kaspersky

Kaspersky Security Center 15 Linux

© 2025 AO Kaspersky Lab

Contenu

Aide de Kaspersky Security Center Linux

Nouveautés

À propos de Kaspersky Security Center Linux

- Configurations logicielle et matérielle
  - Configuration requise pour le Serveur d'administration
  - Configuration requise pour Web Console
  - Configuration requise pour l'Agent d'administration
- Kit de distribution
- À propos de la compatibilité du Serveur d'administration et de Kaspersky Security Center Web Console
- Comparaison de Kaspersky Security Center : basé sur Windows et basé sur Linux
- À propos de Kaspersky Security Center Cloud Console

Architecture et concepts de base

- Architecture
- Diagramme de déploiement du Serveur d'administration de Kaspersky Security Center Linux et de Kaspersky Security Center Web Console
- Ports utilisés par Kaspersky Security Center Linux
- Ports utilisés par Kaspersky Security Center Web Console
- Notions principales
  - Serveur d'administration
  - Hiérarchie des Serveurs d'administration
  - Serveur d'administration virtuel
  - Serveur Web
  - Agent d'administration
  - Groupes d'administration
  - Appareil administré
  - Appareil non défini
  - Poste de travail de l'administrateur
  - 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

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 Linux et des applications de sécurité : plus d'informations
  - Conventions utilisées dans les schémas d'interaction
  - Serveur d'administration et SGBD
  - 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
Guide de démarrage
Installation
Configuration du serveur MariaDB x64 pour fonctionner avec Kaspersky Security Center Linux
Configuration du serveur PostgreSQL ou Postgres Pro pour fonctionner avec Kaspersky Security Center Linux
Installation de Kaspersky Security Center Linux
Installation de Kaspersky Security Center Linux en mode silencieux
Installation de Kaspersky Security Center Linux sur Astra Linux dans un environnement logiciel fermé
Installation de Kaspersky Security Center Web Console
Paramètres d'installation de Kaspersky Security Center Web Console
Installation de Kaspersky Security Center Web Console sur Astra Linux à l'aide de l'environnement logiciel fermé
Installation de Kaspersky Security Center Web Console connecté au Serveur d'administration installé sur les nœuds du cluster de basculement Kaspersky Security Center Linux
Déploiement du cluster de basculement Kaspersky Security Center Linux
Scénario : Déploiement du cluster de basculement Kaspersky Security Center Linux
À propos du cluster de basculement Kaspersky Security Center Linux
Préparation d'un serveur de fichiers pour un cluster de basculement Kaspersky Security Center Linux
Préparation des nœuds pour un cluster de basculement Kaspersky Security Center Linux
Installation de Kaspersky Security Center Linux sur les nœuds du cluster de basculement Kaspersky Security Center Linux
Démarrage et arrêt manuels des nœuds de cluster
Comptes pour travailler avec le SGBD
Configuration du compte SGBD pour travailler avec MySQL et MariaDB
Configuration des comptes SGBD pour l'utilisation avec PostgreSQL et Postgres Pro
Certificats pour l'utilisation de Kaspersky Security Center Linux
À propos des certificats de Kaspersky Security Center
Conditions requises pour les certificats personnalisés utilisés dans Kaspersky Security Center Linux
Réémission du certificat pour Kaspersky Security Center Web Console
Remplacement de certificat pour Kaspersky Security Center Web Console
Conversion d'un certificat PFX au format PEM
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
Désignation du dossier partagé
Connexion et déconnexion de Kaspersky Security Center Web Console
Modification de la langue de l'interface de Kaspersky Security Center Web Console
Configuration du serveur MySQL x64 pour fonctionner avec Kaspersky Security Center Linux
Assistant de démarrage rapide de l'application
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. Téléchargement des paquets de distribution et création des paquets d'installation
Étape 7. Configuration de Kaspersky Security Network

Étape 8. Sélection de la méthode d'activation de l'application
Étape 9. Création de la configuration de base de la protection d'un réseau
Étape 10. Configuration des notifications par email
Étape 11. Fin de l'Assistant de configuration initiale de l'application
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. Suppression des applications incompatibles avant l'installation
Étape 8. Déplacement des appareils vers Appareils administrés
Étape 9. Sélection des comptes pour accéder aux appareils
Étape 10. Démarrage de l'installation
Mise à jour de Kaspersky Security Center Linux
Mise à niveau de Kaspersky Security Center Linux à l'aide du fichier d'installation
Mise à niveau de Kaspersky Security Center Linux via la sauvegarde
Mise à jour de Kaspersky Security Center sur les nœuds du cluster de basculement Kaspersky Security Center Linux
Mise à niveau de Kaspersky Security Center Web Console
Mise à jour de Kaspersky Security Center Web Console sur Astra Linux en mode environnement logiciel fermé
Migration vers Kaspersky Security Center Linux
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
Configuration du Serveur d'administration
Configuration de la connexion de Kaspersky Security Center Web Console au serveur d'administration
Configuration d'une liste d'autorisation d'adresses IP pour se connecter à Kaspersky Security Center Linux
Configuration des paramètres d'accès Internet du Serveur d'administration
Hiérarchie des Serveurs d'administration
Création d'une hiérarchie des Serveurs d'administration : ajout d'un Serveur d'administration secondaire
Affichage de la liste des Serveurs d'administration secondaires
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
Configuration du journal des événements de connexion au Serveur d'administration
Définition du nombre d'événements maximal dans le stockage d'événements
Déplacement du Serveur d'administration sur un autre appareil
Modification des informations d'identification du SGBD
Copie de sauvegarde et restauration des données du Serveur d'administration
Création d'une tâche de copie de sauvegarde des données du Serveur d'administration
Sauvegarde et restauration des données à l'aide de l'utilitaire klbackup
Maintenance du Serveur d'administration
Suppression d'une hiérarchie des Serveurs d'administration
Accès aux serveurs DNS publics

- Configuration de l'interface
- Chiffrer la communication selon TLS
- Liste globale des sous-réseaux

Recherche d'appareils en réseau
- Scénario de recherche d'appareils en réseau
- 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
- 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
  - Déplacement dans le groupe d'administration des appareils qui font partie de VDI

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
  - Scénario : Authentification du serveur MySQL
  - Scénario : Authentification du serveur PostgreSQL
- Préparatifs du déploiement
  - Planification du déploiement de Kaspersky Security Center Linux
    - Schémas typiques de déploiement du système de protection
    - À propos de la planification du déploiement de Kaspersky Security Center Linux dans le réseau de l'entreprise
    - Sélection de la structure de protection de la société
    - Configurations typiques de Kaspersky Security Center Linux
      - Configuration typique : un bureau
      - Configuration typique : quelques bureaux importants répartis géographiquement avec leurs propres administrateurs
      - Configuration typique : plusieurs petits bureaux isolés
    - Choix d'un SGBD
    - 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
    - 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
    - Serveurs d'administration virtuels
  - 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

