersky Security Center. Ce paquet est un *paquet d'installation autonome*. Le paquet d'installation autonome peut être publié sur le Serveur Web interne (qui fait partie de Kaspersky Security Center), si cela se justifie (l'accès à ce serveur Web depuis l'extérieur est configuré pour les utilisateurs des appareils) ou sur un serveur Web spécialement déployé qui fait partie de Kaspersky Security Center Web Console. Vous pouvez également copier les paquets autonomes sur un autre serveur Web.

Kaspersky Security Center permet d'envoyer un lien aux utilisateurs sélectionnés par email. Ce lien mène au fichier du paquet autonome sur le serveur Web et le message invite le destinataire à lancer le fichier (en mode interactif ou en mode silencieux avec la clé " -s "). Le paquet d'installation autonome peut être joint au message électronique pour les utilisateurs des appareils qui n'ont pas accès au Serveur Web. L'administrateur peut également copier le paquet autonome sur l'appareil externe et livrer le paquet à l'appareil requis en vue de son prochain démarrage.

Le paquet autonome peut être créé au départ du paquet de l'Agent d'administration, du paquet d'une autre application (par exemple, l'application de sécurité) ou directement au départ des deux paquets. Si le paquet autonome est créé au départ de l'Agent d'administration et d'une autre application, l'installation commence par l'Agent d'administration.

Lors de la création d'un paquet autonome avec l'Agent d'administration, il est possible d'indiquer le groupe d'administration dans lequel les nouveaux appareils (qui ne figuraient pas encore dans des groupes d'administration) vont être automatiquement placés à l'issue de l'installation de l'Agent d'administration.

Les paquets autonomes peuvent être installés interactivement (par défaut), avec l'affichage du résultat de l'installation des applications qu'ils contiennent ou en mode silencieux (lancement avec la clé " -s "). Le mode " silencieux " peut être utilisé pour une installation au départ de certains scripts (par exemple, des scripts configurés pour être lancés à la fin du déploiement de l'image du système d'exploitation, etc.). Le résultat de l'installation en mode " silencieux " est défini par le code de retour du processus.

Possibilités d'installation manuelle des applications

Les administrateurs ou les utilisateurs expérimentés peuvent installer les applications manuellement en mode interactif. Ils peuvent utiliser dans ce cas de figure des distributions originales ou des paquets d'installation créés au départ de celles-ci et stockés dans le dossier partagé de Kaspersky Security Center. Les programmes d'installation fonctionnent par défaut en mode interactif et demande à l'utilisateur de confirmer toutes les valeurs des paramètres. Mais en cas de lancement du processus setup.exe depuis la racine du paquet d'installation avec la clé " -s ", le programme d'installation fonctionne en mode " silencieux " selon les paramètres définis lors de la configuration du paquet d'installation.

Lors du lancement de setup.exe depuis la racine du paquet d'installation, on assiste d'abord à la copie du paquet dans un dossier local temporaire, puis le programme d'installation de l'application est lancé depuis le dossier local.

Installation à distance des applications sur les appareils dotés de l'Agent d'administration

Si un Agent d'administration opérationnel et connecté au Serveur d'administration principal (ou à un de ses Serveurs secondaires) est installé sur l'appareil, il est possible de mettre à niveau la version de l'Agent d'administration sur cet appareil ainsi que d'installer, mettre à niveau ou supprimer n'importe quelle application prise en charge à l'aide de l'Agent d'administration.

Cette fonction est activée via la case **Utilisation de l'Agent d'administration** aux cases dans les propriétés de la tâche d'installation à distance des applications.

Si la case est cochée, la transmission des paquets d'installation avec les paramètres d'installation définis par l'administrateur se réalise via les canaux de communication entre l'Agent d'administration et le Serveur d'administration.

Pour optimiser la charge sur le Serveur d'administration et limiter le trafic entre le Serveur d'administration et les appareils, il est conseillé de désigner des points de distribution sur chaque réseau distant ou dans chaque domaine de diffusion (cf. les sections Rôle des points de distribution et Élaboration de la structure de groupes d'administration et désignation des points de distribution). Dans ce cas, la diffusion des paquets d'installation et des paramètres du programme d'installation se réalise depuis le Serveur d'administration sur les appareils via les points de distribution.

De même, l'utilisation des points de distribution permet de réaliser une multidiffusion des paquets d'installation. Ceci contribue à une réduction sensible du trafic réseau lors du déploiement des applications.

Lors de la transmission des paquets d'installation aux appareils via les canaux de communication entre les Agents d'administration et le Serveur d'administration, les paquets d'installation préparés pour la transmission sont également mis en cache dans le dossier %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\.working\FTServer. En cas d'utilisation d'un grand nombre de paquets d'installation divers de grande taille et en présence d'un nombre élevé de points de distribution, la taille de ce dossier peut sensiblement augmenter.

Il est impossible de supprimer manuellement des fichiers du dossier FTServer. Lors de la suppression des paquets d'installation d'origine, les données correspondantes sont également supprimées automatiquement du dossier FTServer.

Les données acceptées du côté des points de distribution sont conservées dans le %ALLUSERSPROFILE %\Application Data\KasperskyLab\adminkit\1103 \$ FTCITmp.

Il est impossible de supprimer manuellement des fichiers du dossier $FTCITmp. Le contenu de ce dossier est supprimé automatiquement au fur et à mesure que les tâches qui utilisent les données de ce dossier se terminent.

Puisque les paquets d'installation sont diffusés via les canaux de communication entre le Serveur d'administration et les Agents d'administration depuis un stockage intermédiaire et dans un format optimisé pour le transfert via le réseau, il ne faut pas modifier les paquets d'installation dans le dossier source du paquet d'installation. Ces modifications ne seraient pas automatiquement prises en compte par le Serveur d'administration. S'il est nécessaire de modifier manuellement les fichiers des paquets d'installation (bien que cela soit déconseillé), il faut absolument introduire la moindre modification des paramètres du paquet d'installation dans la Console d'administration. La modification des paramètres du paquet d'installation dans la Console d'administration oblige le Serveur d'administration à mettre à jour l'image du paquet dans le cache préparé pour le transfert sur les appareils.

Administration du redémarrage des appareils dans la tâche d'installation à distance

Souvent, pour terminer l'installation à distance des applications (surtout sur la plateforme Windows), il faut redémarrer l'appareil.

En cas d'utilisation de la tâche d'installation à distance des applications de Kaspersky Security Center, l'Assistant de création d'une tâche ou la fenêtre des propriétés de la tâche créée (section **Redémarrage du système d'exploitation**) vous permet de sélectionner l'action à effectuer lorsque l'appareil Windows nécessite un redémarrage :

- **Ne pas redémarrer l'appareil**. Dans ce cas, le redémarrage automatique n'a pas lieu. Pour terminer l'installation, il faut redémarrer l'appareil (par exemple, manuellement ou à l'aide d'une tâche d'administration des appareils). Les informations sur la nécessité du redémarrage seront enregistrées dans les résultats de la tâche et dans l'état de l'appareil. Cette option convient aux tâches d'installation sur les serveurs et autres appareils pour lesquels la continuité des opérations est critique.

- **Redémarrer l'appareil**. Dans ce cas, le redémarrage est toujours exécuté automatiquement, si celui-ci est requis pour terminer l'installation. Cette option convient aux tâches d'installation sur des appareils pour lesquels des interruptions périodiques sont admises (débranchement, redémarrage).

- **Demander à l'utilisateur**. Dans ce cas, le message sur le fait que l'appareil client doit être redémarré à la main s'affiche sur l'écran de l'appareil. Pour cette option, il est possible de configurer des paramètres avancés : le texte du message pour l'utilisateur, la fréquence du message, ainsi que le délai à l'issue duquel le redémarrage sera forcé (sans confirmation de l'utilisateur). L'option **Demander à l'utilisateur** convient le mieux aux postes de travail dont les utilisateurs doivent pouvoir choisir le moment qu'ils préfèrent pour le redémarrage.

Utilité de la mise à jour des bases de données dans le paquet d'installation de l'application antivirus

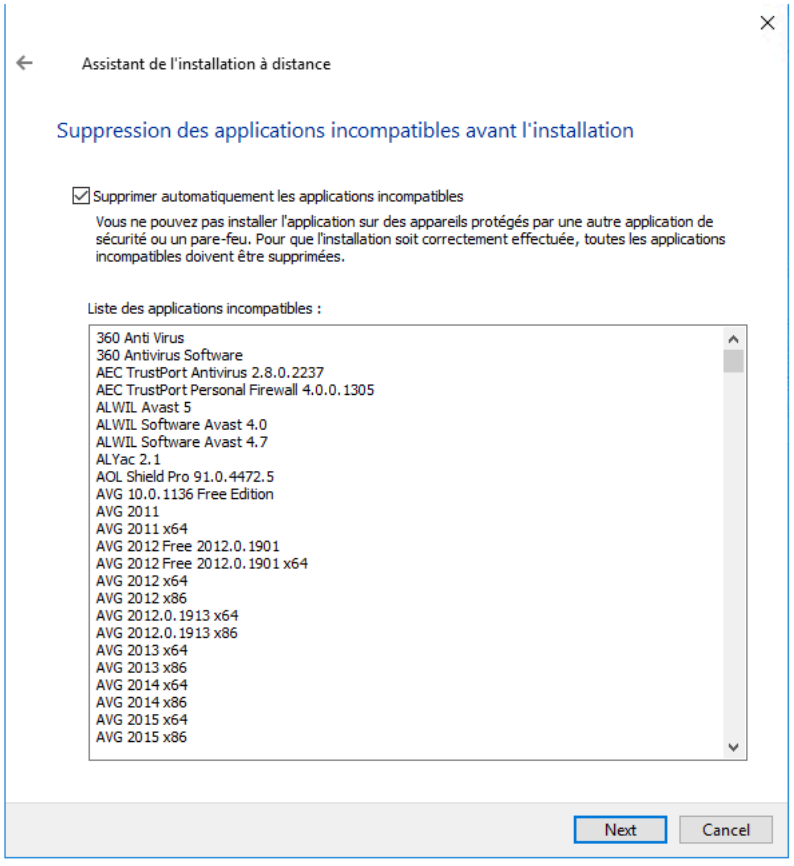
Avant de déployer la protection, il faut tenir compte de la possibilité de mettre à jour les bases antivirus (y compris les modules des correctifs automatiques), diffusés en même temps que le paquet de distribution de l'application de sécurité. Il est conseillé de forcer la mise à jour dans le paquet d'installation de l'application avant le début du déploiement (par exemple, à l'aide de la commande correspondante dans le menu contextuel du paquet d'installation sélectionné). Cela réduit le nombre de redémarrages requis pour terminer le déploiement de la protection sur les appareils. Si votre installation à distance requiert des paquets d'installation diffusés sur les Serveurs d'administration virtuels depuis le Serveur d'administration principal, la mise à jour des bases est requise uniquement dans le paquet d'origine sur le serveur principal. Dans ce cas, il n'est pas nécessaire de mettre à jour les bases dans les paquets diffusés sur les serveurs virtuels.

Remplacement de programmes de protection incompatibles d'éditeurs tiers

Pour installer des applications de sécurité de Kaspersky à l'aide des outils de Kaspersky Security Center, il faut peut-être supprimer tout logiciel tiers incompatible avec l'application à installer. Il y a deux méthodes principales pour exécuter cette tâche.

Suppression automatique des applications incompatibles à l'aide du programme d'installation

Lorsque vous lancez le programme d'installation, une liste des applications incompatibles avec une application Kaspersky s'affiche :



La liste des applications incompatibles qui s'affiche dans l'Assistant de l'installation à distance

Kaspersky Security Center détecte les logiciels incompatibles. En conséquence, vous pouvez cocher la case **Supprimer automatiquement les applications incompatibles** pour poursuivre l'installation. Si vous décochez cette case et ne désinstallez pas les logiciels incompatibles, l'erreur se produit et l'application Kaspersky n'est pas installée.

La suppression automatique des applications incompatibles est prise en charge par différents types d'installation.

Suppression des applications incompatibles à l'aide d'une tâche distincte

Les applications incompatibles sont supprimées à l'aide de la tâche *Désinstallation à distance d'une application*. Il faut lancer la tâche sur les appareils avant la tâche d'installation de l'application de sécurité. Par exemple, dans la tâche d'installation, vous pouvez sélectionner **Après l'exécution d'une autre tâche** en tant que type de programmation lorsque l'autre tâche est *Désinstallation à distance d'une application*.

Ce mode de suppression est recommandé si le programme d'installation de l'application de sécurité ne parvient pas à supprimer une des applications incompatibles.

Suppression de l'Agent d'administration protégé par mot de passe à l'aide de l'invite de commande

Pour désinstaller à distance l'Agent d'administration pour lequel vous avez défini un mot de passe de désinstallation, vous pouvez utiliser l'invite de commande.

En cas de perte ou d'oubli du mot de passe de l'Agent d'administration protégé par mot de passe, installé sur l'appareil qui n'est plus administré par Kaspersky Security Center, vous ne pouvez pas supprimer l'Agent d'administration à l'aide de l'utilitaire klmover, de l'outil Cleaner (cleaner.exe), ou l'invite de commande. Dans ce cas, il faut réinstaller le système d'exploitation sur l'appareil qui dispose de l'Agent d'administration protégé par un mot de passe.

Pour désinstaller l'Agent d'administration via l'invite de commande, procédez comme suit :

1. Convertissez le mot de passe de désinstallation en code hexadécimal.

   Utilisez une ressource Internet, un environnement de programmation, un éditeur de texte ou tout autre outil approprié pour convertir votre mot de passe en code hexadécimal.

   > Assurez-vous que le délimiteur de sortie utilisé pour séparer le code hexadécimal généré en parties est défini sur `00`. Par exemple, le code hexadécimal `51 77 65 72 74 79` est incorrect et le code hexadécimal `5100770065007200740079 00` est correct.

2. Saisissez la commande suivante à l'invite de commande, puis appuyez sur la touche **ENTRÉE** :

   ```
   msiexec.exe /x{<product code>} /qn KLUNINSTPASSWD=<hex code of your uninstallation password>
   ```

   Vous pouvez trouver le code produit de votre Agent d'administration dans le tableau ci-dessous.

Codes produits des Agents d'administration

Localisation	Code produit
Arabe	{FA7BF140-F356-404A-BDA3-3EF0878D7C63}
Bulgare	{4DBF6741-FA51-4C14-AFD2-B7D9246995F6}
Tchèque	{478A6A0B-D177-4402-B703-808C05C56B13}
anglais ;	{BCF4CF24-88AB-45E1-A6E6-40C8278A70C5}
français ;	{2924BEDA-E0D7-4DAF-A224-50D2E0B12F5B}
allemand ;	{2F383CB3-6D7C-449D-9874-164E49E1E0F5}
Hongrois	{8899A4D4-D678-49F8-AD96-0B784F58D355}
italien ;	{DC3A3164-36B3-4FB4-B7BF-16A41C35A728}
japonais.	{790C176F-7780-4C84-8B9C-455F5C0E61C5}
Coréen	{70812A40-973B-4DA1-96B9-C2011280CD99}
polonais ;	{1A7B331A-ABBE-4230-995E-BCD99C5A18CF}
portugais ;	{0F05E4E5-5A89-482C-9A62-47CC58643788}
Roumain	{FF802D76-E241-41D3-AAB4-DC7FBD659446}
russe ;	{ED1C2D7E-5C7A-48D8-A697-57D1C080ABA7}
Chinois simplifié	{FBD7C01E-49CB-4182-8714-9DB1EAE255CB}
espagnol ;	{F03982CF-1C5C-4E12-9F9E-D36C35E62402}
Espagnol-mx	{29748B5F-D88A-4933-B614-1CCCD6EFB0B7}
Chinois traditionnel	{F6AD731A-36B4-4739-B1D4-70D6EDA35147}
Turc	{2475A66D-698B-4050-93FF-9B48EE82E2BA}

Utilisation des outils d'installation à distance des applications de Kaspersky Security Center pour lancer des fichiers exécutables arbitraires sur les appareils administrés

L'Assistant de création du paquet d'installation permet de choisir un fichier exécutable arbitraire et de définir pour celui-ci les paramètres de la ligne de commande. De plus, vous pouvez placer dans ce paquet d'installation le fichier sélectionné lui-même ou l'ensemble du dossier dans lequel ce fichier se trouve. Puis il faut créer la tâche d'installation à distance et choisir le paquet d'installation créé.

Lors de l'exécution de la tâche sur les appareils, le fichier exécutable indiqué à la création est lancé via la ligne de commande avec les paramètres définis.

En cas d'utilisation de programmes d'installation au format Microsoft Windows Installer (MSI), Kaspersky Security Center utilise les possibilités standard d'analyse du résultat de l'installation.

En présence d'une licence de Gestion des vulnérabilités et des correctifs, Kaspersky Security Center peut également utiliser les règles d'installation et d'analyse des résultats de l'installation, présents dans sa base mise à jour, lors de la création d'un paquet d'installation pour une des applications prises en charge et diffusées dans l'environnement de l'entreprise.

Dans d'autres cas, la tâche attend par défaut la fin du processus lancé et de tous ses processus enfants pour les fichiers exécutables. A la fin des processus lancés, la tâche réussit, quel que soit le code de retour du processus d'origine. Pour modifier ce comportement de tâche, avant la création de la tâche, vous devez modifier manuellement le fichier .kpd généré par Kaspersky Security Center dans le dossier et les sous-dosiers du paquet d'installation qui vient d'être créé.

Les fichiers .kpd utilisent le codage ASCII. Les fichiers .kud utilisent le codage Unicode.