À propos des tâches d'installation à distance des applications de Kaspersky Security Center Linux
Déploiement par prise d'image et copie d'image d'un appareil
Mode de clonage du disque de l'Agent d'administration
Déploiement forcé à l'aide d'une tâche d'installation à distance des applications de Kaspersky Security Center Linux
Lancement de paquets autonomes créés par Kaspersky Security Center Linux
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
Surveillance du déploiement
Configuration des paramètres des programmes d'installation
Informations générales
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 de l'Agent d'administration pour Linux en mode interactif
Installation de l'Agent d'administration pour Windows en mode interactif
Installation de l'Agent d'administration pour Windows en mode silencieux
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
Configuration manuelle d'une tâche de groupe d'analyse de l'appareil de Kaspersky Endpoint Security
Administration des appareils clients
Paramètres de l'appareil administré
Règles de déplacement des appareils
Création des règles de déplacement des appareils
Copie des règles de déplacement des appareils
Conditions d'une règle de déplacement de l'appareil
Ajout manuel d'appareils à un groupe d'administration
Déplacement manuel des appareils ou des clusters à un groupe d'administration
À propos des clusters et des groupes des serveurs
Propriétés d'un cluster ou d'un groupe de serveurs
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
Calcul de la quantité et de la configuration 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
Activation d'un serveur push
À propos des états des appareils
Configuration de la permutation des états des appareils
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
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
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
Consultation et configuration des actions quand les appareils sont inactifs
Envoi d'un message aux utilisateurs des appareils
Démarrage, arrêt et redémarrage à distance des appareils clients
Administration des groupes d'administration
Création des groupes d'administration
Installation automatique des applications sur les appareils du groupe d'administration
Déplacement des groupes d'administration
Suppression des groupes d'administration
Déploiement des applications Kaspersky
Scénario : déploiement des applications Kaspersky
Obtention des plug-ins d'administration pour les applications de Kaspersky
Téléchargement et création des paquets d'installation pour les applications de Kaspersky
Création de paquets d'installation à partir d'un fichier
Création de paquets d'installation autonomes
Modification de la limite de la taille des données du paquet d'installation personnalisé
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
Affichage de la liste des paquets d'installation autonomes
Propagation des paquets d'installation sur les Serveurs d'administration secondaires
Préparation d'un appareil Linux et installation de l'Agent d'administration sur un appareil Linux à distance
Installation des applications à l'aide de la tâche d'installation à distance
Installation d'une application à distance

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.
Remplacement d'application de sécurité d'éditeurs tiers
Suppression d'applications ou de mises à jour logicielles à distance
Préparation d'un appareil exécutant SUSE Linux Enterprise Server 15 pour l'installation de l'Agent d'administration
Préparation de l'appareil Windows pour l'installation à distance
Préparation de l'appareil fonctionnant sous le système d'exploitation macOS à l'installation à distance de l'Agent d'administration
Licences
License de Kaspersky Security Center Linux
À propos du contrat de licence utilisateur final
À propos de la licence
À propos du certificat de licence
À propos de la clé de licence
Consultation de la politique de confidentialité
Options de licence de Kaspersky Security Center
À propos du fichier clé
À propos de la collecte des données
À propos de l'abonnement
Activation de Kaspersky Security Center Linux
Licence des applications Kaspersky administrées
Licence des applications administrées
Ajout de la clé de licence dans le stockage 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
Événements de dépassement de la restriction de licence
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 des applications Kaspersky
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
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
Paramètres généraux de la stratégie

Modification d'une 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
Synchronisation forcée
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
Copie d'un profil de stratégie
Création d'une règle d'activation du profil de stratégie
Suppression d'un profil de stratégie
Paramètres de la stratégie de l'Agent d'administration
Utilisation de l'Agent d'administration pour Windows, Linux et macOS : comparaison
Comparaison des paramètres de l'Agent d'administration par système d'exploitation
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
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
Gérer les 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
Affichage de l'historique des tâches entreposé sur le Serveur d'administration

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
Autorisation de l'accès hors ligne à l'appareil externe bloqué par le Contrôle des appareils
Utilisation de l'utilitaire klsclag pour ouvrir le port 13291
Enregistrement de l'application Kaspersky Industrial CyberSecurity for Networks dans Kaspersky Security Center Web Console
Administration des utilisateurs et des rôles d'utilisateur
À propos des comptes utilisateurs
À propos des rôles d'utilisateurs
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
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
Activation de la protection du compte contre les modifications non autorisées
Vérification en deux étapes
Scénario : configuration de la vérification en deux étapes pour tous les utilisateurs
À propos de la vérification en deux étapes pour un compte
Activation de la vérification en deux étapes pour votre compte
Activation de la vérification en deux étapes obligatoire pour tous les utilisateurs
Désactivation de la vérification en deux étapes d'un compte utilisateur
Désactivation de la vérification en deux étapes obligatoire pour tous les utilisateurs
Exclusion de comptes de la vérification en deux étapes
Configuration de la vérification en deux étapes pour votre compte
Interdire aux nouveaux utilisateurs de configurer eux-mêmes la vérification en deux étapes
Création d'une nouvelle clé secrète
Modification du nom d'un émetteur de code de sécurité
Modification du nombre de tentatives de saisie du mot de passe autorisées
Suppression d'un utilisateur ou d'un groupe de sécurité
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
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 dans les stockages des points de distribution
Ajout des sources de mises à jour pour la tâche Télécharger les mises à jour dans le référentiel du Serveur d'administration
Installation automatique des mises à jour pour Kaspersky Endpoint Security for Windows
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
Téléchargement des mises à jour par les points de distribution
Mise à jour des bases de données et des modules logiciels de Kaspersky sur des appareils déconnectés
Sauvegarde et restauration des plug-ins Web
Surveillance, reporting et audit
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 Linux
Événements des modules de Kaspersky Security Center Linux
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 d'avertissement de l'Agent d'administration
Événements informatifs de l'Agent d'administration
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
Blocage des événements fréquents
À propos du blocage des événements fréquents
Gestion du blocage des événements fréquents
Suppression du blocage des événements fréquents
Traitement et stockage des événements sur le Serveur d'administration
Notifications et états de l'appareil
Utilisation des notifications
Affichage des notifications à l'écran
À propos des états des appareils
Configuration des paramètres d'envoi des notifications
Vérification de déploiement 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
Exportation des événements dans les systèmes SIEM
Configuration de l'export d'événements vers des systèmes SIEM
Conditions préalables
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
Configuration de Kaspersky Security Center Linux 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 Linux
Consultation des résultats de l'exportation
Utilisation des révisions des objets
Restauration d'un objet à une révision précédente
Suppression d'objets
Téléchargement et suppression de fichiers de la Quarantaine et de la Sauvegarde
Téléchargement de fichiers à partir de la Quarantaine et de la Sauvegarde
À propos de la suppression d'objets des référentiels Quarantaine, Sauvegarde ou Menaces actives
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 informations système à partir d'un appareil client
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 Linux 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
Administration des applications et des fichiers exécutables tiers sur les appareils clients
Utilisation du Contrôle des applications pour gérer les fichiers exécutables
Modes et catégories du Contrôle des applications
Obtention et consultation d'une liste des applications installées sur les appareils client
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
Configuration du Contrôle des applications dans la stratégie Kaspersky Endpoint Security for Windows
Ajout de fichiers exécutables liés par un événement à la catégorie d'applications
Guide de référence de l'API
Meilleures pratiques pour les prestataires de services
Planification du déploiement de Kaspersky Security Center Linux
Octroi de l'accès au Serveur d'administration via Internet
Configuration typique de Kaspersky Security Center Linux
À propos des points de distribution
Hiérarchie des Serveurs d'administration
Serveurs d'administration virtuels
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
Déploiement de l'Agent d'administration et des applications de sécurité
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
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
À propos des profils de connexion pour les utilisateurs itinérants
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
Guide de dimensionnement
Présentation du manuel
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 disque
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
Bonnes pratiques pour un Serveur d'administration qui gère un grand nombre d'appareils
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 de la base de données
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
Problèmes connus
Glossaire
Administrateur de Kaspersky Security Center Linux
Administrateur du client
Administrateur du prestataire de services
Administration centralisée des applications

Agent d'administration
Agent d'authentification
Appareils administrés
Application incompatible
Base antivirus
Boutique des apps
Certificat du Serveur d'administration
Certificat général
Clé active
Clé de licence complémentaire (ou de réserve)
Client du Serveur d'administration (Appareil client)
Console d'administration
Domaine multicast
Dossier de sauvegarde
Durée de validité de la licence
État de la protection
État de la protection du réseau
Fichier clé
Gestion directe des applications
Groupe d'administration
Groupe de rôle
HTTPS
Importance de l'événement
Installation à distance
Installation locale
Installation manuelle
JavaScript
Kaspersky Private Security Network (KPSN)
Kaspersky Security Center System Health Validator (SHV)
Lightweight Nagent (LWNGT)
Mise à jour
Mise à jour disponible
Paquet d'installation
Paramètres de l'application
Paramètres de la tâche
Passerelle des connexions
Point de distribution
Poste de travail de l'administrateur
Prestataire de services de protection antivirus
Privilèges d'administrateur
Profil
Profil de configuration
Profil provisioning
Propriétaire de l'appareil
Protection antivirus du réseau
Restauration
Restauration des données du Serveur d'administration
Sans utiliser la reconnaissance de l'emplacement réseau (NLA).

Sauvegarde des données du Serveur d'administration
Serveur d'administration
Serveur d'administration domestique
Serveur d'administration virtuel
Serveur Web de Kaspersky Security Center Linux
Serveurs de mise à jour de Kaspersky
SSL
Stockage d'événements
Stratégie
Tâche
Tâche de groupe
Tâche locale
Tâches pour l'ensemble d'appareils
Utilisateur de Kaspersky Security Center
Utilisateurs internes
Zone démilitarisée (DMZ)
Informations sur le code tiers
Avis de marques déposées

Aide de Kaspersky Security Center Linux

Nouvelles fonctionnalités

- Nouveautés

Configurations logicielle et matérielle

- Configuration requise pour le Serveur d'administration
- Configuration requise pour Web Console
- Configuration requise pour l'Agent d'administration

Guide de démarrage

- Installation
- Assistant de configuration initiale de l'application
- Assistant de déploiement de la protection

Licence et activation

- Activation de Kaspersky Security Center Linux
- Licence des applications administrées

Déploiement et configuration

- Recherche d'appareils en réseau
- Réglage des points de distribution et/ou des passerelles de connexion
- Remplacement d'application de sécurité d'éditeurs tiers
- Applications Kaspersky. Déploiement centralisé
- Configuration de la protection réseau

- Applications Kaspersky. Mise à jour des bases de données et des modules d'application

Surveillance

- Suivi et rapports

Fonctionnalités supplémentaires

- Exportation des événements dans les systèmes SIEM
- Guide de dimensionnement (Aide en ligne uniquement)

Nouveautés

Kaspersky Security Center 15 Linux

Kaspersky Security Center 15 Linux comprend plusieurs nouvelles fonctionnalités et améliorations :

- Le sondage du contrôleur de domaine vous permet d'interroger un contrôleur de domaine Microsoft Active Directory et un contrôleur de domaine Samba. Vous pouvez utiliser le Serveur d'administration ou un point de distribution pour interroger Microsoft Active Directory. Vous pouvez interroger un contrôleur de domaine Samba uniquement via un point de distribution basé sur Linux. 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.

- Kaspersky Security Center Linux prend désormais en charge les SGBD suivants :

  - PostgreSQL 15.x

  - Postgres Pro 15.x

- Si vous utilisez PostgreSQL ou Postgres Pro comme SGBD, Kaspersky Security Center Linux prend en charge jusqu'à 50 000 appareils administrés.

- Migration de Kaspersky Security Center Windows vers Kaspersky Security Center Linux. Vous pouvez exécuter un Assistant pour migrer les objets de Kaspersky Security Center, notamment les tâches, les stratégies et la structure des groupes d'administration. Après cela, vous pouvez déplacer les appareils administrés importés vers Kaspersky Security Center Linux.

- Kaspersky Security Center Linux prend désormais en charge les applications Kaspersky suivantes :

  - Kaspersky Security for Virtualization Light Agent

  - Kaspersky Embedded Systems Security for Windows

  - Kaspersky Embedded Systems Security for Linux

  - Kaspersky Industrial CyberSecurity for Nodes

  - Kaspersky Industrial CyberSecurity for Networks

  - Kaspersky Endpoint Security for Mac

  - Kaspersky Endpoint Agent

  - Kaspersky Security for Virtualization Light Agent

- Diagnostics à distance des appareils administrés basés sur Windows et Linux.

- Module de contrôle des applications amélioré. Vous pouvez désormais créer une catégorie d'applications basée sur la liste des fichiers exécutables d'un dossier sélectionné ou basée sur une catégorie d'applications Kaspersky. Vous pouvez ensuite spécifier si vous souhaitez autoriser ou bloquer les applications de la catégorie créée dans votre organisation.

- Exporter et importer les sélections d'événements. Vous pouvez exporter une sélection d'événements définie par l'utilisateur et ses paramètres vers un fichier KLO, puis importer la sélection d'événements enregistrée dans

Kaspersky Security Center Windows ou Kaspersky Security Center Linux.

- Dans le Rapport sur les menaces, vous pouvez désormais ouvrir une chaîne de développement des menaces en cliquant sur le lien **Afficher l'alerte**.

- Kaspersky Security Center Linux prend désormais en charge la technologie de 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.

- Certaines plateformes ne sont plus prises en charge par Kaspersky Security Center Linux, car ces plateformes ne sont plus prises en charge par leurs fournisseurs.

Kaspersky Security Center 14.2 Linux

Kaspersky Security Center 14.2 Linux comprend plusieurs nouvelles fonctionnalités et améliorations :

- Dans une hiérarchie de Serveurs d'administration, un Serveur d'administration basé sur Linux peut désormais agir en tant que Serveur primaire et peut administrer des Serveurs Linux ou Windows en tant que Serveur secondaire.

- Kaspersky Security Center Linux prend désormais en charge Kaspersky Security Network (KSN), le service KSN Proxy et Kaspersky Private Security NetworK (KPSN).

- Kaspersky Security Center Linux prend désormais en charge Kaspersky Endpoint Security for Windows en tant qu'application administrée.

  L'installation à distance de l'Agent d'administration pour Windows sur les appareils clients est possible uniquement à l'aide des outils du système d'exploitation via les points de distribution Windows.

- Les données sur les appareils administrés Windows peuvent désormais être chiffrées afin de réduire le risque de fuite involontaire de données sensibles et d'entreprise en cas de vol ou de perte d'un ordinateur portable ou d'un disque dur. Cette fonctionnalité est implémentée via Kaspersky Endpoint Security for Windows.

- Kaspersky Security Center Linux vous permet de télécharger et de mettre à jour les paquets de distribution des applications Kaspersky et les plug-ins Web d'administration directement dans l'interface utilisateur de Kaspersky Security Center Linux.

- Par défaut, les informations sur les applications installées sur les appareils administrés basés sur Linux et Windows sont envoyées au Serveur d'administration.

- 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 données sensibles transmises entre le Serveur d'administration principal, les Serveurs d'administration secondaires et les Agents d'administration sont désormais protégées par l'algorithme de chiffrement AES.

- 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 Linux 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)

- 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*

Kaspersky Security Center 14 Linux

Kaspersky Security Center Linux comprend plusieurs nouvelles fonctionnalités et améliorations :

- Outre la tâche *Téléchargement des mises à jour sur le stockage du Serveur d'administration*, il est désormais possible de télécharger les bases antivirus des applications de sécurité de Kaspersky via la tâche *Téléchargement des mises à jour sur les stockages des points de distribution*.
- Les bases de données antivirus et les modules d'application sur les appareils administrés peuvent être propagés et mis à jour via le Serveur d'administration ou les points de distribution. Vous pouvez choisir un schéma de mise à jour optimal pour votre organisation, afin de réduire la charge du Serveur d'administration et d'optimiser le trafic de données sur le réseau de l'entreprise.
- Kaspersky Security Center Linux ne télécharge depuis les serveurs de mise à jour de Kaspersky que les mises à jour demandées par les applications de sécurité de Kaspersky. Cela réduit la taille des données téléchargées.
- Vous pouvez désormais utiliser la fonction de fichiers diff pour télécharger des bases de données antivirus et des modules logiciels. 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.
- La tâche *Vérification de la mise à jour* a été ajoutée. En utilisant cette tâche, vous pouvez vérifier automatiquement le fonctionnement et les erreurs des mises à jour téléchargées avant d'installer les mises à jour sur les appareils administrés.
- Kaspersky Security Center Linux prend désormais en charge Kaspersky Industrial CyberSecurity for Linux Nodes 1.3 en tant qu'application administrée.