Pour que la tâche n'attende pas la fin du processus lancé, il faut attribuer la valeur 0 au paramètre Wait dans la section [SetupProcessResult] :

```
[SetupProcessResult]
Wait=0
```

Sous Windows, pour que la tâche attende uniquement la fin du processus original et pas celle des processus enfant, il faut attribuer la valeur 0 au paramètres WaitJob dans la section [SetupProcessResult] :

```
[SetupProcessResult]
WaitJob=0
```

Pour que la tâche se termine correctement ou renvoie une erreur en fonction du code de retour du processus en cours d'exécution, créez un fichier .bat exécutable qui enregistre le code d'erreur dans un fichier, par exemple :

```
echo [ResponseResult] > setup.log
echo ResultCode=2 >> setup.log
exit 0
```

Modifiez ensuite les fichiers .kud générés par Kaspersky Security Center dans le dossier du paquet d'installation nouvellement créé :

```
[SetupMainResult]
File=setup.log
Section=ResponseResult
Value=ResultCode
[SetupMainResult_SuccessCodes]
0=Installation completed successfully.
[SetupMainResult_ErrorCodes]
1=Installation script error
2=Custom error
```

Dans ce cas, n'importe quel code différent des codes cités indique une erreur.

Pour que les résultats de la tâche reprennent une ligne avec un commentaire sur la réussite de la tâche ou un message d'erreur, il faut définir des descriptions brèves des erreurs correspondant aux codes de retour du processus dans les sections [SetupProcessResult_SuccessCodes] et [SetupProcessResult_ErrorCodes], par exemple :

```
[SetupProcessResult_SuccessCodes]
0= Installation completed successfully
3010=A reboot is required to complete the installation
[SetupProcessResult_ErrorCodes]
1602=Installation cancelled by the user
1603=Fatal error during installation
```

Pour que les outils de Kaspersky Security Center interviennent dans l'administration du redémarrage de l'appareil (si le redémarrage est nécessaire pour terminer l'opération), il faut énumérer en plus les codes de retour du processus qui indiquent la nécessité du redémarrage dans la section [SetupProcessResult_NeedReboot] :

```
[SetupProcessResult_NeedReboot]
3010=
```

Surveillance du déploiement

Pour contrôler le déploiement de Kaspersky Security Center et pour s'assurer de la présence sur les appareils administrés d'une application de sécurité et de l'Agent d'administration, vous devez vérifier l'indicateur de couleur dans la section **Déploiement**. L'indicateur se trouve dans l'espace de travail de l'entrée Serveur d'administration dans la fenêtre principale de la Console d'administration. L'indicateur affiche l'état actuel du déploiement. À côté de l'indicateur, on retrouve le nombre d'appareils dotés d'un Agent d'administration et d'applications de sécurité. En présence de tâches d'installation actives, l'état d'avancement de la tâche s'affiche. En cas d'erreur d'installation, le nombre d'erreurs apparaît ici. Pour voir les détails d'une erreur, cliquez sur le lien.

Vous pouvez également utiliser le diagramme de déploiement dans l'espace de travail du dossier **Appareils administrés** sous l'onglet **Groupes**. Le diagramme illustre le processus de déploiement : la quantité d'appareils sans Agent d'administration, avec Agent d'administration, avec Agent d'administration et application de sécurité.

Une description plus détaillée du déroulement du déploiement (ou de l'exécution d'une tâche d'installation en particulier) apparaît dans la fenêtre des résultats de l'exécution de la tâche correspondante d'installation à distance. La fenêtre des résultats est accessible via un clic droit et la sélection de **Résultats** dans le menu contextuel. La fenêtre propose deux listes : la liste du haut contient la liste des états de la tâche sur les appareils et la liste du bas reprend les événements de la tâche sur l'appareil sélectionné dans la liste du haut.

Les informations sur les erreurs de déploiement sont enregistrées dans le journal des événements Kaspersky sur le Serveur d'administration. Les informations sur les erreurs sont également accessibles dans la sélection d'événements correspondante dans le dossier **Rapports et notifications**, sous-dossier **Événements**.

Configuration des paramètres des programmes d'installation

La section contient des informations sur les fichiers des programmes d'installation de Kaspersky Security Center et sur les paramètres d'installation, ainsi que des recommandations sur l'installation du Serveur d'administration et l'Agent d'administration en mode « silencieux ».

Informations générales

Les programmes d'installation des composants de Kaspersky Security Center 15.1 (le Serveur d'administration, l'Agent d'administration et la Console d'administration) ont été élaborés selon les technologies Windows Installer. Le noyau du programme d'installation est un paquet MSI. Ce format d'empaquetage de la distribution permet d'utiliser tous les avantages de la technologie Windows Installer : montée en puissance, possibilité d'utiliser le système d'application de correctifs et le système de transformation, possibilité d'installer des solutions tierces de manière centralisée, transparence de l'enregistrement dans le système d'exploitation.

Installation en mode silencieux (avec fichier des réponses)

Les programmes d'installation du Serveur d'administration et de l'Agent d'administration permettent d'utiliser un fichier de réponses (ss_install.xml) qui contient les paramètres de l'installation en mode silencieux sans intervention de l'utilisateur. Le fichier ss_install.xml se trouve dans le même dossier que le paquet MSI et il est utilisé automatiquement lors de l'installation en mode silencieux. Vous pouvez activer le mode silencieux d'installation à l'aide de la touche de ligne de commande "/s".

Exemple de lancement :

```
setup.exe /s
```

Avant de lancer le programme d'installation en mode silencieux, lisez le Contrat de licence utilisateur final (CLUF). Si le kit de distribution Kaspersky Security Center ne contient pas de fichier TXT avec le texte du CLUF, vous pouvez télécharger le fichier depuis le site de Kaspersky.

Le fichier ss_install.xml représente le format interne des paramètres du programme d'installation de Kaspersky Security Center. Les paquets de la distribution reprennent le fichier ss_install.xml avec les paramètres par défaut.

Veuillez ne pas modifier le fichier ss_install.xml manuellement. Ce fichier est modifié à l'aide des outils de Kaspersky Security Center lors de la modification des paramètres des paquets d'installation dans la Console d'administration.

Pour modifier le fichier de réponses pour l'installation du Serveur d'administration :

1. Ouvrez le paquet de distribution de Kaspersky Security Center. Si vous utilisez un fichier EXE de paquet complet, décompressez-le.
2. Créez le dossier Server, ouvrez la ligne de commande, puis exécutez la commande suivante :
   ```
   setup.exe /r ss_install.xml
   ```
   Le programme d'installation de Kaspersky Security Center démarre.
3. Suivez les étapes de l'Assistant pour configurer l'installation de Kaspersky Security Center.

Lorsque vous avez terminé l'Assistant, le fichier de réponses est automatiquement modifié en fonction des nouveaux paramètres que vous avez définis.

Installation de l'Agent d'administration en mode silencieux (sans fichier des réponses)

L'Agent d'administration peut être installé à l'aide d'un seul paquet .msi, avec la définition des valeurs des propriétés MSI selon la méthode standard. Ce scénario permet d'installer l'Agent d'administration à l'aide de stratégies de groupe.

Ne renommez pas le paquet d'installation Kaspersky Network Agent.msi. Le fait de renommer ce paquet peut entraîner des erreurs d'installation lors de futures mises à jour de l'Agent d'administration.

Pour éviter tout conflit entre les paramètres définis à l'aide des propriétés MSI et les paramètres définis dans le fichier des réponses, il est possible de désactiver le fichier des réponses en définissant la propriété `DONT_USE_ANSWER_FILE=1`. Le fichier MSI se trouve dans le paquet de distribution de Kaspersky Security Center, dans le dossier Packages\NetAgent\exec. Vous trouverez ci-après un exemple de lancement du programme d'installation de l'Agent d'administration à l'aide du paquet .msi.

L'installation de l'Agent d'administration en mode silencieux requiert l'acceptation des dispositions du Contrat de licence utilisateur final (CLUF). Utilisez le paramètre `EULA=1` uniquement si vous avez entièrement lu, compris et accepté les conditions du Contrat de licence utilisateur final.

Exemple :
```
msiexec /i "Kaspersky Network Agent.msi" /qn DONT_USE_ANSWER_FILE=1 SERVERADDRESS=kscserver.mycompany.com EULA=1
```

Il est également possible de définir les paramètres d'installation du paquet msi en préparant au préalable un fichier de réponse (fichier avec l'extension mst). La commande ressemble à ceci :

Exemple :
```
msiexec /i "Kaspersky Network Agent.msi" /qn TRANSFORMS=test.mst;test2.mst
```

Plusieurs fichiers de transformation peuvent être indiqués dans une seule commande.

Si vous souhaitez mettre à niveau l'Agent d'administration à l'aide du programme d'installation de Windows, exécutez la commande suivante :

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
REINSTALL=ALL REINSTALLMODE=vomus /norestart
```

Configuration partielle des paramètres d'installation via setup.exe

Le lancement de 'installation des applications via setup.exe permet de transmettre au paquet MSI les valeurs de n'importe quelle propriété MSI.

La commande ressemble à ceci :

Exemple :
```
/v"PROPERTY_NAME1=PROPERTY_VALUE1 PROPERTYNAME2=PROPERTYVALUE2"
```

Paramètres d'installation du Serveur d'administration

Le tableau ci-après décrit les propriétés MSI que l'on peut configurer lors de l'installation du Serveur d'administration. Tous les paramètres sont facultatifs, à l'exception du Contrat de licence utilisateur final (EULA) et de la politique de confidentialité (PRIVACYPOLICY).

Propriété MSI	Description	Valeurs possibles
CLUF	Acceptation des conditions du Contrat de licence utilisateur final (paramètre obligatoire).	• 1 : j'ai entièrement lu, compris et accepté les conditions du Contrat de licence utilisateur final. • Une autre valeur ou non définie - Je refuse les conditions du Contrat de licence (l'installation n'aura pas lieu).
PRIVACYPOLICY	Acceptation des conditions de la Politique de confidentialité (paramètre obligatoire)	• 1—Je sais et j'accepte que mes données soient traitées et transmises (y compris à des pays tiers) comme décrit dans la Politique de confidentialité. Je confirme que j'ai entièrement lu et que je comprends la Politique de confidentialité. • Une autre valeur ou non définie - Je refuse les conditions de la Politique de confidentialité (l'installation n'aura pas lieu).
INSTALLATIONMODETYPE	Type d'installation du Serveur d'administration	• Standard. • Personnalisée.
INSTALLDIR	Dossier d'installation de l'application	Valeur de chaîne.
ADDLOCAL	Liste des modules à installer (séparés par une virgule).	CSAdminKitServer, NAgent, CSAdminKitConsole, NSAC, MobileSupport, KSNProxy, SNMPAgent, GdiPlusRedist, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86. Minimum suffisant pour l'installation correcte du Serveur d'administration dans la liste des modules : `ADDLOCAL=CSAdminKitServer, CSAdminKitConsole, KSNProxy, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86`
NETRANGETYPE	Taille du réseau.	• NRT_1_100 — de 1 à 100 appareils. • NRT_100_1000 : de 101 à 1000 appareils. • NRT_GREATER_1000 : plus de 1000 appareils.
SRV_ACCOUNT_TYPE	Mode de désignation de l'utilisateur pour le fonctionnement du service du Serveur d'administration.	• SrvAccountDefault : le compte utilisateur va être créé automatiquement. • SrvAccountUser : le compte utilisateur est créé manuellement.
SERVERACCOUNTNAME	Nom d'utilisateur pour le service.	Valeur de chaîne.
SERVERACCOUNTPWD	Mot de passe de l'utilisateur pour le service.	Valeur de chaîne.
DBTYPE	Type de la base de données.	• MySQL : une base de données MySQL ou MariaDB sera utilisée. • MSSQL : une base de données Microsoft SQL Server (SQL Express) sera utilisée.
MYSQLSERVERNAME	Nom complet du serveur MySQL ou MariaDB server	Valeur de chaîne.
MYSQLSERVERPORT	Le numéro de port pour se connecter au serveur MySQL ou MariaDB	Valeur numérique.
MYSQLDBNAME	Nom de la base de données du serveur MySQL ou MariaDB	Valeur de chaîne.
MYSQLACCOUNTNAME	Nom d'utilisateur pour la connexion à la base de données du serveur MySQL ou MariaDB	Valeur de chaîne.
MYSQLACCOUNTPWD	Mot de passe pour la connexion à la base de données du serveur MySQL ou MariaDB	Valeur de chaîne.
MSSQLCONNECTIONTYPE	Type d'utilisation de la base de données MSSQL.	• InstallMSSEE : installer à partir du paquet. • ChooseExisting : utiliser le serveur installé.
MSSQLSERVERNAME	Nom complet de l'instance de SQL Server.	Valeur de chaîne.

Propriété MSI	Description	Valeurs possibles
MSSQLDBNAME	Nom de la base de données de SQL Server.	Valeur de chaîne.
MSSQLAUTHTYPE	Mode d'authentification lors de la connexion à SQL Server.	• Windows. • SQLServer.
MSSQLACCOUNTNAME	Nom d'utilisateur pour la connexion à SQL Server en mode SQLServer.	Valeur de chaîne.
MSSQLACCOUNTPWD	Mot de passe de l'utilisateur pour la connexion à SQL Server en mode SQLServer.	Valeur de chaîne.

CREATE_SHARE_TYPE	Mode de définition du dossier partagé	• Create : créer un dossier partagé. Dans ce cas, il faut définir les propriétés :
		  • SHARELOCALPATH : le chemin d'accès au dossier local.
		  • SHAREFOLDERNAME : le nom de réseau du dossier.
		• Vide : il faut définir la propriété EXISTSHAREFOLDERNAME.

EXISTSHAREFOLDERNAME	Le chemin d'accès complet au dossier partagé existant.	Valeur de chaîne.
SERVERPORT	Le numéro de port pour se connecter au Serveur d'administration	Valeur numérique.
SERVERSSLPORT	Numéro de port pour l'établissement de la connexion SSL avec le Serveur d'administration.	Valeur numérique.
SERVERADDRESS	Adresse du Serveur d'administration	Valeur de chaîne.
SERVERCERT2048BITS	Longueur de la clé pour le certificat de Serveur d'administration (en bits)	• 1 : la longueur de la clé pour le certificat du Serveur d'administration est de 2048 bits. • 0 : la longueur de la clé pour le certificat du Serveur d'Administration est de 1024 bits. • Si la valeur n'est pas définie, la longueur de la clé pour le certificat du Serveur d'administration est de 2 048 bits.
MOBILESERVERADDRESS	Adresse du Serveur d'administration pour la connexion des appareils mobiles est ignoré si le module MobileSupport n'a pas été sélectionné.	Valeur de chaîne.

Paramètres d'installation de l'Agent d'administration

Le tableau ci-après décrit les propriétés MSI que l'on peut configurer lors de l'installation de l'Agent d'administration. Tous les paramètres sont facultatifs, à l'exception de SERVERADDRESS.

Propriétés de MSI

Propriété MSI	Description	Valeurs possibles
DONT_USE_ANSWER_FILE	Lire les paramètres d'installation dans le fichier des réponses	• 1 • Aucune valeur
INSTALLDIR	Dossier d'installation	
SERVERADDRESS	Adresse du Serveur d'administration (paramètre obligatoire)	
SERVERPORT	Numéro de port pour se connecter au Serveur d'administration	
SERVERSSLPORT	Numéro de port pour la connexion SSL	

Propriété MSI	Description	Valeurs possibles
USESSL	S'il faut utiliser la connexion SSL	• 1 • Aucune valeur
OPENUDPPORT	S'il faut ouvrir le port UDP	• 1 • Aucune valeur
UDPPORT	Numéro Port UDP	
USEPROXY	S'il faut utiliser le serveur proxy	• 1 • Aucune valeur
PROXYADDRESS	Adresse proxy	
PROXYPORT	Numéro de port pour se connecter au Serveur d'administration	
PROXYLOGIN	Compte utilisateur pour se connecter au serveur proxy	
PROXYPASSWORD	Mot de passe du compte pour la connexion au serveur proxy. N'indiquez pas dans les paramètres des paquets d'installation les données des comptes utilisateur privilégiés.	
GATEWAYMODE	Mode d'utilisation de la passerelle des connexions	• 0 : ne pas utiliser la passerelle de connexion • 1 : utiliser l'Agent d'administration donné en tant que passerelle de connexion • 2 : se connecter au Serveur d'administration via la passerelle de connexion
GATEWAYADDRESS	Adresse de la passerelle de connexion	
CERTSELECTION	Mode d'obtention du certificat	• GetOnFirstConnection : obtenir un certificat du Serveur d'administration. • GetExistent : sélectionner un certificat existant. Si cette option est sélectionnée, la propriété CERTFILE doit être définie.
CERTFILE	Chemin d'accès au certificat	
VMVDI	Activer le mode dynamique pour VDI	• 1 • Aucune valeur
LAUNCHPROGRAM	S'il faut lancer le service de l'Agent d'administration après l'installation	• 1 • Aucune valeur

Infrastructure virtuelle

Kaspersky Security Center prend en charge les machines virtuelles. Vous pouvez installer l'Agent d'administration et l'application de sécurité sur chaque machine virtuelle, et vous pouvez protéger les machines virtuelles au niveau de l'hyperviseur. Dans le premier cas, la protection des machines virtuelles peut être confiée à une application de sécurité standard ou à Kaspersky Security for Virtualization Light Agent. Dans le second cas, vous pouvez utiliser Kaspersky Security for Virtualization Agentless.

Kaspersky Security Center prend en charge le retour à l'état antérieur des machines virtuelles.

Recommandations sur la réduction de la charge sur les machines virtuelles

En cas d'installation de l'Agent d'administration sur une machine virtuelle, il faut envisager la possibilité de désactiver la partie des fonctions de Kaspersky Security Center qui ne sont pas très utiles aux machines virtuelles.

Lors de l'installation de l'Agent d'administration sur une machine virtuelle ou sur un modèle qui servira plus tard à créer des machines virtuelles, nous recommandons de réaliser les opérations suivantes :

- En cas d'installation à distance, sélectionnez l'option **Optimiser les paramètres pour VDI** dans la fenêtre des propriétés du paquet d'installation de l'Agent d'administration, dans la section **Avancé**.
- En cas d'installation interactive à l'aide de l'assistant, sélectionnez l'option **Optimiser les paramètres de l'Agent d'administration pour l'infrastructure virtuelle** dans la fenêtre de l'assistant.

En sélectionnant ces options, vous modifiez les paramètres de l'Agent d'administration afin que les fonctions suivantes soient désactivées par défaut (avant l'application d'une stratégie) :

- Réception d'informations sur les logiciels installés
- Réception d'informations sur la configuration matérielle
- Réception d'informations sur la présence de vulnérabilités
- Réception d'informations sur les mises à jour nécessaires

En général, les fonctions énumérées ne sont pas nécessaires sur les machines virtuelles dans la mesure où le logiciel et la configuration matérielle virtuelle sont homogènes.

Les fonctions peuvent être réactivées. Si n'importe laquelle des fonctions désactivées est malgré tout requise, elle peut être activée à l'aide d'une stratégie de l'Agent d'administration ou dans les paramètres locaux de l'Agent d'administration. Les paramètres locaux de l'Agent d'administration sont accessibles via le menu contextuel de l'appareil concerné dans la Console d'administration.

Prise en charge des machines virtuelles dynamiques

Kaspersky Security Center prend en charge les machines virtuelles dynamiques. Si une infrastructure virtuelle a été déployée sur le réseau de l'entreprise, il est possible d'utiliser dans certains cas des machines virtuelles dynamiques (temporaires). Ces machines sont créées avec des noms uniques au départ d'un modèle préparé par l'administrateur. L'utilisateur travaille un certain temps sur la machine créée et une fois désactivée, cette machine virtuelle disparaît de l'infrastructure virtuelle. Si Kaspersky Security Center a été déployé sur le réseau de l'entreprise, la machine virtuelle dotée de l'Agent d'administration est ajoutée à la base de données du Serveur d'administration. Une fois que machine virtuelle a été désactivée, son enregistrement doit également être supprimé de la base de données du Serveur d'administration.

Pour garantir le fonctionnement de la suppression automatique des enregistrements relatifs aux machines virtuelles, sélectionnez l'option **Activer le mode dynamique pour VDI** lors de l'installation de l'Agent d'administration sur le modèle qui va servir à la création des machines virtuelles dynamiques :

- En cas d'installation à distance : dans la fenêtre des propriétés du paquet d'installation de l'Agent d'administration (section **Avancé**)
- En cas d'installation interactive – dans l'assistant d'installation de l'Agent d'administration

Évitez de sélectionner l'option **Activer le mode dynamique pour VDI** lors de l'installation de l'Agent d'administration sur des appareils physiques.

Si les événements sur les machines virtuelles dynamiques doivent être conservés un certain temps sur le Serveur d'administration après la suppression des machines virtuelles, vous devez sélectionner l'option **Conserver les événements après la suppression des appareils** dans la section **Stockage d'événements** de la fenêtre des propriétés du Serveur d'administration, puis indiquer la durée de conservation maximale des événements en jours.

Nous vous déconseillons d'activer le chiffrement des disques sur les machines virtuelles dynamiques.

Prise en charge de la copie des machines virtuelles

Copier une machine virtuelle dotée de l'Agent d'administration ou la créer au départ d'un modèle doté de l'Agent d'administration est similaire au déploiement par prise d'une image du disque dur et copie de celui-ci. Pour cette raison, en général, lors de la copie de machines virtuelles, il faut réaliser les mêmes actions que lors du déploiement de l'Agent d'administration par copie d'une image du disque.

Cependant, dans les deux cas décrits ci-après, l'Agent d'administration détecte la copie automatiquement. Il n'est dès lors pas nécessaire d'exécuter les actions complexes décrites dans la section " Déploiement par prise d'image et copie d'image du disque dur de l'appareil " :

- Lors de l'installation de l'Agent d'administration, l'option **Activer le mode dynamique pour VDI** a été sélectionnée : après chaque redémarrage du système d'exploitation, cette machine virtuelle est considérée comme un nouvel appareil, qu'elle ait été copiée ou non.
- Utilisation d'un des hyperviseurs suivants : VMware™, HyperV® ou Xen® : l'Agent d'administration détermine l'opération de copie de la machine virtuelle à l'aide de la modification des indicateurs de la configuration matérielle virtuelle.

L'analyse des modifications de la configuration matérielle virtuelle n'est pas absolument sûre. Avant d'utiliser largement cette méthode, il faut d'abord confirmer son fonctionnement sur un nombre restreint de machines virtuelles pour la version de l'hyperviseur utilisée par l'entreprise.

Prise en charge de la restauration du système de fichiers pour les appareils dotés de l'Agent d'administration

Kaspersky Security Center est une application distribuée. La restauration du système de fichiers à un état antérieur sur un des appareils dotés de l'Agent d'administration entraîne une perte de la synchronisation des données et le fonctionnement incorrect de Kaspersky Security Center.

La restauration du système de fichiers (ou d'une de ses parties) à un état antérieur peut se produire dans les cas suivants :

- Lors de la copie de l'image du disque dur.
- Lors de la restauration de l'état de la machine virtuelle à l'aide des outils de l'infrastructure virtuelle.
- Lors de la restauration des données depuis la copie de sauvegarde ou du point de restauration.

S'agissant de Kaspersky Security Center, les seuls scénarios critiques sont ceux où un logiciel tiers sur les appareils dotés de l'Agent d'administration touche le dossier %ALLUSERSPROFILE %\Application Data\KasperskyLab\adminkit\. Pour cette raison, il faut veiller, dans la mesure du possible, à toujours exclure ce dossier de la procédure de restauration.

Vu que dans plusieurs entreprises, le règlement de travail prévoit la restauration de l'état du système de fichiers des appareils, Kaspersky Security Center, depuis la version 10 Maintenance Release 1 (le Serveur d'administration et les Agents d'administration doivent correspondre à la version 10 Maintenance Release 1 ou suivante), prend en charge la détection de la restauration du système de fichiers sur les appareils dotés de l'Agent d'administration. En cas de détection, ces appareils sont automatiquement reconnectés au Serveur d'administration avec un nettoyage et une synchronisation des données complets.

Dans Kaspersky Security Center 15.1, la prise en charge de la détection de la restauration du système de fichiers est activée par défaut.

Dans la mesure du possible, il faut éviter de restaurer le dossier %ALLUSERSPROFILE %\Application Data\KasperskyLab\adminkit\ sur les appareils dotés de l'Agent d'administration car la nouvelle synchronisation complète des données requiert un volume important de ressources.

La restauration de l'état du système n'est pas disponible sur les appareils dotés du Serveur d'administration. La restauration à l'état antérieur de la base de données utilisée par le Serveur d'administration est également impossible.

La restauration de l'état du Serveur d'administration au départ de la copie de sauvegarde est possible uniquement à l'aide de l'utilitaire standard klbackup.

À propos des profils de connexion pour les utilisateurs itinérants

Le travail des utilisateurs itinérants avec des ordinateurs portables (ci-après, les " appareils ") peut imposer une modification du mode de connexion au Serveur d'administration ou la permutation entre les Serveurs d'administration en fonction de la situation actuelle de l'appareil sur le réseau.

Les profils des connexions ne sont pris en charge que pour les appareils fonctionnant sous Windows et macOS.

Utilisation de différentes adresses du même Serveur d'administration

Les appareils dotés de l'Agent d'administration peuvent, à différents moments, se connecter au Serveur d'administration depuis le réseau interne de l'entreprise ou depuis Internet. Dans ce cas, il peut être nécessaire que l'Agent d'administration utilise différentes adresses pour la connexion au Serveur d'administration : l'adresse externe du Serveur pour la connexion depuis Internet et l'adresse interne du Serveur pour la connexion depuis le réseau interne.

Pour cela, vous devez ajouter un profil (pour la connexion au Serveur d'administration via Internet) à la stratégie de l'Agent d'administration. Ajoutez le profil dans les propriétés de la stratégie (section **Connectivité**, sous-section **Connexion**). Dans la fenêtre de création de profil, vous devez désactiver l'option **Utiliser uniquement pour récupérer les mises à jour** et sélectionner l'option **&Synchroniser les paramètres de connexion aux paramètres du Serveur d'administration indiqués dans ce profil**. Si l'accès au Serveur d'administration s'opère via une passerelle de connexion (cf. la configuration de Kaspersky Security Center de type Accès depuis Internet : Agent d'administration en tant que passerelle de connexion dans la zone démilitarisée), il faut indiquer l'adresse de la passerelle dans le champ correspondant.

Permutation entre les Serveurs d'administration en fonction du réseau actuel

Si la société compte plusieurs bureaux avec différents Serveurs d'administration et qu'une partie des appareils dotés de l'Agent d'administration se déplace entre ceux-ci, il faut que l'Agent d'administration puisse se connecter au Serveur d'administration du réseau local du bureau dans lequel l'appareil se trouve.

Dans ce cas, il faut créer un profil de connexion au Serveur d'administration pour chaque bureau dans les propriétés de la stratégie de l'Agent d'administration, à l'exception du bureau domestique où se trouve le Serveur d'administration domestique d'origine. Vous devez indiquer les adresses des Serveurs d'administration correspondants dans les profils de connexion et activer ou désactiver l'option **Utiliser uniquement pour récupérer les mises à jour** :

- Sélectionnez cette option si vous souhaitez que l'Agent d'administration soit synchronisé avec le Serveur d'administration domestique, tout en utilisant le Serveur local pour télécharger les mises à jour uniquement.
- Désactivez cette option si l'Agent d'administration doit être entièrement administré par le Serveur d'administration local.

Ensuite, il faut configurer les conditions de permutation vers les profils créés : pas moins d'une condition pour chacun des bureaux, à l'exclusion du "bureau domestique". L'idée de cette condition est de détecter dans l'environnement réseau des détails propres à un des bureaux. Si la condition se vérifie, le profil correspondant s'active. Si aucune des conditions ne se vérifie, l'Agent d'administration passe au Serveur d'administration domestique.

Déploiement de la fonction Administration des appareils mobiles

Cette section fournit des informations sur le déploiement initial de la Fonction Administration des appareils mobiles.

Connexion des appareils KES au Serveur d'administration

En fonction du mode de connexion des appareils au Serveur d'administration, il existe deux schémas de déploiement de Kaspersky Device Management for iOS pour les appareils KES :

- schéma de déploiement avec utilisation de la connexion directe des appareils au Serveur d'administration
- Schéma de déploiement impliquant un proxy inversé qui prend en charge la délégation restreinte Kerberos

Connexion directe des appareils au Serveur d'administration

Les appareils KES peuvent se connecter directement au port 13292 du Serveur d'administration.

En fonction du mode d'authentification, il existe deux options de connexion des appareils KES au Serveur d'administration :

- Connexion des appareils avec utilisation du certificat utilisateur
- Connexion des appareils sans certificat utilisateur

Connexion d'un appareil avec utilisation du certificat utilisateur

Lors de la connexion de l'appareil avec un certificat utilisateur, cet appareil est associé au compte utilisateur auquel les outils du Serveur d'administration ont attribué le certificat correspondant.

Dans ce cas, c'est l'authentification bilatérale SSL (authentification mutuelle) qui est utilisée. Aussi bien le Serveur d'administration que l'appareil sont authentifiés à l'aide de certificats.

Connexion d'un appareil sans certificat utilisateur

Lors de la connexion d'un appareil sans certificat utilisateur, l'appareil n'est associé à aucun compte utilisateur sur le Serveur d'administration. Mais dès que l'appareil reçoit un certificat quelconque, cet appareil est associé à l'utilisateur auquel les outils du Serveur d'administration ont attribué le certificat correspondant.

Lors de la connexion de l'appareil au Serveur d'administration, l'authentification utilisée est l'authentification unilatérale SSL (one-way SSL authentication) dans le cadre de laquelle seul le Serveur d'administration est authentifié à l'aide du certificat. Après l'appareil a reçu un certificat utilisateur, le type d'authentification devient l'authentification bilatérale SSL (2-way SSL authentication, mutual authentication).

Schéma de la connexion des appareils KES au serveur avec utilisation de la délégation forcée Kerberos (KCD)

Le schéma de connexion des appareils KES au Serveur d'administration avec utilisation de Kerberos Constrained Delegation (KCD) suppose :

- Intégration avec un proxy inversé qui prend en charge KCD.
- L'utilisation de la délégation forcée Kerberos Constrained Delegation (ci-après KCD) pour l'authentification des appareils mobiles.
- L'intégration à l'infrastructure à clés publiques (Public Key Infrastructure, ci-après) pour l'utilisation des certificats utilisateurs.

Lors de l'utilisation de ce schéma de connexion, il faut tenir compte des points suivants :

- Le type de connexion des appareils KES au proxy inversé doit être une authentification bilatérale SSL (« two-way SSL authentication »), à savoir que l'appareil doit se connecter au proxy inversé selon son certificat utilisateur. Pour cela, il faut intégrer le certificat utilisateur au paquet d'installation de Kaspersky Endpoint Security for Android installé sur l'appareil. Ce paquet KES doit être créé par le Serveur d'administration spécialement pour cet appareil (utilisateur).
- Au lieu du certificat de serveur, il faut indiquer par défaut pour le protocole mobile un certificat spécial (personnalisé) :

  1. Dans la section **Paramètres** de la fenêtre des propriétés du Serveur d'administration, cocher la case **Ouvrir le port pour les appareils mobiles**, puis choisir **Ajouter un certificat** dans la liste déroulante.
  2. Dans la fenêtre qui s'ouvre, indiquer le même certificat que celui désigné sur le proxy inversé lors de la publication du point d'accès au protocole mobile sur le Serveur d'administration.

- Les certificats utilisateurs pour les appareils KES doivent être émis par l'Autorité de certification du domaine (AC). De plus, il ne faut pas oublier que si le domaine compte plusieurs AC racine, les certificats utilisateurs doivent être émis par l'AC indiqué dans la publication sur le proxy inversé.

  Il existe plusieurs moyens pour garantir la conformité du certificat utilisateur avec l'exigence présentée ci-dessus :

  - Désigner le certificat utilisateur spécial dans l'Assistant de création du paquet d'installation et dans l'Assistant d'installation des certificats.
  - Intégrer le Serveur d'administration à la PKI du domaine et configurer le paramètre correspondant dans les règles d'émission des certificats :

    1. Dans l'arborescence de la console, développez le dossier **Administration des appareils mobiles** et sélectionnez le sous-dossier **Certificats**.
    2. Dans l'espace de travail du dossier **Certificats**, cliquez sur le bouton **Configurer les règles d'émission des certificats** pour ouvrir la fenêtre **Règles d'émission des certificats**.
    3. Configurez l'intégration à l'infrastructure à clé publique dans la section **Intégration avec PKI**.
    4. Dans la section **Émission des certificats de messagerie**, indiquez la source des certificats.

Voyons l'exemple de configuration de la délégation restreinte KCD avec les conditions suivantes :

- Le point d'accès au protocole mobile sur le Serveur d'administration est offert sur le port 13292.
- Le nom de l'appareil doté du proxy inversé est firewall.mydom.local.
- Le nom de l'appareil avec le Serveur d'administration est ksc.mydom.local.
- Le nom de la publication externe du point d'accès au protocole mobile est kes4mob.mydom.global.

Compte utilisateur de domaine pour le Serveur d'administration

Il faut créer un compte utilisateur de domaine (par exemple, KSCMobileSrvcUsr) sous lequel le service du Serveur d'administration va fonctionner. Il est possible d'indiquer le compte utilisateur du service du Serveur d'administration lors de l'installation du Serveur d'administration ou à l'aide de l'utilitaire klsrvswch. L'utilitaire klsrvswch se trouve dans le dossier d'installation du Serveur d'administration. Chemin d'installation par défaut : <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

Il faut désigner le compte utilisateur de domaine pour les raisons suivantes :

- La fonction d'administration des appareils KES est une partie intégrante du Serveur d'administration.
- Pour garantir le bon fonctionnement de la délégation forcée (KCD), la partie réceptrice, qui est le Serveur d'administration, doit fonctionner sous un compte utilisateur de domaine.

Service Principal Name pour http/kes4mob.mydom.local

Dans le domaine, il faut prescrire sous le compte utilisateur KSCMobileSrvcUsr Service Principal Name (SPN) pour la publication du service du protocole mobile sur le port 13292 de l'appareil avec le Serveur d'administration. Pour l'appareil kes4mob.mydom.local avec le Serveur d'administration, cela ressemble à ceci :