À propos de Kaspersky Security Center Linux

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

Kaspersky Security Center Linux (également appelé Kaspersky Security Center) est conçu pour déployer et administrer la protection des appareils clients à l'aide d'un Serveur d'administration basé sur Linux.

Kaspersky Security Center Linux vous permet d'installer des applications de protection Kaspersky sur les appareils d'un réseau d'entreprise, d'exécuter à distance des tâches d'analyse et de mise à jour et d'administrer les stratégies de sécurité des applications administrées. En tant qu'administrateur, vous pouvez utiliser un tableau de bord détaillé qui fournit un instantané des états des appareils de l'entreprise, des rapports détaillés et des paramètres précis dans les stratégies de protection.

Par rapport à Kaspersky Security Center doté du Serveur d'administration Windows®, Kaspersky Security Center Linux possède un ensemble de fonctionnalités différent.

L'application Kaspersky Security Center Linux 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.

- Effectuer l'installation à distance des applications par Kaspersky et d'autres éditeurs de logiciels.

- 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.

- Gérez le chiffrement des informations stockées sur les disques durs des appareils Windows et sur les disques amovibles.

- Gérez l'accès des utilisateurs aux données chiffrées sur les appareils Windows.

- 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 Linux via Kaspersky (par exemple, à l'adresse https://www.kaspersky.fr) ou par l'intermédiaire d'entreprises partenaires.

Si vous achetez Kaspersky Security Center Linux 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.

Configurations logicielle et matérielle

- Configuration requise pour le Serveur d'administration
- Configuration requise pour Web Console
- Configuration requise pour l'Agent d'administration

Configuration requise pour le Serveur d'administration

Configuration matérielle minimale requise :

- Processeur cadencé à 1,4 GHz ou plus.
- Mémoire vive : 4 Go.
- Espace disponible sur le disque : 10 Go requis pour le dossier dans lequel les données du Serveur d'administration sont stockées (/var/opt/kaspersky/klnagent_srv).

Les systèmes d'exploitation suivants sont pris en charge :

- Debian GNU/Linux 10.x (Buster) 64 bits
- Debian GNU/Linux 11.x (Bullseye) 64 bits
- Debian GNU/Linux 12 (Bookworm) 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
- CentOS 7.x 64 bits
- CentOS Stream 9 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
- Astra Linux Special Edition RUSB.10015-01 (mise à jour opérationnelle 1.6) 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 Common Edition (mise à jour opérationnelle 2.12) 64 bits
- ALT SP Server 10 64 bits
- ALT Server 10 64 bits
- ALT Server 9.2 64 bits
- ALT 8 SP Server (LKNV.11100-01) 64 bits
- ALT 8 SP Server (LKNV.11100-02) 64 bits
- ALT 8 SP Server (LKNV.11100-03) 64 bits
- Oracle Linux 7 64 bits
- Oracle Linux 8 64 bits
- Oracle Linux 9 64 bits
- RED OS 7.3 Server 64 bits
- RED OS 7.3 Édition certifiée 64 bits
- ROSA COBALT 7.9 64 bits

Nous vous recommandons d'utiliser le système de fichiers EXT4 avec ses paramètres par défaut.

Plateformes de virtualisation prises en charge :

- VMware vSphere 6.7
- VMware vSphere 7.0
- VMware vSphere 8.0
- VMware Workstation 16 Pro
- VMware Workstation 17 Pro
- Microsoft Hyper-V Server 2012 64 bits
- Microsoft Hyper-V Server 2012 R2 64 bits

- Microsoft Hyper-V Server 2016 64 bits
- 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 17
- Oracle VM VirtualBox 6.x
- Oracle VM VirtualBox 7.x
- Machine virtuelle basée sur le noyau (tous les systèmes d'exploitation Linux pris en charge par le serveur d'administration)

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

- MySQL 5.7 Community 32 bits / 64 bits
- MySQL 8.0 32 bits / 64 bits
- MariaDB 10.1 (version 10.1.30 et versions ultérieures) 32 bits / 64 bits
- MariaDB 10.3 (version 10.3.22 et supérieures) 32 bits / 64 bits
- MariaDB 10.4 (version 10.4.20 et versions ultérieures) 32 bits / 64 bits
- MariaDB 10.5 (version 10.5.27 et versions ultérieures) 32 bits / 64 bits
- MariaDB 10.6 (version 10.6.20 et versions ultérieures) 32 bits / 64 bits
- MariaDB 10.11 (version 10.11.10 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 64 bits (toutes les éditions)
- Postgres Pro 14.x 64 bits (toutes les éditions)
- Postgres Pro 15.x 64 bits (toutes les éditions)
- Platform V Pangolin 5.4.0 64 bits
- Jatoba 4 64 bits

Configuration requise pour Web Console

Serveur de Kaspersky Security Center Web Console

Configuration matérielle minimale requise :

- Processeur : quadri-cœur, cadencé à 2,5 GHz.
- Mémoire vive : 8 Go.
- Espace disponible sur le disque : 40 Go requis pour le dossier dans lequel les données du Serveur d'administration sont stockées (/var/opt/kaspersky).

L'un des systèmes d'exploitation suivants (versions 64 bits uniquement) :

- Debian GNU/Linux 10.x (Buster)
- Debian GNU/Linux 11.x (Bullseye)
- Debian GNU/Linux 12 (Bookworm)
- Ubuntu Server 18.04 LTS (Bionic Beaver)
- Ubuntu Server 20.04 LTS (Focal Fossa)
- Ubuntu Server 22.04 LTS (Jammy Jellyfish)
- CentOS Stream 9
- Red Hat Enterprise Linux Server 7.x
- Red Hat Enterprise Linux Server 8.x
- Red Hat Enterprise Linux Server 9.x
- SUSE Linux Enterprise Server 12 (Tous Service Packs)
- SUSE Linux Enterprise Server 15 (Tous Service Packs)
- Astra Linux Special Edition RUSB.10015-01 (mise à jour opérationnelle 1.6)
- Astra Linux Special Edition RUSB.10015-01 (mise à jour opérationnelle 1.7)
- Astra Linux Special Edition RUSB.10015-01 (mise à jour opérationnelle 1.8) 64 bits
- Astra Linux Common Edition (mise à jour opérationnelle 2.12)
- ALT SP Server 10
- ALT Server 10
- ALT Server 9.2

- ALT 8 SP Server (LKNV.11100-01)
- ALT 8 SP Server (LKNV.11100-02)
- ALT 8 SP Server (LKNV.11100-03)
- Oracle Linux 7
- Oracle Linux 8
- Oracle Linux 9
- RED OS 7.3 Server
- RED OS 7.3 Certified Edition
- ROSA COBALT 7.9
- Machine virtuelle basée sur le noyau (tous les systèmes d'exploitation Linux pris en charge par le Serveur de Kaspersky Security Center Web Console)

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 100.0.4896.88 ou suivant (version officielle)
- Microsoft Edge 100 ou suivant
- Safari 15 sur macOS
- "Yandex" Browser 23.5.0.2271 ou version ultérieure
- Mozilla Firefox Extended Support Release 102.0 ou ultérieure

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.