```
setspn -a http/kes4mob.mydom.local:13292 mydom\KSCMobileSrvcUsr
```

Configuration des propriétés du domaine de l'appareil doté du proxy inversé (firewall.mydom.local)

Pour déléguer le trafic, il faut confier l'appareil avec le proxy inversé (firewall.mydom.local) au service défini selon SPN (http/kes4mob.mydom.local:13292).

Pour confier l'appareil avec le proxy inversé au service défini selon SPN (http/kes4mob.mydom.local:13292), l'administrateur doit exécuter les actions suivantes :

1. Dans le module logiciel enfichable de Microsoft Management Console "Active Directory Users and Computers", il faut choisir l'appareil doté du proxy inversé (firewall.mydom.local).
2. Dans les propriétés de l'appareil, sous l'onglet **Delegation**, choisir l'option **Use any authentication protocol** pour le commutateur **Trust this computer for delegation to specified service only**.
3. Dans la liste **Services to which this account can present delegated credentials** ajouter SPN http/kes4mob.mydom.local:13292.

Certificat spécial (personnalisé) pour la publication (kes4mob.mydom.global)

Pour la publication du protocole mobile du Serveur d'administration il faut octroyer un certificat spécial (personnalisé) au nom de domaine complet kes4mob.mydom.global et le désigner en substitution au certificat serveur par défaut dans les paramètres du protocole mobile du Serveur d'administration dans la Console d'administration. Pour cela, dans la section **Paramètres** de la fenêtre des propriétés du Serveur d'administration, il faut cocher la case **Ouvrir le port pour les appareils mobiles**, puis choisir **Ajouter un certificat** dans la liste déroulante.

N'oubliez pas que le conteneur où se trouve le certificat serveur (fichier avec extension p12 ou pfx) doit également contenir la chaîne de certificats racines (les parties publiques).

Configuration de la publication sur le pare-feu d'entreprise

Sur le proxy inversé, pour le trafic allant du côté de l'appareil mobile sur le port 13292 port kes4mob.mydom.global, il faut configurer KCD sur SPN kes4mob.mydom.global:13292 avec l'utilisation du certificat serveur émis pour le nom de domaine complet kes4mob.mydom.global. N'oubliez pas qu'il faut prévoir le même certificat serveur pour les publications et pour le point d'accès publié (port 13292 du Serveur d'administration).

Utilisation de Firebase Cloud Messaging

Pour une livraison opportune des commandes sur les appareils KES sous le système d'exploitation Android, le mécanisme des notifications push est utilisé dans Kaspersky Security Center. Les notifications push entre les appareils KES et le Serveur d'Administration sont échangées à l'aide de Firebase Cloud Messaging (ci-après dénommé FCM). La Console d'administration de Kaspersky Security Center permet d'indiquer les paramètres du service Firebase Cloud Messaging pour connecter les appareils KES à ce service.

Pour obtenir les paramètres de Firebase Cloud Messaging, vous devez avoir un compte utilisateur Google.

Pour activer FCM, procédez comme suit :

1. Dans la Console d'administration, sélectionnez l'entrée **Administration des appareils mobiles**, puis le dossier **Appareils mobiles**.
2. Dans le menu contextuel du dossier **Appareils mobiles**, sélectionnez l'option **Propriétés**.
3. Dans les propriétés du dossier, sélectionnez la section **Paramètres de Firebase Cloud Messaging**.
4. Dans le champ **Numéro de projet Firebase**, indiquez l'identificateur de l'expéditeur de FCM.
5. Dans le champ **Fichier clé privé (au format JSON)**, sélectionnez le fichier de clé privée.

   Lors de la synchronisation suivantes avec le Serveur d'administration, les appareils administrés KES sous le système d'exploitation Android seront connectés au service Firebase Cloud Messaging.

Vous pouvez modifier les paramètres de Firebase Cloud Messaging à l'aide du bouton **Abandonner les paramètres**.

Lorsque vous passez à un autre projet Firebase, vous devez attendre 10 minutes que FCM reprenne.

Le service FCM fonctionne sur les plages d'adresses suivantes :

- Du côté de l'appareil KES, il faut octroyer l'accès aux ports 443 (HTTPS), 5228 (HTTPS), 5229 (HTTPS), 5230 (HTTPS) des adresses suivantes :
  - google.com
  - fcm.googleapis.com
  - android.apis.google.com
  - ou sur toutes les adresses IP de la liste " Google ASN 15169 "
- Du côté du Serveur d'administration, il faut octroyer l'accès sur le port 443 (HTTPS) des adresses suivantes :
  - fcm.googleapis.com
  - ou sur toutes les adresses IP de la liste « Google ASN 15169 »

Si les paramètres du serveur proxy ont été définis dans les propriétés du Serveur d'administration de la Console d'administration (**Avancé** / **Paramètres d'accès au réseau Internet**), ils seront utilisés pour coopérer avec FCM.

Configuration de FCM : obtention de l'identificateur de l'expéditeur et du fichier de clé privée

Pour configurer FCM, procédez comme suit :

1. S'inscrire sur le portail Google.
2. Accéder à la console Firebase.
3. Exécutez une des actions suivantes :
   - Pour créer un projet, cliquez sur **Créer un projet** et suivez les instructions à l'écran.
   - Ouvrez un projet existant.
4. Cliquez sur l'icône en forme d'engrenage et choisissez **Paramètres du projet**.

   La fenêtre **Paramètres du projet** s'ouvre.
5. Sélectionnez l'onglet **Messagerie Cloud**.
6. Récupérez l'identificateur de l'expéditeur dans le champ **Identificateur de l'expéditeur** dans la section **API de Firebase Cloud Messaging (V1)**.
7. Sélectionnez l'onglet **Comptes de services** et cliquez sur **Générer une nouvelle clé privée**.
8. Dans la fenêtre qui s'ouvre, cliquez sur **Générer une clé** pour générer et télécharger un fichier de clé privée.

Firebase Cloud Messaging est maintenant configuré.

Intégration avec l'infrastructure à clé publique

L'intégration à l'infrastructure à clés publiques (Public Key Infrastructure, ensuite PKI) sert avant tout à simplifier l'émission des certificats utilisateurs de domaine par le Serveur d'administration.

L'administrateur peut attribuer à l'utilisateur un certificat de domaine dans la Console d'administration. Pour cela, il a le choix entre les méthodes suivantes :

- Attribuer à l'utilisateur un certificat spécial (personnalisé) depuis un fichier dans l'Assistant d'installation des certificats.
- Exécuter l'intégration avec PKI et désigner la PKI comme source du certificat pour le type concret de certificat ou pour tous les types de certificat.

Les paramètres d'intégration avec PKI sont accessibles dans l'espace de travail du dossier **Administration des appareils mobiles** / **Certificats** via le lien **Intégrer à l'infrastructure de clés ouvertes**.

Principe général de l'intégration avec PKI pour l'émission des certificats de domaine des utilisateurs

Dans la Console d'administration, cliquez sur le lien **Intégrer à l'infrastructure de clés ouvertes** de l'espace de travail du dossier **Administration des appareils mobiles** / **Certificats** pour désigner le compte de domaine que le Serveur d'administration va utiliser pour émettre les certificats utilisateurs de domaine via l'AC de domaine (ci-après, le compte utilisateur sous lequel l'intégration avec PKI a lieu).

Il faut tenir compte des points suivants :

- Dans les paramètres de l'intégration avec PKI, il est possible de désigner une modèle par défaut pour tous les types de certificat. Sachez que les règles d'émission des certificats (disponibles dans l'espace de travail du dossier **Administration des appareils mobiles** / **Certificats** en cliquant sur le bouton **Configurer les règles d'émission des certificats**) permettent de définir un modèle pour chaque type de certificat séparément.
- Sur l'appareil doté du Serveur d'administration, le certificat spécial Enrollment Agent (EA) doit être installé dans le stockage des certificats du compte utilisateur sous lequel l'intégration avec PKI a lieu. Le certificat Enrollment Agent (EA) est émis par l'administrateur de l'AC (autorité de certification) de domaine.

Le compte utilisateur sous lequel l'intégration avec PKI a lieu doit répondre aux critères suivants :

- Est l'utilisateur de domaine.
- Est l'administrateur local de l'appareil doté du Serveur d'administration depuis lequel l'intégration avec PKI a lieu.
- Possède le droit *Connexion en tant que service*.
- Pour créer le profil permanent de l'utilisateur, il faut lancer au moins une fois sous ce compte utilisateur l'appareil doté du Serveur d'administration.

Serveur Web de Kaspersky Security Center

Le Serveur Web de Kaspersky Security Center (si après le Serveur Web) est un module de Kaspersky Security Center. Le Serveur Web intervient dans la publication des paquets d'installation autonomes, des paquets d'installation autonomes pour les appareils mobiles, ainsi que des fichiers du dossier partagé.

Les paquets d'installation créés sont publiés automatiquement sur le Serveur Web et sont supprimés après le premier chargement. L'administrateur peut transférer à l'utilisateur le lien formé à l'aide d'un moyen commode quelconque, par exemple, via email.

A l'aide du lien reçu, l'utilisateur peut télécharger les informations sur l'appareil mobile.

Paramètres du Serveur Web

Pour permettre la configuration approfondie du Serveur Web, les propriétés du Serveur Web prévoient la possibilité de remplacer les ports pour les protocoles HTTP (8060) et HTTPS (8061). De plus, outre la substitution des ports, il est possible de substituer le certificat serveur pour le protocole HTTPS et de remplace le nom de domaine complet du Serveur Web pour le protocole HTTP.

Autres travaux de routine

Cette section contient des recommandations sur l'utilisation quotidienne de Kaspersky Security Center.

Surveillance des indicateurs de couleur et des événements consignés dans la Console d'administration

La Console d'administration permet d'évaluer rapidement l'état actuel de Kaspersky Security Center et des appareils administrés grâce à des indicateurs de couleur. Les indicateurs s'affichent dans l'espace de travail de l'entrée **Serveur d'administration** sous l'onglet **Surveillance**. L'onglet affiche six panneaux d'information avec des indicateurs de couleur et les événements enregistrés. Un feu de circulation est une barre verticale colorée sur le côté gauche d'un panneau. Chaque bloc avec un indicateur est consacré à une zone fonctionnelle distincte de Kaspersky Security Center (cf. le tableau ci-dessous).

Zones de responsabilité des indicateurs de couleur dans la Console d'administration

Nom du panneau	Zone de responsabilité de l'indicateur de couleur
Déploiement	Installation de l'Agent d'administration et des applications de sécurité sur les appareils du réseau de l'organisation
Structure d'administration	Structure des groupes d'administration. Sondage de réseau. Règles de déplacement des appareils
Configuration de la protection	Fonctions de l'application de sécurité : état de la protection, analyse des logiciels malveillants
Mise à jour	Mises à jour et correctifs
Surveillance	État de la protection
Serveur d'administration	Fonctions et propriétés du Serveur d'administration

L'indicateur peut être une des cinq couleurs suivantes (cf. le tableau ci-après). La couleur de l'indicateur dépend de l'état actuel de Kaspersky Security Center et des événements enregistrés.

Codes couleur des indicateurs

État	Couleur de l'indicateur	Valeur de la couleur de l'indicateur
Pour information	Vert	L'intervention de l'administrateur n'est pas requise
Avertissement	Jaune	L'intervention de l'administrateur est requise.
Critique	Rouge	Des problèmes importants sont survenus. Leur résolution requiert l'intervention de l'administrateur.
Pour information	Bleu	Enregistrement d'événements non liés à des menaces potentielles ou réelles pour la sécurité des appareils administrés.
Pour information	Gris	Les détails relatifs aux événements ne sont pas disponibles ou n'ont pas encore été récupérés.

L'objectif de l'administrateur est que les témoins de couleur sur tous les panneaux d'informations de l'onglet **Surveillance** soient verts.

Le panneau d'informations affiche également les événements enregistrés ayant un impact sur l'indicateur et l'état de Kaspersky Security Center (cf. le tableau ci-dessous).

Nom, description et couleurs des indicateurs de couleur des événements enregistrés

Couleur de l'indicateur	Nom affiché du type d'événement	Type d'événement	Description
Rouge	**La licence a expiré sur %1 appareil(s)**	IDS_AK_STATUS_LIC_EXPAIRED	Des événements de ce type se produisent lorsque la licence commerciale a expiré. Une fois par jour, Kaspersky Security Center vérifie si la licence n'a pas expiré sur les appareils. À l'expiration de la licence commerciale, Kaspersky Security Center ne fournit que les fonctionnalités de base. Pour continuer à utiliser Kaspersky Security Center, renouvelez la licence commerciale.
Rouge	**Application de sécurité désactivée : %1 appareils**	IDS_AK_STATUS_AV_NOT_RUNNING	Des événements de ce type se produisent lorsque l'application de sécurité installée sur l'appareil ne fonctionne pas. Assurez-vous que Kaspersky Endpoint Security est exécuté sur l'appareil.
Rouge	**La protection n'est pas lancée : %1 appareils**	IDS_AK_STATUS_RTP_NOT_RUNNING	Des événements de ce type se produisent lorsque l'application de sécurité sur l'appareil est désactivée pendant plus longtemps que la durée indiquée. Vérifiez l'état actuel de la protection en temps réel sur l'appareil et assurez-vous que tous les modules de protection dont vous avez besoin sont activés.
Rouge	**Une vulnérabilité a été découverte dans les applications des appareils**	IDS_AK_STATUS_VULNERABILITIES_FOUND	Des événements de ce type se produisent lorsque la tâche *Recherche de vulnérabilités et de mises à jour requises* a détecté des vulnérabilités avec le niveau de gravité indiqué dans les applications installées sur l'appareil. Consultez la liste des mises à jour disponibles dans le sous-dossier **Mises à jour du logiciel** inclus dans le dossier **Gestion des applications**. Ce dossier contient la liste des mises à jour obtenues par le Serveur d'administration des applications de Microsoft et d'autres éditeurs du logiciel qui peuvent être diffusées sur les appareils. Après la consultation des informations sur les mises à jour disponibles, installez-les sur l'appareil.

Couleur de l'indicateur	Nom affiché du type d'événement	Type d'événement	Description
Rouge	**Des événements critiques ont été enregistrés sur le Serveur d'administration**	IDS_AK_STATUS_EVENTS_OCCURED	Les événements de ce type se produisent en cas d'événements critiques du Serveur d'administration détectés. Consultez la liste des événements enregistrée sur le Serveur d'administration, puis corrigez les événements critiques un par un.
Rouge	**Des erreurs ont été enregistrées dans des événements sur le Serveur d'administration**	IDS_AK_STATUS_ERROR_EVENTS_OCCURED	Des événements de ce type se produisent lorsque des erreurs inattendues sont enregistrées du côté du Serveur d'administration. Consultez la liste des événements enregistrée sur le Serveur d'administration, puis corrigez les erreurs une par une.
Rouge	**La connexion avec %1 appareils est perdue**	IDS_AK_STATUS_ADM_LOST_CONTROL1	Des événements de ce type se produisent lorsque la connexion entre le Serveur d'administration et l'appareil est perdue. Consultez la liste des appareils déconnectés et essayez de les reconnecter.
Rouge	**%1 appareil(s) n'ont pas connecté(s) au Serveur d'administration depuis longtemps**	IDS_AK_STATUS_ADM_NOT_CONNECTED1	Des événements de ce type se produisent lorsque l'appareil ne s'est pas connecté au Serveur d'administration dans l'intervalle de temps indiqué, car l'appareil était éteint. Assurez-vous que l'appareil est sous tension et que l'Agent d'administration est en cours d'exécution.
Rouge	**Il existe %1 appareils avec l'état différent de OK**	IDS_AK_STATUS_HOST_NOT_OK	Des événements de ce type se produisent lorsque l'état *OK* de l'appareil connecté au Serveur d'administration devient *Critique* ou *Avertissement*. Vous pouvez résoudre le problème à l'aide de l'utilitaire de diagnostic à distance de Kaspersky Security Center.
Rouge	**Les bases sont dépassées sur : %1 appareil(s)**	IDS_AK_STATUS_UPD_HOSTS_NOT_UPDATED	Des événements de ce type se produisent lorsque les bases antivirus n'ont pas été mises à jour sur l'appareil dans les intervalles de temps indiqués. Suivez les instructions pour mettre à jour les bases de Kaspersky.
Rouge	**Appareil(s) sur lesquels la vérification des mises à jour Windows Update n'a pas été effectuée depuis longtemps : %1**	IDS_AK_STATUS_WUA_DATA_OBSOLETE	Des événements de ce type se produisent lorsque la tâche *Synchronisation des mises à jour Windows Update* n'a pas été exécutée dans l'intervalle de temps spécifié. Suivez les instructions pour synchroniser les mises à jour de Windows Update avec le Serveur d'administration.
Rouge	**L'installation de %1 plug-in(s) pour Kaspersky Security Center est requise**	IDS_AK_STATUS_PLUGINS_REQUIRED2	Des événements de ce type se produisent lorsque vous devez installer des plug-ins supplémentaires pour les applications de Kaspersky. Téléchargez et installez les plug-ins d'administration de l'application Kaspersky nécessaires à partir du site du Support Technique de Kaspersky.

Accès à distance aux appareils administrés

Cette section contient des informations sur l'accès à distance aux appareils administrés.

Utilisation de l'option "Maintenir la connexion au Serveur d'administration" pour fournir une connexion permanente entre un appareil administré et le Serveur d'administration

Si vous n'utilisez pas de serveurs push, Kaspersky Security Center ne fournit pas de connexion permanente entre les appareils administrés et le Serveur d'administration. Les agents d'administration sur les appareils administrés établissent périodiquement une connexion et se synchronisent avec le Serveur d'administration. L'intervalle entre ces sessions de synchronisation est défini dans une stratégie de l'Agent d'administration. Si une synchronisation s'impose plus tôt, le Serveur d'administration (ou un point de distribution, s'il est en cours d'utilisation) envoie un paquet réseau signé sur un réseau IPv4 ou IPv6 vers le port UDP de l'Agent d'administration. Le numéro de port est de 15000 par défaut. Si aucune connexion via UDP entre le Serveur d'administration et l'appareil administré n'est possible, la synchronisation se déroulera lors de la prochaine connexion ordinaire de l'Agent d'administration au Serveur d'administration pendant l'intervalle de synchronisation.

Certaines opérations ne peuvent pas être exécutées sans connexion anticipée de l'Agent d'administration au Serveur d'administration, telles que le lancement et l'arrêt des tâches locales, la réception des statistiques de l'application administrée ou la création d'un tunnel. Pour résoudre ce problème, si vous n'utilisez pas de serveurs push, vous pouvez utiliser l'option **Maintenir la connexion au Serveur &d'administration** pour s'assurer qu'il existe une connectivité continue entre un appareil administré et le Serveur d'administration.

Pour assurer une connexion permanente entre un appareil administré et le Serveur d'administration :

1. Dans l'arborescence de la console sélectionnez le dossier **Appareils administrés**.