Les systèmes d'exploitation suivants sont pris en charge :

- Microsoft Windows Embedded POSReady 2009 avec le dernier Service Pack 32 bits
- Microsoft Windows Embedded 7 Standard avec Service Pack 1 32 bits / 64 bits
- Microsoft Windows Embedded 8.1 Industry Pro 32 bits / 64 bits
- Microsoft Windows 10 Enterprise 2015 LTSB 32 bits / 64 bits
- Microsoft Windows 10 Enterprise 2016 LTSB 32 bits / 64 bits
- Microsoft Windows 10 IoT Enterprise 2015 LTSB 32 bits / 64 bits
- Microsoft Windows 10 IoT Enterprise 2016 LTSB 32 bits / 64 bits
- Microsoft Windows 10 Enterprise 2019 LTSC 32 bits / 64 bits
- Microsoft Windows 10 IoT Enterprise version 1703 32 bits / 64 bits
- Microsoft Windows 10 IoT Enterprise version 1709 32 bits / 64 bits
- Microsoft Windows 10 IoT Enterprise version 1803 32 bits / 64 bits
- Microsoft Windows 10 IoT Enterprise version 1809 32 bits / 64 bits
- Microsoft Windows 10 20H2 IoT Enterprise 32 bits / 64 bits
- Microsoft Windows 10 21H2 IoT Enterprise 32 bits / 64 bits
- Microsoft Windows 10 IoT Enterprise 32 bits / 64 bits
- Microsoft Windows 10 IoT Enterprise version 1909 32 bits / 64 bits
- Microsoft Windows 10 IoT Enterprise LTSC 2021 32 bits / 64 bits
- Microsoft Windows 10 IoT Enterprise version 1607 32 bits / 64 bits
- Microsoft Windows 10 Home RS3 (Fall Creators Update, v1709) 32 bits / 64 bits
- Microsoft Windows 10 Pro RS3 (Fall Creators Update, v1709) 32 bits / 64 bits
- Microsoft Windows 10 Pro for Workstations RS3 (Fall Creators Update, v1709) 32 bits / 64 bits
- Microsoft Windows 10 Enterprise RS3 (Fall Creators Update, v1709) 32 bits / 64 bits
- Microsoft Windows 10 Education RS3 (Fall Creators Update, v1709) 32 bits / 64 bits
- Microsoft Windows 10 Home RS4 (Mise à jour avril 2018, 17134) 32 bits / 64 bits
- Microsoft Windows 10 Pro RS4 (mise à jour d'avril 2018, 17134) 32 bits / 64 bits
- Microsoft Windows 10 Pro for Workstations RS4 (mise à jour d'avril 2018, 17134) 32 bits / 64 bits

- Microsoft Windows 10 Enterprise RS4 (mise à jour avril 2018, 17134) 32 bits / 64 bits
- Microsoft Windows 10 Education RS4 (mise à jour avril 2018, 17134) 32 bits / 64 bits
- Microsoft Windows 10 Famille RS5 (Octobre 2018) 32 bits / 64 bits
- Microsoft Windows 10 Pro RS5 (Octobre 2018) 32 bits / 64 bits
- Microsoft Windows 10 Pro pour les Stations de travail RS5 (Oct 2018) 32 bits / 64 bits
- Microsoft Windows 10 Entreprise RS5 (Octobre 2018) 32 bits / 64 bits
- Microsoft Windows 10 Education RS5 (Octobre 2018) 32 bits / 64 bits
- Microsoft Windows 10 Home 19H1 32 bits / 64 bits
- Microsoft Windows 10 Pro 19H1 32 bits / 64 bits
- Microsoft Windows 10 Pro pour les postes de travail 19H1 32 bits / 64 bits
- Microsoft Windows 10 Entreprise 19H1 32 bits / 64 bits
- Microsoft Windows 10 Education 19H1 32 bits / 64 bits
- Microsoft Windows 10 Home 19H2 32 bits / 64 bits
- Microsoft Windows 10 Pro 19H2 32 bits / 64 bits
- Microsoft Windows 10 Pro pour les Stations de travail 19H2 32 bits / 64 bits
- Microsoft Windows 10 Enterprise 19H2 32 bits / 64 bits
- Microsoft Windows 10 Education 19H2 32 bits / 64 bits
- Microsoft Windows 10 Home 20H1 (mise à jour mai 2020) 32 bits / 64 bits
- Microsoft Windows 10 Pro 20H1 (mise à jour mai 2020) 32 bits / 64 bits
- Microsoft Windows 10 Entreprise 20H1 (mise à jour mai 2020) 32 bits / 64 bits
- Microsoft Windows 10 Education 20H1 (mise à jour mai 2020) 32 bits / 64 bits
- Microsoft Windows 10 Home 20H2 (mise à jour octobre 2020) 32 bits / 64 bits
- Microsoft Windows 10 Pro 20H2 (mise à jour octobre 2020) 32 bits / 64 bits
- Microsoft Windows 10 Entreprise 20H2 (mise à jour octobre 2020) 32 bits / 64 bits
- Microsoft Windows 10 Education 20H2 (mise à jour octobre 2020) 32 bits / 64 bits
- Microsoft Windows 10 Home 21H1 (mise à jour mai 2021) 32 bits / 64 bits
- Microsoft Windows 10 Pro 21H1 (mise à jour mai 2021) 32 bits / 64 bits
- Microsoft Windows 10 Entreprise 21H1 (mise à jour mai 2021) 32 bits / 64 bits

- Microsoft Windows 10 Education 21H1 (mise à jour mai 2021) 32 bits / 64 bits
- Microsoft Windows 10 Home 21H2 (mise à jour octobre 2021) 32 bits / 64 bits
- Microsoft Windows 10 Pro 21H2 (mise à jour octobre 2021) 32 bits / 64 bits
- Microsoft Windows 10 Entreprise 21H2 (mise à jour octobre 2021) 32 bits / 64 bits
- Microsoft Windows 10 Education 21H2 (mise à jour octobre 2021) 32 bits / 64 bits
- Microsoft Windows 10 Home 22H2 (mise à jour octobre 2023) 32 bits / 64 bits
- Microsoft Windows 10 Pro 22H2 (mise à jour octobre 2023) 32 bits / 64 bits
- Microsoft Windows 10 Entreprise 22H2 (mise à jour octobre 2023) 32 bits / 64 bits
- Microsoft Windows 10 Education 22H2 (mise à jour octobre 2023) 32 bits / 64 bits
- Microsoft Windows 11 Home 64 bits
- Microsoft Windows 11 Pro 64 bits
- Microsoft Windows 11 Enterprise 64 bits
- Microsoft Windows 11 Education 64 bits
- Microsoft Windows 11 22H2
- Microsoft Windows 8.1 Pro 32 bits / 64 bits
- Microsoft Windows 8.1 Entreprise 32 bits / 64 bits
- Microsoft Windows 8 Pro 32 bits / 64 bits
- Microsoft Windows 8 Entreprise 32 bits / 64 bits
- Microsoft Windows 7 Professional avec Service Pack 1 et suivants 32 bits / 64 bits
- Microsoft Windows 7 Enterprise/Ultimate avec Service Pack 1 et suivants 32 bits / 64 bits
- Microsoft Windows 7 Home Basic/Premium avec Service Pack 1 et versions ultérieures 32 bits / 64 bits
- Microsoft Windows XP Professional with Service Pack 2 32 bits / 64 bits (uniquement pris en charge par l'Agent d'administration version 10.5.1781)
- Microsoft 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)
- Microsoft 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, que vous pouvez demander via le Support technique)