2. Dans l'espace de travail du dossier, sélectionnez l'appareil administré avec lequel vous souhaitez assurer une connexion permanente.
3. Dans le menu contextuel de l'appareil, sélectionnez l'option **Propriétés**.

   La fenêtre des propriétés de l'appareil sélectionné s'ouvre.
4. Dans la section **Général** de la fenêtre affichée, sélectionnez l'option **Maintenir la connexion au Serveur &d'administration**.

La connexion permanente est établie entre l'appareil administré et le Serveur d'administration.

Le total des appareils pour lesquels l'option **Maintenir la connexion au Serveur &d'administration** a été sélectionnée ne peut être supérieur à 300.

À propos de la vérification de la durée de connexion de l'appareil avec le Serveur d'administration

Lors de la désactivation de l'appareil, l'Agent d'administration signale celle-ci au Serveur d'administration. Dans la Console d'administration, cet appareil apparaît comme désactivé. Cependant l'Agent d'administration ne parvient pas toujours à informer le Serveur d'administration. C'est pourquoi le Serveur d'administration analyse à intervalle régulier pour chaque appareil l'attribut **Connexion au Serveur d'administration** (la valeur de l'attribut s'affiche dans la Console d'administration, dans la section **Général** des propriétés de l'appareil) et le compare à la période de synchronisation des paramètres actifs de l'Agent d'administration. Si l'appareil n'a pas établi de communication pendant plus de trois périodes de synchronisation, cet appareil est signalé comme désactivé.

À propos de la synchronisation forcée

Malgré le fait que Kaspersky Security Center synchronise automatiquement l'état, les paramètres, les tâches et les stratégies pour les appareils administrés, il existe des cas où l'administrateur doit savoir exactement si la synchronisation de cette appareil a eu lieu à ce moment.

Dans le menu contextuel des appareils administrés de la Console d'administration, l'option de menu **Toutes les tâches** contient la commande **Forcer la synchronisation**. Quand Kaspersky Security Center 15.1 exécute cette commande, le Serveur d'administration tente de contacter l'appareil. Si cette tentative réussit, la synchronisation forcée a lieu. Dans le cas contraire, la synchronisation ne sera forcée qu'après la prochaine connexion prévue entre l'Agent d'administration et le Serveur d'administration.

À propos du tunneling

Kaspersky Security Center permet d'établir des connexions TPC en tunnel depuis la Console d'administration via le Serveur d'administration et puis via l'Agent d'administration vers le port défini sur l'appareil administré. Le tunnel est utilisé pour connecter une app cliente qui se trouve sur un appareil doté de la Console d'administration au port TCP sur l'appareil administré si la connexion directe de l'appareil avec la Console d'administration et l'appareil n'est pas possible.

Plus particulièrement, le tunnel est utilisé pour établir une connexion à un poste de travail distant : aussi bien pour la connexion à une session en cours que pour la création d'une nouvelle session à distance.

Le tunnel peut également être utilisé à l'aide du mécanisme des outils externes. Ainsi, l'administrateur peut lancer de la sorte l'utilitaire putty, un client VNC et d'autres outils.

Guide de dimensionnement

Cette section fournit des informations sur la mise à l'échelle de Kaspersky Security Center.

Présentation du manuel

Le guide de dimensionnement de Kaspersky Security Center 15.1 (ci-après aussi Kaspersky Security Center) est destiné aux experts chargés de l'installation et de l'administration de Kaspersky Security Center, et aux spécialistes un support technique au sein des organisations qui utilisent Kaspersky Security Center.

Toutes les recommandations et tous les calculs sont donnés pour les réseaux où Kaspersky Security Center administre la protection des appareils avec le logiciel Kaspersky installé, y compris des appareils mobiles. Si des appareils mobiles ou d'autres appareils administrés doivent être pris en compte séparément, cette mention est indiquée spécifiquement.

Pour atteindre et conserver les performances optimales dans les conditions d'utilisation les plus diverses, vous devez tenir compte du nombre d'appareils dans le réseau, la topologie du réseau et des fonctions de Kaspersky Security Center dont vous avez besoin.

Le manuel contient les informations suivantes :

- Restrictions de Kaspersky Security Center
- Calculs des nœuds clés de Kaspersky Security Center (Serveurs d'administration et points de distribution) :
  - Configuration matérielle des Serveurs d'administration et des points de distribution
  - Calcul du nombre et de la hiérarchie des Serveurs d'administration
  - Calcul du nombre et de la configuration des points de distribution
- Configuration des paramètres d'enregistrement des événements dans la base de données en fonction du nombre d'appareils dans le réseau
- Meilleures pratiques générales pour l'optimisation des performances
- Configuration des paramètres de certaines tâches pour une performance optimale de Kaspersky Security Center
- Consommation du trafic (charge sur le réseau) entre le Serveur d'administration de Kaspersky Security Center et chaque appareil protégé.

Il est recommandé de consulter ce manuel dans les cas suivants :

- Pour la planification des ressources avant l'installation de Kaspersky Security Center
- Pour la planification de changements importants sur la taille du réseau dans lequel Kaspersky Security Center est déployé

- Lors du passage de l'utilisation de Kaspersky Security Center dans un segment de réseau limité (environnement de test) au déploiement à grande échelle de Kaspersky Security Center sur le réseau d'entreprise
- Pour les modifications de l'ensemble des fonctionnalités utilisées par Kaspersky Security Center

Informations sur les restrictions de Kaspersky Security Center

Le tableau ci-après reprend les restrictions de la version actuelle de Kaspersky Security Center.

Restrictions de Kaspersky Security Center

Type de restriction	Valeur
Nombre maximal d'appareils administrés par un Serveur d'administration	100 000
Nombre maximum d'appareils pour lesquels l'option **Maintenir la connexion au Serveur d'administration** est sélectionnée	300
Nombre maximum des groupes d'administration	10 000
Nombre maximum d'événements enregistrés	45 000 000
Nombre maximum de stratégies	2000
Nombre maximum de tâches	2000
Nombre total maximum d'objets Active Directory (unités organisationnelles (OUs) et comptes utilisateurs, appareils et groupes de sécurité)	1 000 000
Nombre maximum de profils dans une stratégie	100
Nombre maximum de Serveurs d'administration secondaires pour un Serveur d'administration principal	500
Nombre maximum de Serveurs d'administration virtuels	500
Nombre maximum d'appareils qu'un point de distribution peut couvrir (les points de distribution ne peuvent couvrir que des appareils non mobiles)	10 000
Nombre maximum d'appareils qui peuvent utiliser une passerelle de connexion unique	10 000, y compris des appareils mobiles
Nombre maximal d'appareils mobiles sur un Serveur d'administration	100 000, moins le nombre d'appareils administrés fixes

Calculs pour les Serveurs d'administration

Cette section donne les exigences logicielles et matérielles applicables aux appareils utilisés comme Serveurs d'administration, Elle fournit également des recommandations sur le calcul du nombre de serveurs d'administration et de leur hiérarchie en fonction de la configuration du réseau de l'organisation.

Calcul des ressources matérielles pour le Serveur d'administration

Cette section donne les calculs servant à guider la planification des ressources matérielles pour le Serveur d'administration. On trouve séparément des recommandations de calcul de l'espace sur le disque lors de l'utilisation de la fonctionnalité Gestion des vulnérabilités et des correctifs.

Configuration matérielle pour le SGBD et le Serveur d'administration

Les tableaux suivants indiquent la configuration matérielle minimale recommandée pour un SGBD et un Serveur d'administration obtenus lors des tests. Pour obtenir la liste complète des systèmes d'exploitation et des SGBD pris en charge, consultez la liste Configuration logicielle et matérielle.

Le Serveur d'administration et SGBD se trouvent sur des appareils, dans un réseau de 50 000 appareils

Configuration de l'appareil avec le Serveur d'administration

Matériel	Valeur
Processeur	4 noyaux, 2500 MHz
Mémoire vive	8 Go
Disque dur	300 Go, RAID souhaité
Adaptateur réseau	1 Gbit

Configuration de l'appareil sur lequel le SGBD est installé

Matériel	Valeur
Processeur	4 noyaux, 2500 MHz
Mémoire vive	16 Go
Disque dur	200 Go, SATA RAID
Adaptateur réseau	1 Gbit

Le Serveur d'administration et SGBD sont sur le même appareil dans un réseau de 50 000 appareils

Configuration de l'appareil avec le Serveur d'administration et SGBD

Matériel	Valeur
Processeur	8 noyaux, 2500 MHz
Mémoire vive	16 Go
Disque dur	500 Go, SATA RAID
Adaptateur réseau	1 Gbit

Le Serveur d'administration et SGBD se trouvent sur des appareils, dans un réseau de 100 000 appareils

Configuration de l'appareil avec le Serveur d'administration

Matériel	Valeur
Processeur	8 noyaux, 2,13 GHz
Mémoire vive	8 Go
Disque dur	1 To avec RAID
Adaptateur réseau	1 Gbit

Configuration de l'appareil avec SGBD installé

Matériel	Valeur
Processeur	8 noyaux, 2,53 GHz
Mémoire vive	26 Go
Disque dur	500 Go, SATA RAID
Adaptateur réseau	1 Gbit

Le test s'est passé avec les configurations suivantes :

- L'assignation automatique des points de distribution est activée sur le Serveur d'administration, ou les points de distribution sont assignés manuellement selon le tableau recommandé.
- La tâche de sauvegarde enregistre les copies de sauvegarde sur une ressource fichier qui se trouve sur un serveur distinct
- La période de synchronisation des Agents d'administration est configurée conformément au tableau ci-après.

  Période de synchronisation des Agents d'administration

Période de synchronisation, minutes	Nombre des appareils administrés
15	10 000
30	20 000
45	30 000
60	40 000
75	50 000
150	100 000

Calcul de l'espace dans la base de données

La formule suivante permet d'évaluer l'espace occupé par la base de données :

(600 * C + 2.3 * E + 2.5 * A + 1.2 * N * F), Ko

où :

- C représente le nombre d'appareils.
- " E " représente le nombre d'événements enregistrés.
- " A " représente le nombre d'objets d'Active Directory :
  - Comptes utilisateurs d'appareils
  - Comptes utilisateurs
  - Comptes utilisateurs du groupe de sécurité
  - Sous-sections Active Directory

  Si l'analyse d'Active Directory est désactivée, " A " sera environ égal à zéro.

- N est le nombre moyen de fichiers exécutables inventoriés sur un terminal.
- F est le nombre d'appareils d'extrémité, où les fichiers exécutables ont été inventoriés.

Si vous envisagez d'inclure dans les paramètres de la stratégie de Kaspersky Endpoint Security l'information du Serveur d'administration sur les applications lancées, l'enregistrement des informations sur les applications lancées dans la base de données nécessitera (0,03 * C) gigaoctets.

Si le Serveur d'administration publie les mises à jour de Windows (joue le rôle du serveur Windows Server Update Services), 2,5 Go supplémentaires seront nécessaires dans la base de données.

Pendant l'utilisation, il se forme toujours ce que l'on appelle de l'*espace non alloué* (unallocated space) dans la base de données. C'est pourquoi la taille réelle d'un fichier de la base de données (par défaut le fichier KAV.MDF si vous utilisez le SGBD « serveur SQL ») est souvent deux fois supérieure à l'espace occupé dans la base de données.

Il n'est pas recommandé de limiter explicitement la taille du journal des transactions (par défaut le fichier KAV_log.LDF, si vous utilisez SQL Server comme SGBD). Il est recommandé de conserver la valeur par défaut du paramètre MAXSIZE. Cependant, si vous devez limiter la taille de ce fichier, prenez en compte le fait que la valeur minimale généralement requise du paramètre MAXSIZE de KAV_log.LDF est de 20480 Mo.

Calcul de l'espace sur le disque (avec et sans utilisation de la Gestion des vulnérabilités et des correctifs)

Calcul de l'espace sur le disque sans tenir compte de l'utilisation de la fonctionnalité Gestion des vulnérabilités et des correctifs

L'espace sur le disque du Serveur d'administration requis pour le dossier %ALLUSERSPROFILE %\Application Data\KasperskyLab\adminkit peut être approximativement estimé selon la formule :

(724 * C + 0.15 * E + 0.17 * A), Ko

où :

- C représente le nombre d'appareils.
- " E " représente le nombre d'événements enregistrés.
- " A " représente le nombre d'objets d'Active Directory :
  - Comptes utilisateurs d'appareils
  - Comptes utilisateurs
  - Comptes utilisateurs du groupe de sécurité
  - Sous-sections Active Directory

Si l'analyse d'Active Directory est désactivée, « A » sera environ égal à zéro.

Calcul de l'espace supplémentaire sur le disque en tenant compte de l'utilisation de la fonctionnalité Gestion des vulnérabilités et des correctifs

- Mises à jour. Le dossier partagé requiert au moins 4 Go supplémentaires pour le stockage des mises à jour.
- Paquets d'installation. Si des paquets d'installation se trouvent dans le dossier partagé du Serveur d'administration, il faut prévoir un volume égal au total du volume des paquets d'installation hébergés à installer.
- Tâches de l'installation à distance. En présence de tâches d'installation à distance sur le Serveur d'administration, il faut également avoir sur le disque (dossier %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit) un espace égal à la taille totale des paquets d'installation à installer.
- Correctifs. Si le Serveur d'administration est utilisé pour installer des correctifs, il faut prévoir de l'espace en plus sur le disque :
  - Dans le dossier de stockage des correctifs, l'espace doit être égal à la taille total de l'ensemble des correctifs téléchargés. Par défaut, les correctifs sont enregistrés dans le dossier %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\.working\wusfiles.

    Vous pouvez utiliser l'utilitaire klsrvswch pour spécifier un dossier différent pour enregistrer les correctifs. L'utilitaire klsrvswch se trouve dans le dossier dans lequel le Serveur d'administration est installé. Chemin d'installation par défaut : <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

    Si le Serveur d'administration est utilisé en tant que WSUS, il est conseillé de réserver pour ce dossier au moins 100 Go.
  - Dans le dossier %ALLUSERSPROFILE %\Application Data\KasperskyLab\adminkit : espace égal à la taille totale des correctifs auxquels font référence les instances existantes de la tâche d'installation des mises à jour (correctifs) et de correction des vulnérabilités.

Calcul du nombre et de la configuration des Serveurs d'administration

Pour réduire la charge sur le Serveur d'administration principal, vous attribuez à chaque groupe d'administration un Serveur d'administration séparé. Le nombre de Serveurs d'administration secondaires soumis à un Serveur d'administration principal ne peut pas excéder 500.

Il est recommandé de procéder à la configuration des Serveurs d'administration en fonction de la manière dont le réseau est organisé dans votre organisation.

Recommandations pour la connexion des machines virtuelles dynamiques à Kaspersky Security Center

Les machines virtuelles dynamiques (également appelées machines virtuelles dynamiques) consomment plus de ressources que les machines virtuelles statiques.

Pour plus d'informations sur les machines virtuelles dynamiques, consultez Prise en charge des machines virtuelles dynamiques.

Lorsqu'une nouvelle VM dynamique est connectée, Kaspersky Security Center crée une icône pour cette VM dynamique dans la Console d'administration et déplace la VM dynamique vers le groupe d'administration. Ensuite, la VM dynamique est ajoutée à la base de données du Serveur d'administration. Le Serveur d'administration est entièrement synchronisé avec l'Agent d'administration installé sur cette VM dynamique.

Dans le réseau d'une organisation, l'Agent d'administration crée les listes de réseaux suivantes pour chaque VM dynamique :

- Matériel
- Logiciels installés
- Vulnérabilités détectées
- Événements et listes de fichiers exécutables du module Contrôle des applications

L'Agent d'administration transfère ces listes de réseaux au Serveur d'administration. La taille des listes de réseaux dépend des modules installés sur la machine virtuelle dynamique et peut affecter les performances de Kaspersky Security Center et du système d'administration de base de données (SGBD). Notez que la charge peut croître de manière non linéaire.

Une fois que l'utilisateur a terminé de travailler avec la machine virtuelle dynamique et l'a éteinte, cette machine est supprimée de l'infrastructure virtuelle et les entrées concernant cette machine sont supprimées de la base de données du Serveur d'administration.

Toutes ces actions consomment beaucoup de ressources de la base de données de Kaspersky Security Center et du Serveur d'administration et peuvent réduire les performances de Kaspersky Security Center et du SGBD. Nous vous recommandons de connecter jusqu'à 20 000 VM dynamiques à Kaspersky Security Center.

Vous pouvez connecter plus de 20 000 VM dynamiques à Kaspersky Security Center si les VM dynamiques connectées effectuent des opérations standard (par exemple, des mises à jour de bases de données) et ne consomment pas plus de 80 % de la mémoire et 75 à 80 % des noyaux disponibles.

La modification des paramètres de la stratégie, du logiciel ou du système d'exploitation sur la machine virtuelle dynamique peut réduire ou augmenter la consommation de ressources. La consommation de 80 à 95 % des ressources est considérée comme optimale.

Calculs pour les points de distribution et les passerelles de connexion

Cette section donne les exigences matérielles applicables aux appareils utilisés comme points de distribution, et les recommandations pour calculer le nombre de points de distribution et les passerelles de connexion en fonction de l'agencement du réseau de l'organisation.

Exigences d'un point de distribution

Pour pouvoir traiter un maximum de 10 000 appareils clients, un point de distribution doit répondre à la configuration suivante (une configuration pour banc d'essai est fournie) :

- Processeur : Intel® Core™ i7-7700 CPU, 3,60 GHz 4 noyaux.
- Mémoire vive : 8 Go.
- Espace de stockage disponible : 120 Go.

Il n'est pas recommandé de désigner le Serveur d'administration comme point de distribution, car la charge sur le Serveur d'administration augmentera.

En présence, sur le Serveur d'administration, de tâches d'installation à distance, l'appareil avec le point de distribution demande en plus une quantité d'espace sur le disque égale à la taille totale des paquets d'installation installés.

En présence sur le Serveur d'administration d'un ou plusieurs exemplaires de tâches d'installation des mises à jour (correctifs) et de correction des vulnérabilités, l'appareil avec le point de distribution demande en plus une quantité d'espace sur le disque égale à la taille totale de tous les correctifs installés.