- Windows Server 2008 Foundation avec SP2 32 bits / 64 bits
- Microsoft Windows Server 2008 avec Service Pack 2 (toutes les versions) 32 bits / 64 bits
- Windows Server 2008 R2 Datacenter avec Service Pack 1 et suivants 64 bits
- Windows Server 2008 R2 Enterprise avec Service Pack 1 et suivants 64 bits
- Windows Server 2008 R2 Foundation avec Service Pack 1 et suivants 64 bits
- Windows Server 2008 R2 Core Mode avec Service Pack 1 et versions ultérieures 64 bits
- Windows Server 2008 R2 Standard avec Service Pack 1 et suivants 64 bits
- Windows Server 2008 R2 avec Service Pack 1 (toutes les éditions) 64 bits
- Windows Server 2012 Server Core 64 bits
- Windows Server 2012 Datacenter 64 bits
- Windows Server 2012 Essentials 64 bits
- Windows Server 2012 Foundation 64 bits
- Windows Server 2012 Standard 64 bits
- Windows Server 2012 R2 Server Core 64 bits
- Windows Server 2012 R2 Datacenter 64 bits
- Windows Server 2012 R2 Essentials 64 bits
- Windows Server 2012 R2 Foundation 64 bits
- Windows Server 2012 R2 Standard 64 bits
- Windows Server 2016 Datacenter (LTSB) 64 bits
- Windows Server 2016 Standard (LTSB) 64 bits
- Windows Server 2016 Server Core (option d'installation) (LTSB) 64 bits
- Windows Server 2019 Standard 64 bits
- Windows Server 2019 Datacenter 64 bits
- Windows Server 2019 Core 64 bits
- Windows Server 2022 Standard 64 bits
- Windows Server 2022 Datacenter 64 bits
- Windows Server 2022 Core 64 bits
- 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) 32 bits / 64 bits
- Ubuntu Server 20.04 LTS (Focal Fossa) 32 bits / 64 bits
- Ubuntu Server 22.04 LTS (Jammy Jellyfish) 64 bits
- CentOS 7.x 64 bits
- CentOS Stream 9 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 Desktop 15 avec Service Pack 3 ARM 64 bits
- openSUSE 15 64 bits
- EulerOS 2.0 SP8 ARM 64 bits
- Astra Linux Special Edition RUSB.10015-01 (mise à jour opérationnelle 1.6) 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 Common Edition (mise à jour opérationnelle 2.12) 64 bits
- Astra Linux Special Edition RUSB.10152-02 (mise à jour opérationnelle 4.7) ARM 64 bits
- ALT SP Server 10 64 bits
- ALT SP Workstation 10 64 bits
- ALT Server 10 64 bits
- ALT Server 9.2 64 bits
- ALT Workstation 9.2 32 bits / 64 bits
- ALT Workstation 10 32 bits / 64 bits
- ALT 8 SP Server (LKNV.11100-01) 64 bits

- ALT 8 SP Server (LKNV.11100-02) 64 bits
- ALT 8 SP Server (LKNV.11100-03) 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
- AlterOS 7.5 et suivant 64 bits
- GosLinux IC6 64 bits
- RED OS 7.3 Server 64 bits
- RED OS 7.3 Édition certifiée 64 bits
- ROSA COBALT 7.9 64 bits
- ROSA CHROME 12 64 bits
- macOS 11.x
- macOS 12.x
- macOS 13.x
- macOS 14.x
  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
- VMware Workstation 16 Pro
- VMware Workstation 17 Pro
- Microsoft Hyper-V Server 2012 64 bits

- Microsoft Hyper-V Server 2012 R2 64 bits
- Microsoft Hyper-V Server 2016 64 bits
- 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 17
- Oracle VM VirtualBox 6.x
- Oracle VM VirtualBox 7.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, Windows Server 2008 R2 ou Windows MultiPoint Server 2011, 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 pour Linux que Kaspersky Security Center Linux.

Kaspersky Security Center Linux 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.

Kit de distribution

Vous pouvez acheter l'application via les boutiques en ligne de Kaspersky (par exemple https://www.kaspersky.fr) ou un site d'un partenaire.

En achetant Kaspersky Security Center Linux dans la boutique en ligne, vous copiez l'application depuis le site Internet de la boutique en ligne. Les informations indispensables à l'activation de l'application vous seront envoyées par email après le paiement.

À propos de la compatibilité du Serveur d'administration et de Kaspersky Security Center Web Console

Nous vous recommandons d'utiliser la dernière version du Serveur d'administration de Kaspersky Security Center Linux et de Kaspersky Security Center Web Console. Dans le cas contraire, les fonctionnalités de Kaspersky Security Center Linux peuvent être limitées.

Vous pouvez installer et mettre à niveau le Serveur d'administration de Kaspersky Security Center Linux 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 :

- Web Console inclus dans Kaspersky Security Center 15 prend en charge le Serveur d'administration de Kaspersky Security Center Linux des versions suivantes : 15 et 14.2.
- Le Serveur d'administration inclus dans Kaspersky Security Center 15 prend en charge Kaspersky Security Center Web Console des versions suivantes : 15 et 14.2.

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 Linux. Pour obtenir des informations détaillées sur la solution Windows, consultez l'aide en ligne de Kaspersky Security Center Windows.

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.

Comparaison des fonctionnalités de Kaspersky Security Center fonctionnant comme une solution basée sur Windows et une solution basée sur Linux

Fonctionnalité ou propriété	Kaspersky Security Center 14.2 Windows	Kaspersky Security Center 15 Linux
Emplacement du Serveur d'administration	Sur site	Sur site

Emplacement du système de gestion de base de données (SGBD)	Sur site	Sur site
Système d'exploitation sur lequel installer le Serveur d'administration	Windows	Linux
Type de Console d'administration	Sur site et en ligne	Basé sur le Web
Système d'exploitation sur lequel installer la Console d'administration Web	Windows ou Linux	Linux
Hiérarchie des Serveurs d'administration	✓	✓
Hiérarchie du groupe d'administration	✓	✓
Sondage réseau	✓	✓ (par plages IP et contrôleurs de domaine, Samba 4 Active Directory, Microsoft Active Directory)
Nombre maximum d'appareils administrés	100 000	50 000 (avec PostgreSQL et Postgres Pro)
Protection des appareils administrés Windows, macOS et Linux	✓	✓
Protection des appareils mobiles	✓	—
Protection des machines virtuelles	✓	✓
Protection de l'infrastructure Cloud publique	✓	—
Administration de la sécurité centrée sur l'appareil	✓	✓
Administration de la sécurité centrée sur l'utilisateur	✓	✓
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	✓	✓
Mise à jour automatique des bases antivirus	✓	✓
Prise en charge des Serveurs d'administration virtuels	✓	✓
Installation des mises à jour du logiciel tiers et correction des vulnérabilités dans les applications tierces	✓	— (en utilisant une tâche d'installation à distance uniquement)
Notifications sur les événements survenus sur les appareils administrés	✓	✓
Création et gestion des comptes utilisateurs	✓	✓
Se connecter à la console à l'aide de l'authentification de domaine	✓	✓ (L'authentification unique n'est pas prise en charge)
Intégration avec les systèmes SIEM	✓	✓ (en utilisant Syslog uniquement)
Surveillance de l'état des stratégies et des tâches	✓	✓
Déploiement du cluster de basculement Kaspersky Security Center	✓	✓
Installation du Serveur d'administration sur un cluster de basculement Windows Server	✓	—
Utilisation de SNMP pour envoyer les statistiques du Serveur d'administration à des applications tierces	✓	—
Diagnostic à distance des appareils clients	✓	✓
Connexion à distance au bureau d'un appareil client	✓	—