Si vous utilisez le schéma dans lequel les points de distribution reçoivent les mises à jour des bases et des modules d'application directement depuis les serveurs de mise à jour de Kaspersky, les points de distribution doivent être connectés à Internet.

Calcul de la quantité et de la configuration des points de distribution

Plus un réseau compte d'appareils clients, plus le nombre de points de distribution requis augmente. Il est recommandé de ne pas désactiver la définition automatique des points de distribution. Lorsque la définition automatique des points de distribution est activée, le Serveur d'administration désigne les points de distribution si le nombre des appareils clients est assez élevé, et définit leur configuration.

Utilisation de points de distribution assignés exclusivement

Si vous envisagez d'utiliser des ensembles d'appareils (à savoir, des serveurs affectés de manière exclusive) en tant que points de distribution, vous pouvez ne pas utiliser la définition automatique des points de distribution. Dans ce cas, assurez-vous que les appareils dont vous souhaitez faire des points de distribution disposent de suffisamment d'espace libre sur le disque, qu'ils ne sont pas régulièrement éteints et que le " mode veille " est désactivé.

Nombre de points de distribution exclusivement attribués sur un réseau qui contient un segment unique, sur la base du nombre d'appareils en réseau

Nombre d'appareils clients administrés dans le segment du réseau	Nombre des points de distribution
Moins de 300	0 (ne pas assigner de points de distribution)
Plus de 300	Acceptable : (N/10 000 + 1), recommandé : (N/5 000 + 2), où N représente le nombre d'appareils sur le réseau

Nombre de points de distribution exclusivement attribués sur un réseau qui contient plusieurs segments, sur la base du nombre d'appareils en réseau

Nombre d'appareils clients par segment de réseau	Nombre des points de distribution
Moins de 10	0 (ne pas assigner de points de distribution)
10–100	1
Plus de 100	Acceptable : (N/10 000 + 1), recommandé : (N/5 000 + 2), où N représente le nombre d'appareils sur le réseau

Utilisation d'appareils clients standard (postes de travail) en tant que points de distribution

Si vous avez l'intention d'utiliser des appareils clients standard (à savoir, des postes de travail) en tant que points de distribution, nous vous conseillons de les désigner comme dans les tableaux ci-dessous afin d'éviter une charge excessive des canaux de communication et du Serveur d'administration :

Nombre de postes de travail servant de points de distribution sur un réseau qui contient un segment unique, sur la base du nombre d'appareils en réseau

Nombre d'appareils clients administrés dans le segment du réseau	Nombre des points de distribution
Moins de 300	0 (ne pas assigner de points de distribution)
Plus de 300	(N/300 +1), où N est le nombre des appareils sur le réseau ; il doit y avoir au moins 3 points de distribution

Nombre de postes de travail servant de points de distribution sur un réseau qui contient plusieurs segments, sur la base du nombre d'appareils en réseau

Nombre d'appareils clients par segment de réseau	Nombre des points de distribution
Moins de 10	0 (ne pas assigner de points de distribution)
10–30	1
31–300	2
Plus de 300	(N/300 +1), où N est le nombre des appareils sur le réseau ; il doit y avoir au moins 3 points de distribution

Si un point de distribution est éteint (ou indisponible pour toute autre raison), les appareils administrés situés dans sa zone d'action peuvent accéder au Serveur d'administration pour les mises à jour.

Calcul du nombre de passerelles de connexion

Si vous envisagez d'utiliser une passerelle de connexion, nous vous recommandons de désigner un appareil spécial pour cette fonction.

Une passerelle de connexion peut couvrir un maximum de 10 000 appareils administrés, y compris les appareils mobiles.

Conservation des événements pour les tâches et les stratégies

Cette section donne les calculs liés à la conservation des événements dans la base de données du Serveur d'administration, ainsi que des recommandations sur la manière de minimiser le nombre d'événements et ainsi réduire la charge sur le Serveur d'administration.

Par défaut les propriétés de chaque tâche et stratégie indiquent l'enregistrement dans le journal de tous les événements liés à l'exécution de la tâche et à l'application de la stratégie.

Cependant, si la tâche est lancée assez souvent (par exemple, plus d'une fois par semaine) et sur un nombre assez important d'appareils (par exemple, plus de 10 000), le nombre d'événements peut s'avérer trop important, et les événements peuvent remplir la base de données. Dans pareil cas, il est recommandé d'indiquer dans les propriétés de la tâche une des deux autres options :

- **Sauvegarder les événements relatifs à la progression de la tâche**. Dans ce cas, la base de données reçoit uniquement des informations sur le lancement, la progression et l'achèvement de la tâche (succès, avec un avertissement ou une erreur) de chaque appareil sur lequel la tâche est exécutée.

- **Sauvegarder uniquement le résultat de la tâche**. Dans ce cas, à partir de chaque appareil sur lequel est exécutée la tâche, seules les informations sur l'exécution de la tâche (réussi, avec avertissement ou avec erreur) arrivent dans la base de données.

Si la stratégie est définie pour un nombre assez grand d'appareils (par exemple, plus de 10 000), le nombre d'événements peut s'avérer aussi trop grand et les événements peuvent remplir la base de données. Dans pareil cas, il est recommandé de choisir dans les propriétés de la stratégie seulement les événements les plus importants et d'activer leur enregistrement. Il est recommandé de désactiver l'enregistrement de tous les autres événements.

Ainsi, vous diminuez le nombre d'événements dans la base de données, vous augmentez la vitesse de fonctionnement des scénarios liés à l'analyse du tableau des événements dans la base de données, et vous réduisez le risque que les événements critiques soient ignorés.

Vous pouvez également réduire la durée de stockage des événements liés à la tâche ou à la stratégie. Par défaut, ce délai est de 7 jours pour les événements liés à la tâche, et de 30 jours pour les événements liés à la stratégie. Lors de la modification de la durée de stockage des événements, prenez en compte la manière de travailler de votre organisation, et le temps que l'administrateur système peut consacrer à l'analyse de chaque événement.

Il est judicieux d'apporter des modifications dans les paramètres d'enregistrement des événements dans chacun des cas suivants :

- Les événements liés aux modifications des états intermédiaires des tâches de groupe et les événements liés à l'application des stratégies occupent une grande partie de tous les événements de la base de données de Kaspersky Security Center.

- Dans le journal des événements Kaspersky apparaissent des enregistrements sur la suppression automatique des événements lors du dépassement de la limite spécifiée du nombre général des événements conservés dans la base de données.

Choisissez les options d'enregistrement des événements dans le journal sur la base de l'hypothèse selon laquelle le nombre d'événements optimal en provenance d'un seul appareil ne doit pas dépasser 20 par jour. Vous pouvez augmenter cette limite légèrement, le cas échéant, mais uniquement si le nombre d'appareils sur votre réseau est relativement faible (inférieur à 10 000).

Particularités et paramètres optimums de certaines tâches

Certaines tâches présentent des particularités liées au nombre d'appareils dans le réseau. Cette section donne des recommandations de configuration optimale des paramètres de ces tâches.

La recherche d'appareils, la tâche de sauvegarde des données, la tâche de maintenance du Serveur d'administration et les tâches de groupe de la mise à jour de Kaspersky Endpoint Security font partie des fonctionnalités de base de Kaspersky Security Center.

Fréquence de la recherche d'appareils

Il n'est pas recommandé d'augmenter la fréquence par défaut de recherche d'appareils installés par défaut puisque cela peut créer une charge excessive sur les contrôleurs du domaine. Il est au contraire recommandé de programmer le sondage le moins souvent possible, selon les besoins de votre organisation. Le tableau ci-dessous formule des recommandations de calcul de la programmation optimale.

Programmation de la recherche d'appareils

Nombre d'appareils sur le réseau	Fréquence de la recherche d'appareils recommandée
Moins de 10 000	Définie par défaut ou moins souvent
10 000 et plus	Une fois par jour ou moins souvent

Tâches de sauvegarde des données du Serveur d'administration et de maintenance du Serveur d'administration

Le Serveur d'administration cesse de fonctionner pendant l'exécution des tâches suivantes :

- Sauvegarde des données du Serveur d'administration
- Maintenance du Serveur d'administration

Pendant que ces tâches sont exécutés, les données ne peuvent pas accéder à la base de données.

Vous pouvez avoir besoin de modifier la programmation de ces tâches de manière à ce que leur exécution ne coïncide pas avec l'exécution d'autres tâches du Serveur d'administration.

Tâches de groupe de mise à jour de Kaspersky Endpoint Security

Si le Serveur d'administration est la source des mises à jour, pour les tâches de groupe de mise à jour de Kaspersky Endpoint Security version 10 et suivante, il est recommandé de procéder à la programmation **Lors du téléchargement des mises à jour dans le stockage** avec la case **Utiliser un délai aléatoire automatique pour le démarrage des tâches** cochée.

Si vous avez créé une tâche locale de téléchargement des mises à jour dans le stockage depuis les serveurs de Kaspersky sur chaque point de distribution, la solution optimale recommandée pour la tâche de groupe de mise à jour de Kaspersky Endpoint Security est la planification périodique. La valeur de la période de allocation aléatoire doit être dans ce cas d'une heure.

Tâche d'inventaire

Vous pouvez réduire la charge sur la base de données tout en obtenant des informations sur les fichiers exécutables. Pour ce faire, il est recommandé d'exécuter une tâche d'inventaire pour Kaspersky Endpoint Security sur les appareils de référence sur lesquels un ensemble standard de logiciels est installé.

Le nombre de fichiers exécutables reçus par le Serveur d'administration d'un appareil ne peut pas dépasser 150 000. Une fois cette restriction atteinte, Kaspersky Security Center ne recevra pas de nouveaux fichiers.

Le nombre de fichiers sur un appareil client normal n'est en général pas supérieur à 60 000. Le nombre de fichiers exécutables sur le serveur de fichier peut être supérieur, voire dépasser le seuil de 150 000.

Les mesures de test ont montré que sur un appareil fonctionnant sous le système Windows 7 sur lequel est installée l'application Kaspersky Endpoint Security 11 et où aucune application tierce n'est installée, les résultats de l'exécution de la tâche d'inventaire sont les suivants :

- Quand les cases **Inventaire des modules DDL** et **Inventaire des fichiers de script** sont décochées : environ 3 000 fichiers.
- Avec Inventaire **les cases des modules** DLL Inventaire **des fichiers de** script cochées, de 10 000 à 20 000 fichiers, en fonction du nombre de mises à jour du système d'exploitation installées.
- Avec la case **Inventaire des fichiers de script** cochée, près de 10 000 fichiers.

Informations sur la charge sur le réseau entre le Serveur d'administration et les appareils protégés

Cette section vous donne les résultats des mesures de test du trafic au niveau du réseau en indiquant les conditions dans lesquelles les mesures ont été effectuées. Vous pouvez utiliser ces informations comme référence lors de la planification de l'infrastructure réseau et la capacité de service des canaux à l'intérieur de l'organisation (ou entre le Serveur d'administration et l'organisation où les appareils protégés sont disposés). En connaissant la capacité de service du réseau, vous pouvez approximativement estimer aussi le temps que mettra une opération de transmission de données.

Débit du trafic lors de l'exécution de divers scénarios

Le tableau ci-dessous donne les résultats des mesures de test du trafic entre le Serveur d'administration et l'appareil administré lors de l'exécution de divers scénarios.

La synchronisation de l'appareil avec le Serveur d'administration s'effectue par défaut une fois toutes les 15 minutes ou moins souvent. Cependant si vous modifiez les paramètres de la stratégie ou d'une tâche sur le Serveur d'administration, il se produit une synchronisation anticipée des appareils pour lesquels cette stratégie (tâche) est appliquée et les nouveaux paramètres sont transférés sur les appareils.

Trafic entre le Serveur d'administration et l'appareil administré

Scénario	Trafic du Serveur d'administration vers chaque appareil administré	Trafic de chaque appareil administré vers le Serveur d'administration
Installation de Kaspersky Endpoint Security 11.7 for Windows avec des bases mises à jour	390 Mo	3.3 Mo
Installation de l'Agent d'administration	75 Mo	397 Ko
Installation collective de l'Agent d'administration et de Kaspersky Endpoint Security 11.7 for Windows	459 Mo	3.6 Mo
Mise à jour initiale des bases antivirus sans mise à jour des bases dans le paquet (en cas de refus de participation à Kaspersky Security Network)	113 Mo	1,8 Mo
Mise à jour quotidienne des bases antivirus (en cas de participation à Kaspersky Security Network)	22 Mo	373 Mo
Synchronisation initiale jusqu'à la mise à jour des bases de données sur l'appareil (transfert des stratégies et des tâches)	382 Ko	446 Ko
Synchronisation initiale après la mise à jour des bases de données sur l'appareil	20 Ko	157 Ko
Synchronisation en l'absence de modifications sur le Serveur d'administration (selon la planification)	18 Ko	23 Ko
Synchronisation en cas de modification d'un paramètre de la stratégie du groupe (anticipée, immédiatement après la saisie de la modification)	19 Ko	20 Ko
Synchronisation en cas de modification d'un paramètre de la tâche de groupe (anticipée, immédiatement après la saisie de la modification)	14 Ko	11 Ko
Synchronisation forcée	110 Ko	109 Ko
Événement **Virus détecté** (1 virus)	44 Ko	50 Ko
Événement **Virus détecté** (10 virus)	58 Ko	77 Ko
Trafic unique après l'activation de la liste du Registre des applications	jusqu'à 10 Ko	jusqu'à 12 Ko
Trafic quotidien lorsque la liste du Registre des applications est activée	jusqu'à 840 Ko	jusqu'à 1 Mo

Débit moyen du trafic par 24 heures

L'utilisation moyenne du trafic sur 24 heures entre le Serveur d'administration et un appareil administré est la suivante :

- Le trafic du Serveur d'administration vers l'appareil administré est de 840 Ko.
- Le trafic de l'appareil administré vers le Serveur d'administration est de 1 Mo.

Le trafic a été mesuré dans les conditions suivantes :

- L'Agent d'administration et Kaspersky Endpoint Security 11.6 for Windows ont été installés sur l'appareil administré.
- L'appareil n'était pas assigné comme point de distribution.

- La fonctionnalité Gestion des vulnérabilités et des correctifs n'était pas activée.
- La période de synchronisation avec le Serveur d'administration était de 15 minutes.

Contacter le Support Technique

Cette section décrit comment profiter du support technique et les conditions d'accès à celui-ci.

Façons de profiter du support technique

Si vous ne trouvez pas de solution à votre problème dans la documentation de Kaspersky Security Center ou dans les sources d'information relatives à Kaspersky Security Center, contactez le Support technique de Kaspersky. Les experts du support technique répondront à toutes vos questions concernant l'installation et l'utilisation de Kaspersky Security Center.

Kaspersky apporte un soutien en relation avec Kaspersky Security Center pendant son cycle de vie (voir la page du cycle de vie du support de l'application). Avant de contacter le Support Technique, il est recommandé de lire les règles d'octroi du support technique.

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

- En vous rendant sur le site Internet du Support Technique
- En envoyant une demande au Support Technique via le portail Kaspersky CompanyAccount

Support technique via le Kaspersky CompanyAccount

Kaspersky CompanyAccount est un portail dédié aux entreprises utilisant les applications Kaspersky. Le portail Kaspersky CompanyAccount vise à permettre l'interaction entre les utilisateurs et les spécialistes de Kaspersky via des requêtes en ligne. Vous pouvez utiliser Kaspersky CompanyAccount pour suivre l'état des requêtes en ligne et en stocker également un historique.

Vous pouvez enregistrer tous les employés de votre entreprise dans un seul compte utilisateur Kaspersky CompanyAccount. Ce compte utilisateur unique vous permet de centraliser l'administration des requêtes électroniques envoyées à Kaspersky et provenant des employés enregistrés. Il vous permet également d'administrer les privilèges de ces employés 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 le Kaspersky CompanyAccount, veuillez consulter le site Internet du Service de Support Technique.

Obtention des fichiers de vidage du Serveur d'administration

Les fichiers de vidage du Serveur d'administration contiennent toutes les informations relatives aux processus du Serveur d'administration à un moment donné. Les fichiers de vidage du Serveur d'administration sont stockés dans le dossier %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\~dumps. Les fichiers de vidage sont conservés tant que Kaspersky Security Center est utilisé et sont supprimés définitivement après sa suppression. Les fichiers de vidage ne sont pas envoyés automatiquement à Kaspersky.

Si le Serveur d'administration tombe en panne, vous pouvez contacter le Support technique de Kaspersky. Le Support technique peut vous demander d'envoyer les fichiers de vidage du Serveur d'administration pour une analyse plus approfondie chez Kaspersky.

Les fichiers de vidage peuvent contenir des données personnelles. Il est recommandé de protéger vos informations contre tout accès non autorisé avant de les envoyer à Kaspersky.

Sources d'informations sur l'application

Page Kaspersky Security Center sur le site Internet de Kaspersky

La page Kaspersky Security Center sur le site Internet de Kaspersky fournit des informations générales sur l'application, ses possibilités, et ses particularités.

Page Kaspersky Security Center dans la Base de connaissances

La *Base de connaissances* est une section du site Internet du Support Technique de Kaspersky.

La page Kaspersky Security Center dans la Base de connaissances comporte des articles qui proposent des informations utiles, des recommandations et des réponses aux questions fréquemment posées sur l'achat, l'installation et l'utilisation de l'application.

Les articles de la Base de connaissances peuvent répondre à des questions relatives à Kaspersky Security Center et à d'applications de Kaspersky. Les articles de la Base de connaissances peuvent également contenir des actualités du Support Technique.

Discuter des applications Kaspersky avec la communauté

Si votre question n'est pas urgente, vous pouvez la poser aux experts de Kaspersky et aux autres utilisateurs de notre forum.

Le forum vous permet d'afficher des sujets de discussion, d'envoyer des commentaires et de créer de nouveaux sujets de discussion.

> L'accès aux sites Internet requiert une connexion à Internet.

Si vous ne trouvez pas la solution à votre problème, contactez le Support Technique.

Glossaire

Administrateur de Kaspersky Security Center

Personne qui gère les opérations de l'application via le système d'administration centralisé à distance Kaspersky Security Center.

Administrateur du client

L'employé de l'entreprise cliente qui contrôle l'état de la protection antivirus de l'entreprise cliente.

Administrateur du prestataire de services

L'employé de la société-prestataire de services de protection antivirus. Exécute les travaux d'installation et d'exploitation des systèmes de protection antivirus créés sur la base des produits antivirus de Kaspersky, ainsi que le support technique des clients.

Administration centralisée des applications

Administration à distance des applications à l'aide des services d'administration proposés par Kaspersky Security Center.

Agent d'administration

le module de l'application Kaspersky Security Center qui coordonne les interactions entre le Serveur d'administration et les applications Kaspersky installées sur un poste spécifique du réseau (un poste de travail ou un serveur). Ce module est commun à toutes les applications de l'entreprise développées pour Microsoft® Windows®. Il existe d'autres versions de l'Agent d'administration pour les applications Kaspersky développées pour les SE Unix et MacOS.

Agent d'authentification

Interface permettant après le chiffrement du disque dur de chargement de passer la procédure d'authentification pour accéder aux disques durs chiffrés et charger le système d'exploitation.

Appareil KES

Appareil mobile qui se connecte au Serveur d'administration de Kaspersky Security Center et est administré à l'aide de Kaspersky Endpoint Security for Android.

Appareil MDM iOS

Appareil mobile qui se connecte au Serveur MDM iOS via le protocole MDM iOS. Le protocole MDM iOS permet de connecter et d'administrer les appareils ayant un système d'exploitation iOS.

Appareil protégé au niveau UEFI

Appareil doté au niveau BIOS d'une solution ou d'une application Kaspersky pour UEFI. La protection intégrée assure la sécurité de l'appareil au début du lancement du système quand la protection des appareils qui ne sont pas dotés de l'application intégrée commence à fonctionner uniquement après le lancement de l'application de sécurité.

Appareils administrés

Les appareils du réseau inclus dans un groupe d'administration.

Application incompatible

Application antivirus d'un éditeur tiers ou application de Kaspersky qui n'est pas compatible avec l'administration par Kaspersky Security Center.

Attaque MITM

Attaque de l'homme du milieu. Attaque contre l'infrastructure informatique d'une organisation dans laquelle un pirate informatique détourne le lien de communication entre deux points d'accès, le relaie et modifie si nécessaire la connexion entre ces points d'accès.

AWS Application Program Interface (AWS API)

Interface logicielle de l'application de la plateforme AWS utilisée par l'application Kaspersky Security Center. Les outils de l'API AWS effectuent notamment un sondage des segments dans le Cloud et l'installation de l'Agent d'administration sur les instances.

Base antivirus

Bases de données contenant des informations sur les menaces informatiques connues de Kaspersky au moment de la publication des bases antivirus. Les entrées dans les bases antivirus permettent de détecter les codes malveillants dans les objets analysés. Les bases antivirus sont créées par les experts de Kaspersky et sont actualisées toutes les heures.

Boutique des apps

Module de l'application Kaspersky Security Center. La boutique des apps est utilisée pour l'installation d'apps sur les appareils Android des utilisateurs. Dans la boutique d'apps, on peut publier les fichiers apk des apps et les liens vers les apps dans Google Play.

Certificat du Serveur d'administration

Le certificat que le Serveur d'administration utilise aux fins suivantes :

- Authentification du Serveur d'administration lors de la connexion à une Console d'administration MMC ou à Kaspersky Security Center Web Console
- Interaction sécurisée entre le Serveur d'administration et les Agents d'administration sur les appareils administrés
- Authentification des Serveurs d'administration lors de la connexion d'un Serveur d'administration primaire à un Serveur d'administration secondaire

Le certificat est créé automatiquement lors de l'installation du Serveur d'administration et puis sauvegardé sur le Serveur d'administration.

Certificat général

Certificat conçu pour identifier l'appareil mobile de l'utilisateur.

Clé active

Une clé en cours d'utilisation par l'application.

Clé d'accès AWS IAM

Combinaison comprenant l'identifiant de la clé (de type " AKIAIOSFODNN7EXAMPLE ") et la clé secrète (de type " wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY "). Une paire appartient à l'utilisateur IAM et est utilisée pour avoir accès aux services AWS.

Clé de licence complémentaire (ou de réserve)

La clé qui confirme le droit d'utilisation de l'application, mais non utilisée au moment actuel.

Client du Serveur d'administration (Appareil client)

Appareil, serveur ou poste de travail sur lequel l'Agent d'administration est installé, ainsi que les applications administrées de Kaspersky.

Cloud

Les machines virtuelles et les autres ressources virtuelles qui reposent sur une plateforme Cloud et qui sont réunies en réseaux.

Cloud Discovery

Cloud Discovery est un module de la solution Cloud Access Security Broker (CASB) qui protège l'infrastructure cloud d'une organisation. Cloud Discovery gère l'accès des utilisateurs aux services cloud. Les services cloud incluent, par exemple, Microsoft Teams, Salesforce et Microsoft Office 365. Les services cloud sont regroupés en catégories, par exemple, *Échange de données*, *Messageries*, *Email*.

Console d'administration

Module de Kaspersky Security Center pour Windows (également appelé Console d'administration basée sur MMC). Ce module fournit une interface utilisateur pour les services d'administration du Serveur d'administration et de l'Agent d'administration.

Console de gestion AWS

L'interface Internet pour voir et administrer les ressources AWS. La console de gestion AWS est accessible sur Internet à la page https://aws.amazon.com/console/.

Domaine multicast

Segment logique de réseau informatique dans lequel tous les nœuds peuvent se transmettre des données mutuellement à l'aide d'un canal multidiffusion au niveau du modèle réseau OSI (Open Systems Interconnection Basic Reference Model).

Dossier de sauvegarde

Dossier spécial pour la conservation des copies des données du Serveur d'administration, créées à l'aide de l'utilitaire de copie de sauvegarde.

Durée de validité de la licence

Période au cours de laquelle vous pouvez utiliser les fonctions de l'application et les services complémentaires. Le volume des fonctions accessibles et des services complémentaires dépend du type de licence.

État de la protection

État actuel de la protection qui représente le niveau de sécurité de l'ordinateur.

État de la protection du réseau

L'état actuel de la protection qui caractérise le niveau de sécurité des appareils du réseau de l'entreprise. L'état de la protection du réseau inclut les éléments suivants : la présence des applications de sécurité installées sur les appareils du réseau, l'utilisation de clés de licence, le nombre et les types des menaces détectées.

Fichier clé

Le fichier de type xxxxxxx.key qui permet d'utiliser l'application de Kaspersky à l'aide de la licence d'évaluation ou commerciale.

Gestion des identités et des accès (IAM)

Un service d'AWS qui permet d'administrer l'accès des utilisateurs aux autres services et ressources d'AWS.

Gestion directe des applications

Gestion des applications par l'interface locale.

Groupe d'administration

L'ensemble d'appareils regroupés selon les fonctions exécutées et les applications de Kaspersky installées. Les appareils sont regroupés pour en faciliter l'administration dans son ensemble. Un groupe peut inclure d'autres groupes. Des stratégies et des tâches de groupe peuvent être créées pour chaque installation appliquée dans le groupe.

Groupe des applications sous licence

Le groupe des applications créé sur la base des critères définis par l'administrateur (par exemple, selon l'éditeur) pour lesquels le comptage des installations sur les appareils clients a lieu.

Guide de renforcement

Un ensemble de recommandations et de fonctionnalités de configuration de Kaspersky Security Center et de ses modules, dans le but de réduire les risques de compromission.

HTTPS

Le protocole protégé du transfert de données entre le navigateur et le serveur Web avec l'utilisation du chiffrement. HTTPS est utilisé pour accéder aux informations internes telles que les données corporatives et financières.

Image machine Amazon (AMI)

Un modèle contenant la configuration du logiciel indispensable au lancement de la machine virtuelle. Il est possible de créer plusieurs instances au départ d'une seule AMI.

Importance de l'événement

Caractéristique de l'événement consigné dans le fonctionnement de l'application de Kaspersky. Les niveaux de gravité sont les suivants :

- Événement critique
- Erreur de fonctionnement
- Avertissement
- Information

Les événements du même type peuvent avoir différents niveaux de gravité, en fonction du moment où l'événement s'est produit.

Installation à distance

Installation des applications de Kaspersky à l'aide des outils offerts par l'application Kaspersky Security Center.

Installation forcée

Méthode d'installation à distance des applications de Kaspersky qui permet de réaliser l'installation à distance de l'application sur des appareils clients définis. Pour garantir la réussite de l'exécution de la tâche via la méthode de l'installation forcée, le compte utilisateur de lancement de la tâche doit posséder les autorisations de lancement des applications sur les appareils clients. La méthode donnée est recommandée pour l'installation des applications sur les appareils administrés sous les systèmes d'exploitation Microsoft Windows qui permettent cette possibilité.

Installation locale

Installation de l'application de sécurité sur l'appareil du réseau de l'entreprise qui prévoit le lancement manuel d'installation à partir du paquet de distribution de l'application de sécurité ou le lancement manuel du paquet d'installation publié préalablement téléchargé sur l'appareil.

Installation manuelle

Installation de l'application de sécurité sur l'appareil du réseau de l'organisation à partir du paquet de distribution. L'installation manuelle requiert une participation directe de l'administrateur ou d'un autre spécialiste IT. Généralement, l'installation manuelle s'applique si l'installation à distance s'est terminée avec erreur.

Instance Amazon EC2

Une machine virtuelle créée sur la base d'une image AMI à l'aide d'Amazon Web Services.

JavaScript

Le langage de programmation qui élargit les possibilités des pages Web. Les pages Web créées avec JavaScript sont capables d'exécuter les actions complémentaires (par exemple, modifier les types des éléments de l'interface ou ouvrir les fenêtres supplémentaires) sans la mise à jour de la page Web par les données depuis le serveur Web. Pour consulter les pages Web créées à l'aide de JavaScript, il faut activer le support JavaScript dans les paramètres du navigateur.

Kaspersky Private Security Network (KPSN)

Kaspersky Private Security Network est une solution qui permet aux utilisateurs d'appareils qui ont installé des applications Kaspersky d'accéder aux bases de données de réputation de Kaspersky Security Network et à d'autres données statistiques sans envoyer de données de leurs appareils à Kaspersky Security Network. Kaspersky Private Security Network est conçu pour les entreprises qui ne peuvent pas participer à Kaspersky Security Network pour l'une des raisons suivantes :

- Les appareils ne sont pas connectés à Internet.
- La loi ou les stratégies de sécurité de l'entreprise interdisent la transmission de données en hors du pays ou du réseau local de l'entreprise.

Kaspersky Security Center System Health Validator (SHV)

Un module Kaspersky Security Center conçu pour vérifier la puissance du système d'exploitation lors de l'utilisation simultanée de l'application Kaspersky Security Center avec Microsoft NAP.

Kaspersky Security Network (KSN)

Infrastructure des services cloud et offrant l'accès à la base de données de Kaspersky avec des informations constamment mises à jour sur la réputation des fichiers, des ressources Internet et du logiciel. L'utilisation des données de Kaspersky Security Network assure une vitesse de réaction plus élevée des applications de Kaspersky sur les menaces, augmente l'efficacité de fonctionnement de certains modules de protection, ainsi que diminue la possibilité des faux positifs.

Mise à jour

Procédure de remplacement ou d'ajout de nouveaux fichiers (bases de données ou modules de l'application) récupérés sur les serveurs de mise à jour de Kaspersky.

Mise à jour disponible

Un ensemble de mises à jour pour les modules d'applications de Kaspersky, y compris les mises à jour critiques accumulées au fil d'une certaine période et les modifications à l'architecture de l'application.

Mise à niveau de Kaspersky Security Center

La procédure d'installation d'une version plus récente de Kaspersky Security Center sur un appareil sur lequel une version antérieure de cette application est installée.

Nagent léger (LWNGT)

Protocole d'interaction avec Kaspersky Endpoint Security sur les appareils mobiles. Le LWNGT (également appelé protocole mobile) fonctionne comme un Agent d'administration sans installer d'Agent d'administration sur les appareils mobiles.

Niveau d'importance du correctif

Attribut du correctif. Il existe cinq niveaux d'importance pour les correctifs de Microsoft et les correctifs d'éditeurs tiers :

- Critique
- Élevé
- Moyen
- Faible
- Inconnu

Le niveau d'importance du correctif d'un éditeur étranger ou de Microsoft est défini par le niveau de gravité le plus défavorable de la vulnérabilité corrigé par le correctif.

Paquet d'installation

L'ensemble de fichiers pour l'installation à distance de l'application Kaspersky à l'aide du système d'administration à distance Kaspersky Security Center. Le paquet d'installation contient un ensemble de paramètres nécessaires pour installer une application et assurer son efficacité immédiatement après l'installation. Les valeurs des paramètres correspondent aux valeurs des paramètres de l'application par défaut. Le paquet d'installation est créé sur la base de fichiers aux extensions .kpd et .kud inclus dans la distribution de l'application.

Paramètres de l'application

Paramètres des applications, communs à tous les types de tâches et servant au fonctionnement de l'application dans son ensemble, par exemple : paramètres de performances de l'application, paramètres de gestion des rapports, paramètres de la Sauvegarde.

Paramètres de la tâche

Paramètres des applications propres pour chaque type de tâche.

Passerelle des connexions

Une *passerelle de connexion* est un Agent d'administration fonctionnant dans un mode spécial. Une passerelle de connexion accepte les connexions d'autres Agents d'administration et les achemine vers le Serveur d'administration par sa propre connexion avec le serveur. Contrairement à un Agent d'administration ordinaire, une passerelle de connexion attend les connexions du Serveur d'administration au lieu d'établir des connexions avec le Serveur d'administration.

Plug-in d'administration

Module spécial, qui sert d'interface pour l'administration des applications par la Console d'administration. Le plug-in est spécifique à chaque application. Il est repris dans toutes les applications de Kaspersky qui peuvent être administrées à l'aide de Kaspersky Security Center.

Point de distribution

Ordinateur avec un Agent d'administration installé, utilisé pour la diffusion des mises à jour, l'installation à distance des applications, l'obtention d'informations sur les ordinateurs faisant partie du groupe d'administration et/ou d'un domaine multicast. Les points de distribution sont conçus pour réduire la surcharge sur le Serveur d'administration lors de la diffusion des mises à jour et pour optimiser le trafic sur le réseau. Les points de distribution peuvent être assignés automatiquement par le Serveur d'administration ou manuellement par l'administrateur. Le point de distribution s'appelait précédemment agent de mise à jour.

Poste de travail de l'administrateur

Un appareil sur lequel la Console d'administration est installée ou que vous utilisez pour ouvrir Kaspersky Security Center Web Console. Ce module offre une interface d'administration Kaspersky Security Center.

Le poste de travail de l'administrateur sert à configurer et à administrer la partie serveur de Kaspersky Security Center. A l'aide de son poste de travail, l'administrateur met en place et administre un système de protection antivirus centralisé pour un LAN d'entreprise qui repose sur des applications de Kaspersky.

Prestataire de services de protection antivirus

La société présentant les services de protection antivirus des réseaux de l'entreprise cliente sur la base des solutions de Kaspersky.

Privilèges d'administrateur

Le niveau des privilèges et des pouvoirs de l'utilisateur pour administrer les objets Exchange à l'intérieur de l'entreprise Exchange.

Profil de configuration

La stratégie qui contient l'ensemble de paramètres et de restrictions pour l'appareil mobile MDM iOS.

Profil MDM iOS

L'ensemble des paramètres de connexion des appareils mobiles iOS au Serveur d'administration. Le profil MDM iOS est installé par l'utilisateur sur l'appareil mobile, après quoi cet appareil mobile se connecte au Serveur d'administration.

Profil provisioning

L'ensemble des paramètres pour utiliser les applications sur les appareils mobiles iOS. Le profil provisioning contient les informations sur la licence et il est lié à une app concrète.

Propagation de virus

Tentatives multiples d'infection d'un appareil par un virus.

Propriétaire de l'appareil

Le propriétaire de l'appareil est un utilisateur que l'administrateur peut contacter lorsqu'il faut exécuter certaines opérations sur un appareil.

Protection antivirus du réseau

L'ensemble de mesures techniques et d'organisation qui diminuent la possibilité d'intrusion des virus et du spam sur les appareils de réseau de l'entreprise et qui empêchent les attaques de réseau, le phishing et les autres menaces. La protection antivirus du réseau est augmentée lors de l'utilisation des applications de sécurité et des services, et lors de la présence et l'observation de la stratégie de la protection d'information dans l'entreprise.

Reconnaissance de l'emplacement réseau (NLA)

Service Windows qui aide le système d'exploitation à identifier le réseau actuel. La reconnaissance de l'emplacement réseau effectue la détection des modifications apportées au réseau et ajuste la configuration de sécurité de l'appareil.