Utilisation des révisions des objets	✓	—
Mise à jour automatique des applications Kaspersky	✓	—
Déploiement des systèmes d'exploitation sur les appareils clients	✓	—
Serveur Web pour la publication des paquets d'installation et d'autres fichiers	✓	—
Consultation et utilisation des alertes détectées par Kaspersky Endpoint Detection and Response Optimum	✓	✓
Utilisation du Serveur d'administration comme serveur WSUS	✓	—
Intégration avec Kaspersky Managed Detection and Response	✓	—
Prise en charge du Contrôle évolutif des anomalies	✓	—
Prise en charge des clusters et des matrices de serveurs dans les groupes d'administration	✓ (uniquement dans la Console d'administration basée sur MMC)	✓
Administration des licences tierces	✓	—

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

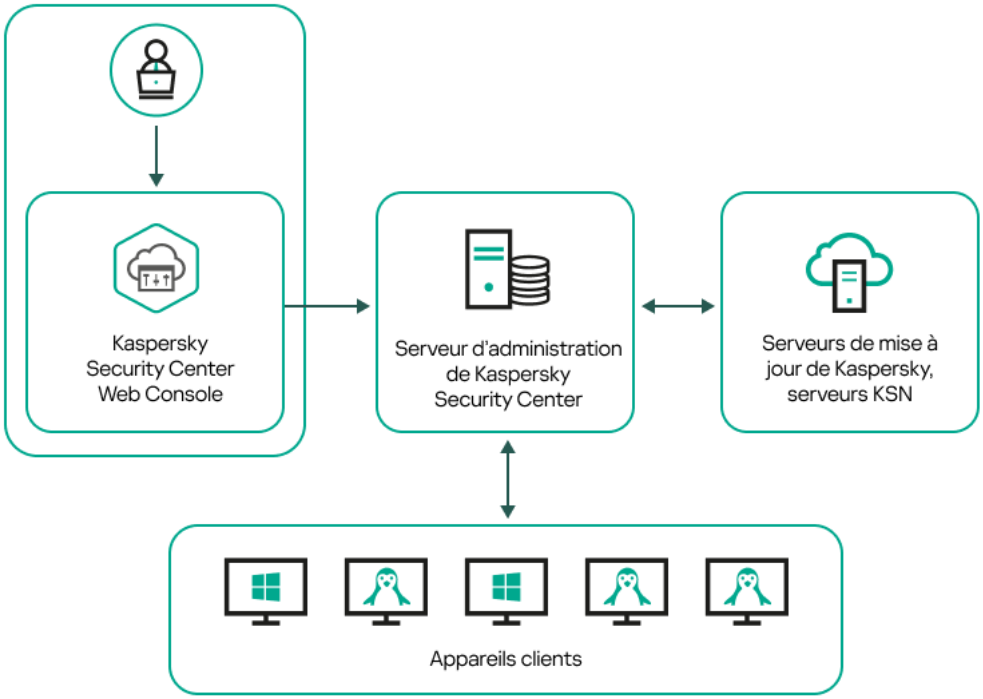
Plus d'informations à propos de Kaspersky Security Center Cloud Console et ses caractéristiques sont disponibles dans la documentation de Kaspersky Security Center Cloud Console et dans la documentation de Kaspersky Endpoint Security for Business.

Architecture et concepts de base

Cette section explique l'architecture de l'application et les concepts de base liés à Kaspersky Security Center Linux.

Architecture

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



Architecture de Kaspersky Security Center Linux

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

- **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 Linux. L'une des applications de sécurité Kaspersky doit être installée sur chacun des appareils à protéger.

Diagramme de déploiement du Serveur d'administration de Kaspersky Security Center Linux et de Kaspersky Security Center Web Console

La figure ci-dessous illustre le diagramme de déploiement du Serveur d'administration de Kaspersky Security Center Linux et de Kaspersky Security Center Web Console

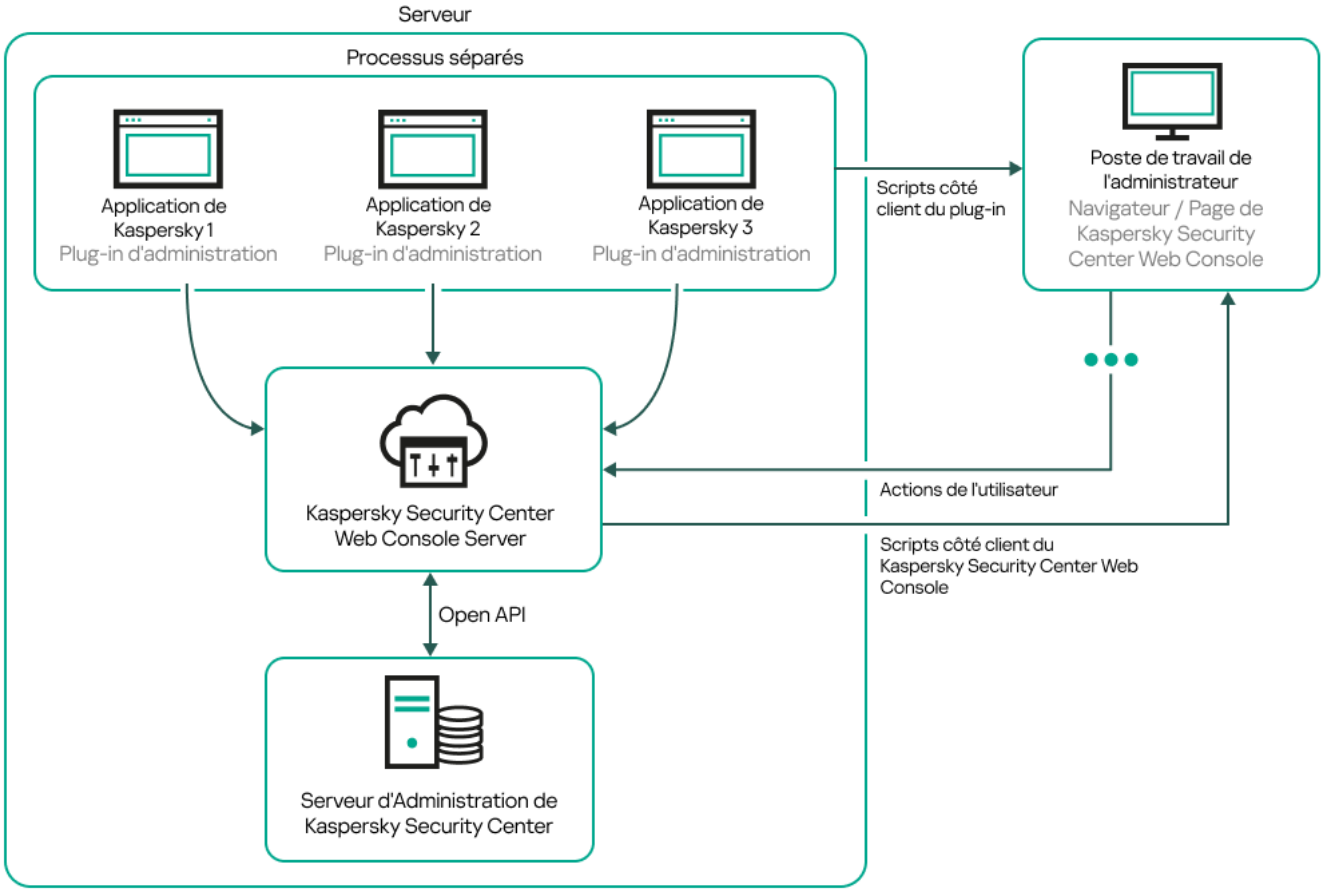


Diagramme de déploiement du Serveur d'administration de Kaspersky Security Center Linux et de Kaspersky Security Center Web Console

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 Linux via OpenAPI. Le serveur Kaspersky Security Center Web Console sollicite les informations requises au Serveur d'administration de Kaspersky Security Center Linux et affiche les résultats de vos opérations dans Kaspersky Security Center Web Console.