Restauration

Le déplacement d'un objet original depuis le dossier de quarantaine ou de sauvegarde vers l'emplacement où il était avant sa mise en quarantaine, sa désinfection ou sa suppression ou vers un dossier spécifié par l'utilisateur.

Restauration des données du Serveur d'administration

Il s'agit de la restauration des données du Serveur d'administration à l'aide d'un utilitaire de sauvegarde sur la base des informations présentes dans le dossier de sauvegarde. L'utilitaire permet de restaurer :

- Base de données du Serveur d'administration (stratégies, tâches, paramètres des applications, événements enregistrés sur le Serveur d'administration)
- les informations de configuration de la structure des groupes d'administration et des appareils clients
- le stockage des fichiers d'installation pour l'installation à distance des application (contenu des dossiers : Packages, Uninstall, Updates)
- Certificat du Serveur d'administration

Rôle IAM

Ensemble de droits pour l'exécution des demandes vers les services AWS. Les rôles IAM ne sont liés à aucun utilisateur ou groupe existant et octroient des droits d'accès sans utilisation des clés d'accès AWS IAM. Vous pouvez attribuer un rôle IAM aux utilisateurs IAM, aux instances EC2 et aux applications ou services basés sur AWS.

Sauvegarde des données du Serveur d'administration

Copie des données du Serveur d'administration pour la sauvegarde et la restauration ultérieure, réalisée à l'aide de l'utilitaire de copie de sauvegarde. L'utilitaire permet d'enregistrer :

- Base de données du Serveur d'administration (stratégies, tâches, paramètres des applications, événements enregistrés sur le Serveur d'administration)
- les informations de configuration de la structure des groupes d'administration et des appareils clients
- le stockage des fichiers d'installation pour l'installation à distance des application (contenu des dossiers : Packages, Uninstall, Updates)
- Certificat du Serveur d'administration

Serveur d'administration

Module de l'application Kaspersky Security Center qui remplit la fonction d'enregistrement centralisé des informations sur les applications Kaspersky installées sur le réseau de l'entreprise. et d'un outil efficace d'administration de ces applications.

Serveur d'administration domestique

Le Serveur d'administration domestique est le Serveur d'administration qui a été indiqué lors de l'installation de l'Agent d'administration. Le Serveur d'administration domestique peut être utilisé dans les paramètres des profils de connexion de l'Agent d'administration.

Serveur d'administration virtuel

Le module de l'application Kaspersky Security Center conçu pour l'administration du système de protection du réseau de l'entreprise cliente.

Le Serveur d'administration virtuel est un cas particulier du Serveur d'administration secondaire et, par rapport à un Serveur d'administration physique, est soumis aux restrictions suivantes :

- Le Serveur d'administration virtuel peut fonctionner uniquement s'il fait partie d'un Serveur d'administration principal.
- Le Serveur d'administration virtuel fonctionne à l'aide de la base de données du Serveur d'administration principal. Les tâches de sauvegarde et de restauration des données, ainsi que les tâches de recherche et de téléchargement des mises à jour, ne sont pas prises en charge sur un Serveur d'administration virtuel.
- La création des Serveurs d'administration secondaires (y compris les Serveurs virtuels) n'est pas prise en charge par le Serveur virtuel.

Serveur des appareils mobiles

Le module de Kaspersky Security Center qui offre l'accès aux appareils mobiles et qui permet de les administrer via la Console d'administration.

Serveur MDM iOS

Module Kaspersky Security Center installé sur l'appareil client et qui permet de connecter les appareils mobiles iOS au Serveur d'administration et de les administrer à l'aide du service Apple Push Notifications (APNs).

Serveur Web de Kaspersky Security Center

Un module de Kaspersky Security Center qui s'installe avec le Serveur d'administration. Le Serveur Web est conçu pour transférer via réseau des paquets d'installation autonomes, des profils MDM iOS, ainsi que des fichiers du dossier partagé.

Serveurs de mise à jour de Kaspersky

Serveurs HTTP(S) Kaspersky sur lesquels les applications de Kaspersky récupèrent les mises à jour des bases de données et des modules de l'application.

Services de mise à jour du serveur Windows (WSUS)

L'application utilisée pour diffuser les mises à jour des applications Microsoft sur les ordinateurs des utilisateurs dans le réseau de l'entreprise.

Seuil d'activité de virus

Nombre d'événements d'un type donné et générés dans un intervalle de temps déterminé qui, une fois dépassé, permettra à l'application de considérer qu'il y a augmentation de l'activité virale et développement d'une menace de propagation de virus. Ces données peuvent être utiles en période de propagation de virus et permettent à l'administrateur de réagir opportunément aux menaces d'une attaque de virus.

SSL

Le protocole du chiffrement des données dans les réseaux locaux et dans Internet. SSL est utilisé dans les applications Web afin de créer les connexions sécurisées entre client et serveur.

Stockage d'événements

Partie de la base de données du Serveur d'administration conçue pour le stockage des information sur les événements qui se produisent dans Kaspersky Security Center.

Stratégie

Une stratégie détermine les paramètres d'une application et gère la capacité de configurer cette application sur les ordinateurs d'un groupe d'administration. Pour chaque application, il est nécessaire de créer une stratégie. Vous pouvez créer plusieurs stratégies différentes pour les applications installées sur les ordinateurs dans chaque groupe d'administration, mais il n'est possible d'appliquer qu'une seule stratégie à la fois à chaque application dans un groupe d'administration.

Tâche

Fonctions exécutées par une application de Kaspersky sont effectuées sous la forme de tâches, par exemple : Protection en temps réel des fichiers, Analyse complète de l'ordinateur et mise à jour des bases de données de données.

Tâche de groupe

Tâche définie pour un groupe d'administration et exécutée sur tous les appareils clients de ce groupe.

Tâche locale

La tâche définie et exécutée sur un ordinateur client particulier.

Tâches pour l'ensemble d'appareils

La tâche définie pour un ensemble d'appareils clients parmi des groupes d'administration aléatoires et exécutée sur ces derniers.

Utilisateur de Kaspersky Security Center

Utilisateur qui est responsable de l'état et du fonctionnement du système de protection administré à l'aide de Kaspersky Security Center.

Utilisateur IAM

Utilisateur des services AWS. Un utilisateur IAM peut posséder les privilèges de sondage du segment dans le Cloud.

Utilisateurs internes

Les comptes utilisateur des utilisateurs internes sont utilisés pour travailler avec les Serveurs d'administration virtuels. Dans le cadre de fonctionnalité de l'application Kaspersky Security Center, les utilisateurs internes possèdent les privilèges des utilisateurs réels.

Les comptes des utilisateurs internes sont créés et utilisés uniquement à l'intérieur de Kaspersky Security Center. Les informations sur les utilisateurs internes ne sont pas transmises au système d'exploitation. Kaspersky Security Center effectue l'authentification des utilisateurs internes.

Vulnérabilité

Un défaut au sein d'un système d'exploitation ou d'une application qui pourrait être exploité par un auteur d'application malveillante afin de s'introduire dans le système d'exploitation ou l'application et d'en endommager l'intégrité. Un nombre important de vulnérabilités dans un système d'exploitation fragilise ce dernier car les virus qui s'installent dans le système d'exploitation peuvent provoquer des échecs du système d'exploitation en lui-même et des applications installées.

Zone démilitarisée (DMZ)

La zone démilitarisée est un segment du réseau local où se trouvent les serveurs qui répondent aux requêtes Internet. Afin de garantir la sécurité du réseau local, l'accès à celui-ci depuis la zone démilitarisée est limité et protégé par un pare-feu.

Informations sur le code tiers

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

Avis de marques déposées

Les autres noms et marques déposés appartiennent à leurs propriétaires respectifs.

Adobe, Acrobat, Flash, Shockwave et PostScript sont des marques commerciales ou déposées d'Adobe aux États-Unis et/ou dans d'autres pays.

AMD et AMD64 sont des marques de commerce ou des marques déposées de Advanced Micro Devices, Inc.

Amazon, Amazon Web Services, AWS, Amazon EC2, AWS Marketplace sont des marques commerciales d'Amazon.com, Inc. ou de ses filiales.

Apache est soit une marque déposée, soit une marque d'Apache Software Foundation.

Apple, AirPlay, AirDrop, AirPrint, App Store, Apple Configurator, AppleScript, FaceTime, FileVault, iBook, iBooks, iCloud, iPad, iPhone, iTunes, Leopard, macOS, Mac, Mac OS, OS X, Safari, Snow Leopard, Tiger, QuickTime, et Touch ID sont des marques déposées d'Apple Inc.

Arm est une marque déposée d'Arm Limited (ou de ses filiales) aux États-Unis et/ou ailleurs.

Le nom commercial Bluetooth et le logo appartiennent à Bluetooth SIG, Inc.

Ubuntu, LTS sont des marques déposées de Canonical Ltd.

Cisco Systems, Cisco, Cisco Jabber et IOS sont des marques ou des marques déposées de Cisco Systems, Inc. et/ou de ses filiales enregistrées aux États-Unis et dans certains pays.

Citrix, XenServer sont des marques déposées ou des marques commerciales de Cloud Software Group, Inc. et/ou de ses filiales aux États-Unis et/ou dans d'autres pays.

Corel est une marque ou une marque déposée de Corel Corporation et/ou de ses filiales au Canada, 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.

Dropbox est une marque déposée de Dropbox.

Radmin est une marque déposée de Famatech.

Firebird est une marque déposée de la Fondation Firebird.

Foxit est une marque déposée de Foxit Corporation.

FreeBSD est une marque déposée de The FreeBSD Foundation.

Google, Android, Chrome, Chromium, Dalvik, Firebase, Google Chrome, Google Earth, Google Play, Google Maps, Hangouts, Google Public DNS, et YouTube sont des marques commerciales de Google LLC.

EulerOS, FusionCompute et FusionSphere sont des marques commerciales de Huawei Technologies Co., Ltd.

Intel, Core, Xeon sont des marques commerciales d'Intel Corporation ou de ses filiales.

IBM, QRadar sont des marques de International Business Machines Corporation déposées dans de nombreux pays.

Node.js est une marque déposée de Joyent, Inc.

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

Logitech est une marque déposée ou une marque de Logitech aux États-Unis et/ou dans d'autres pays.

Microsoft, Active Directory, ActiveSync, BitLocker, Excel, Forefront, Internet Explorer, InfoPath, Hyper-V, Microsoft Edge, MultiPoint, MS-DOS, Office 365, PowerShell, PowerPoint, SharePoint, SQL Server, OneNote, Outlook, Skype, Tahoma, Visio, Win32, Windows, Windows PowerShell, Windows Media, Windows Mobile, Windows Server, Windows Phone, Windows Vista et Windows Azure sont des marques déposées du groupe de sociétés Microsoft.

CVE est une marque commerciale déposée de The MITRE Corporation.

Mozilla, Thunderbird, Firefox sont des marques déposées de la Fondation Mozilla aux États-Unis et dans d'autres pays.

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

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

OpenVPN est une marque commerciale d'OpenVPN, Inc.

OpenSSL est une marque commerciale appartenant à OpenSSL Software Foundation.

Oracle, Java, JavaScript, et TouchDown sont des marques commerciales déposées d'Oracle et/ou de ses filiales.

Parallels, le logo Parallels et Coherence sont des marques ou des marques déposées de Parallels International GmbH.

Chef est une marque ou une marque déposée de Progress Software Corporation et/ou de l'une de ses filiales ou sociétés affiliées aux États-Unis et/ou dans d'autres pays.

Puppet est une marque commerciale ou une marque déposée de Puppet, Inc.

Python est une marque ou une marque déposée de Python Software Foundation.

Red Hat, Fedora et Red Hat Enterprise Linux sont des marques ou des marques déposées de Red Hat, Inc. ou de ses filiales aux États-Unis et dans d'autres pays.

Ansible est une marque commerciale de Red Hat, Inc. déposée aux États-Unis et dans d'autres pays.

CentOS est une marque ou une marque déposée de Red Hat, Inc. ou de ses filiales aux États-Unis et dans d'autres pays.

BlackBerry appartient à Research In Motion Limited, déposée aux États-Unis et peut être en cours de dépôt déposée dans d'autres pays.

Rocky Linux est une marque déposée de The Rocky Enterprise Software Foundation.

SAMSUNG est une marque de SAMSUNG aux États-Unis ou dans d'autres pays.

Debian une marque déposée de Software in the Public Interest, Inc.

Splunk, SPL sont des marques commerciales et des marques commerciales déposées de Splunk Inc. aux États-Unis et dans d'autres pays.

SUSE est une marque déposée de SUSE LLC aux États-Unis et dans d'autres pays.

La marque de commerce Symbian appartient à la Symbian Foundation Ltd.

OpenAPI est la marque de commerce de The Linux Foundation.

UNIX est une marque commerciale déposée aux États-Unis et dans d'autres pays, sous licence exclusive via X/Open Company Limited.

Zabbix est une marque déposée de Zabbix SIA.

Problèmes connus

Kaspersky Security Center Web Console présente une série de restrictions qui n'ont pas une incidence critique sur le fonctionnement de l'application :

- La console affiche la sous-section **Alerte** dans la section **Surveillance et rapports** du menu principal uniquement si vous avez ajouté une clé de licence pour EDR Optimum au répertoire du Serveur d'administration en saisissant le code d'activation.

- Pour garantir la force du chiffrement, le certificat du Serveur d'administration doit être signé à l'aide du hachage SHA-2 et avoir une longueur de clé minimale de 2048. Si vous devez réémettre le certificat, consultez la Base de connaissances de Kaspersky Security Center.

- Si vous créez une tâche avec les **paramètres de planification Tous les N jours** et Selon les jours de la semaine dans Kaspersky Security Center 15.1 Web Console, et que vous ouvrez ensuite la tâche dans des versions antérieures de Kaspersky Security Center Web Console ou dans la Console d'administration de Kaspersky Security Center (par exemple, lorsque la tâche est également appliquée sur les Serveurs d'administration secondaires qui peuvent être basés à la fois sur Linux et sur Windows), les paramètres de planification peuvent être affichés de manière incorrecte ou une erreur peut se produire.

- Lorsque vous configurez l'exportation vers les systèmes SIEM dans Kaspersky Security Center Web Console et sélectionnez le protocole UDP, une erreur est renvoyée après avoir cliqué sur le bouton **Vérifier la connexion**, car le protocole UDP n'établit pas de connexion, et la livraison des données ne peut pas être garantie.

- Lorsque vous exécutez la tâche pour supprimer l'Agent d'administration d'un appareil basé sur l'architecture Arm et exécutant Astra Linux Special Edition RUSB.10015-01 (mise à jour opérationnelle 1.7), l'Agent d'administration est supprimé, mais l'état de la tâche pour la progression actuelle de la tâche la liste est figée.

- La fenêtre des propriétés de la stratégie Kaspersky Device Management for iOS contient toujours la section **Paramètres des appareils EAS**, même si Exchange ActiveSync n'est plus pris en charge.

- La connexion à KSN via HTTPS échoue si Kaspersky Security Center est installé sur un appareil dont le nom de l'appareil comporte des caractères cyrilliques et si le proxy KSN est activé sur le Serveur d'administration.

- Lorsque vous essayez de modifier les propriétés d'un compte d'utilisateur pour lequel l'option **Demander une authentification pour vérifier l'autorisation de modifier les comptes utilisateurs** est activée, puis cliquez sur **Annuler** dans la fenêtre **Protection du compte**, une erreur inattendue se produit.

- Si vous modifiez l'heure ou le fuseau horaire de votre appareil, vous devez redémarrer le service de Kaspersky Security Center Web Console.

- Si un proxy est utilisé sur l'appareil et que les variables d'environnement du proxy sont définies, le programme d'installation de Kaspersky Security Center Web Console peut se bloquer.

- Lorsque vous importez la tâche *Télécharger les mises à jour sur les stockages des points de distribution* ou la tâche *Vérification des mises à jour*, l'option **Sélectionner les appareils auxquels la tâche sera affectée** est activée. Ces tâches ne peuvent pas être affectées à une sélection d'appareils ou à des appareils en particulier. Si vous attribuez la tâche *Télécharger les mises à jour sur les stockages des points de distribution* ou la tâche *Vérification des mises à jour* aux appareils spécifiques, la tâche sera importée de manière incorrecte.

- Si vous effectuez une sondage Active Directory à l'aide d'un point de distribution Linux sur lequel l'Agent d'administration version 15 est installé, vous pouvez sonder uniquement les domaines Active Directory pour lesquels vous spécifiez l'adresse et les informations d'identification de l'utilisateur. Les sondages du domaine Active Directory actuel et de la forêt de domaines Active Directory ne sont pas disponibles.

- Les appareils clients peuvent être introuvables après l'exécution du sondage du réseau Windows.
- Dans l'**Assistant d'ajout de Serveur d'administration secondaire**, si vous indiquez un compte pour lequel la vérification en deux étapes est activée pour l'authentification sur le futur Serveur secondaire, l'Assistant se termine par une erreur. Pour résoudre ce problème, indiquez un compte pour lequel la vérification en deux étapes est désactivée ou créez la hiérarchie à partir du futur Serveur secondaire.
- Lors de la connexion à Kaspersky Security Center Web Console, si vous utilisez l'authentification de domaine et spécifiez un Serveur d'administration virtuel auquel vous connecter, puis vous vous déconnectez, puis essayez de vous connecter au Serveur d'administration principal, Kaspersky Security Center Web Console se connecte au Serveur d'administration virtuel. Pour vous connecter au Serveur d'administration principal, rouvrez le navigateur.
- Le sondage rapide/complet du réseau Windows renvoie un résultat vide.
- Si vous installez Kaspersky Security Center Web Console avec le Gestionnaire des identités et des accès et changez ensuite le Serveur d'administration pour Kaspersky Security Center Web Console, le Gestionnaire des identités et des accès n'obtient pas les informations sur le nouveau Serveur d'administration.
- Un appareil administré doté de plusieurs cartes réseau envoie au Serveur d'administration des informations sur l'adresse MAC de la carte réseau qui n'est pas celle utilisée pour se connecter au Serveur d'administration.
- Le test de connexion au SIEM échoue lorsque le format de données CEF est sélectionné.
- L'authentification NTLM ne fonctionne pas pour les comptes d'utilisateurs au sein du groupe Utilisateurs protégés.