Ports utilisés par Kaspersky Security Center Linux

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

Port utilisé par le Serveur d'administration de Kaspersky Security Center Linux

Numéro de	Nom du	Protocole	Destination du port	Zone de fonctionnement

port	processus qui a ouvert le port			
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 Internet** de la fenêtre des propriétés du Serveur d'administration. 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 Internet** de la fenêtre des propriétés du Serveur d'administration.
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 lors de l'installation de Kaspersky Security Center Linux ; vous pouvez modifier le numéro de port par défaut pour recevoir les connexions des Serveurs d'administration secondaires lors de la création d'une hiérarchie de Serveurs d'administration.
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 la stratégie de l'Agent d'administration.
13291	klserver	TCP (TLS)	Utilisation de l'utilitaire klakaut pour automatiser le fonctionnement de Kaspersky Security Center Linux	Utilisation de l'utilitaire klakaut. Ce port est fermé par défaut. Si vous souhaitez utiliser l'utilitaire klakaut pour automatiser le fonctionnement de Kaspersky Security Center Linux, ouvrez le port 13291 à l'aide de l'utilitaire klscflag.
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	Gestion du Serveur d'administration à l'aide de Kaspersky Security Center Web Console ; fonctionnant avec OpenAPI. Vous pouvez modifier le numéro de port par défaut dans la fenêtre des propriétés du Serveur d'Administration (dans la sous-section **Ports de connexion** de la section **Général**) ou lors de la création d'une hiérarchie de Serveurs d'Administration.
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 Linux 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.
15111 (uniquement si le service KSN Proxy	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.

est exécuté sur l'appareil)				
17000	klactprx	TCP (TLS)	Réception des connexions pour l'activation de l'application depuis les appareils administrés	Serveur proxy d'activation pour les appareils administrés. Vous pouvez modifier le numéro de port par défaut dans la fenêtre des propriétés du Serveur d'administration (dans la sous-section **Ports supplémentaires** de la section **Général**).

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 MariaDB). Veuillez vous référer à la documentation du SGBD pour les informations pertinentes.

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. 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 la stratégie de l'Agent d'administration.
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.
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.

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.

Prenez également en compte le fait que les recommandations sur la compatibilité de Kaspersky Security Center Linux avec les logiciels tiers sont décrites à titre de référence 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 des Agents d'administration et des passerelles de connexion	Administration des appareils client, remise des mises à jour et des paquets d'installation. Vous pouvez modifier le numéro de port par défaut dans les propriétés du point de distribution.
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 les propriétés du point de distribution.
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 les propriétés du point de distribution.

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

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 des plug-ins d'administration
1329,	Service	HTTPS	Ports de l'API utilisés pour recevoir les requêtes du	Mise à jour des composants de

2003	d'administration de Kaspersky Security Center Web Console.		" Service d'administration de Kaspersky Security Center Web Console " s'exécutant sur le même appareil	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 de Kaspersky Security Center Web Console
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 14.2 Web Console et des plug-ins d'administration	Interaction entre Kaspersky Security Center Web Console et les plug-ins d'administration

Notions principales

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

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 :

- Avec le nom `kladminserver_srv`
- Configuré de manière à démarrer automatiquement au démarrage du système d'exploitation
- Avec le compte utilisateur `ksc` ou le compte utilisateur selon la sélection effectuée lors de l'installation du Serveur d'administration

Pour obtenir la liste complète des paramètres d'installation, consultez la rubrique suivante : Installation de Kaspersky Security Center Linux.

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 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 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.

Dans la hiérarchie, un Serveur d'administration basé sur Linux peut fonctionner à la fois comme Serveur primaire et comme Serveur secondaire. Le Serveur primaire basé sur Linux peut gérer à la fois les Serveurs secondaires Linux et Windows. Un Serveur Windows primaire peut administrer un Serveur Linux secondaire.

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 Linux 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 Linux relance le Serveur d'administration principal et tous les Serveurs d'administration 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 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, 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.

Le dossier partagé est utilisé pour le stockage des informations disponibles pour 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 :

- `<nom du Serveur Web>` 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 Linux. 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 Linux.

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 télécharger le paquet d'installation d'Agent d'administration à partir des sources suivantes :

- Stockage du Serveur d'administration (le Serveur d'administration doit être installé)
- Serveurs Web de Kaspersky

Par défaut, l'Agent d'administration est installé aux emplacements suivants :

- Pour Linux :
  - Systèmes 32 bits : /opt/kaspersky/klnagent/
  - Systèmes 64 bits : /opt/kaspersky/klnagent64/
- Pour les appareils Windows :
  - Systèmes 32 bits : C:\Program Files\Kaspersky Lab\NetworkAgent
  - Systèmes 64 bits : C:\Program Files (x86)\Kaspersky Lab\NetworkAgent

Pour les appareils Windows, vous pouvez spécifier un dossier différent pour l'installation de l'Agent d'administration dans les paramètres du paquet d'installation. Cependant, pour les appareils Linux, l'Agent d'administration ne peut être installé que dans le répertoire par défaut.

Le dossier d'installation de l'Agent d'administration contient également des utilitaires permettant de gérer et de diagnostiquer le fonctionnement de l'Agent d'administration, tels que les utilitaires klmover et klnagchk.

Lors de l'installation du Serveur d'administration, l'Agent d'administration version serveur est automatiquement installé avec le Serveur d'administration. Néanmoins, pour administrer l'appareil doté du Serveur d'administration comme tout autre appareil administré, il faut installer l'Agent d'administration pour Linux sur l'appareil du Serveur d'administration. Dans ce cas, l'Agent d'administration pour Linux est installé et fonctionne indépendamment de la version serveur de l'Agent d'administration que vous avez installé avec le Serveur d'administration.

Les noms des processus lancés par l'Agent d'administration sont les suivants :

- klnagent64.service (pour un système d'exploitation 64 bits)
- klnagent.service (pour un système d'exploitation 32 bits)

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 Linux.

Pour tous les appareils administrées 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 Linux, Windows ou macOS et sur lequel l'Agent d'administration est installé. 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 donner à un appareil 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 administrées jusqu'à 20 000 appareils.

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

Les appareils sur lesquels Kaspersky Security Center Web Console Server est installé sont appelés *postes de travail de l'administrateur*. A partir de ces appareils, les administrateurs peuvent administrer à distance de manière centralisée les applications de Kaspersky installées sur les appareils clients.

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 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. L'état d'une stratégie est l'un des suivants :

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.
- 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 Linux 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 Linux 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

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 Kaspersky Security Center Web Console, mais aussi par l'utilisateur de l'appareil à distance (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 le journal des événements Syslog et dans le journal des événements de Kaspersky Security Center Linux, de manière centralisée sur le Serveur d'administration et localement 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) 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 déployer les mises à jour, à installer les applications à distance et à recevoir des informations sur les appareils du réseau.

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 mises à jour et les paquets d'installation reçus du Serveur d'administration aux appareils clients au sein du groupe (y compris la distribution via la multidiffusion à l'aide d'UDP). 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 points de distribution accélèrent la diffusion des mises à jour et permettent d'économiser les ressources du Serveur d'administration.

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

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

  Si une connexion directe entre les appareils administrés au sein du groupe et le Serveur d'administration ne peut pas être établie, vous pouvez utiliser le point de distribution comme passerelle de connexion au Serveur d'administration pour ce groupe. 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 des applications de Kaspersky et d'autres éditeurs de logiciels, y compris 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 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.

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 Linux attribue à chaque Agent d'administration une adresse IP de multidiffusion unique qui diffère de toutes les autres adresses. Cela permet d'éviter un excès de charge sur le réseau, ce qui se produirait en cas d'interaction des adresses. Les adresses de diffusion IP multiple déjà attribuée dans les versions antérieures de l'application ne sont pas modifiées.

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.

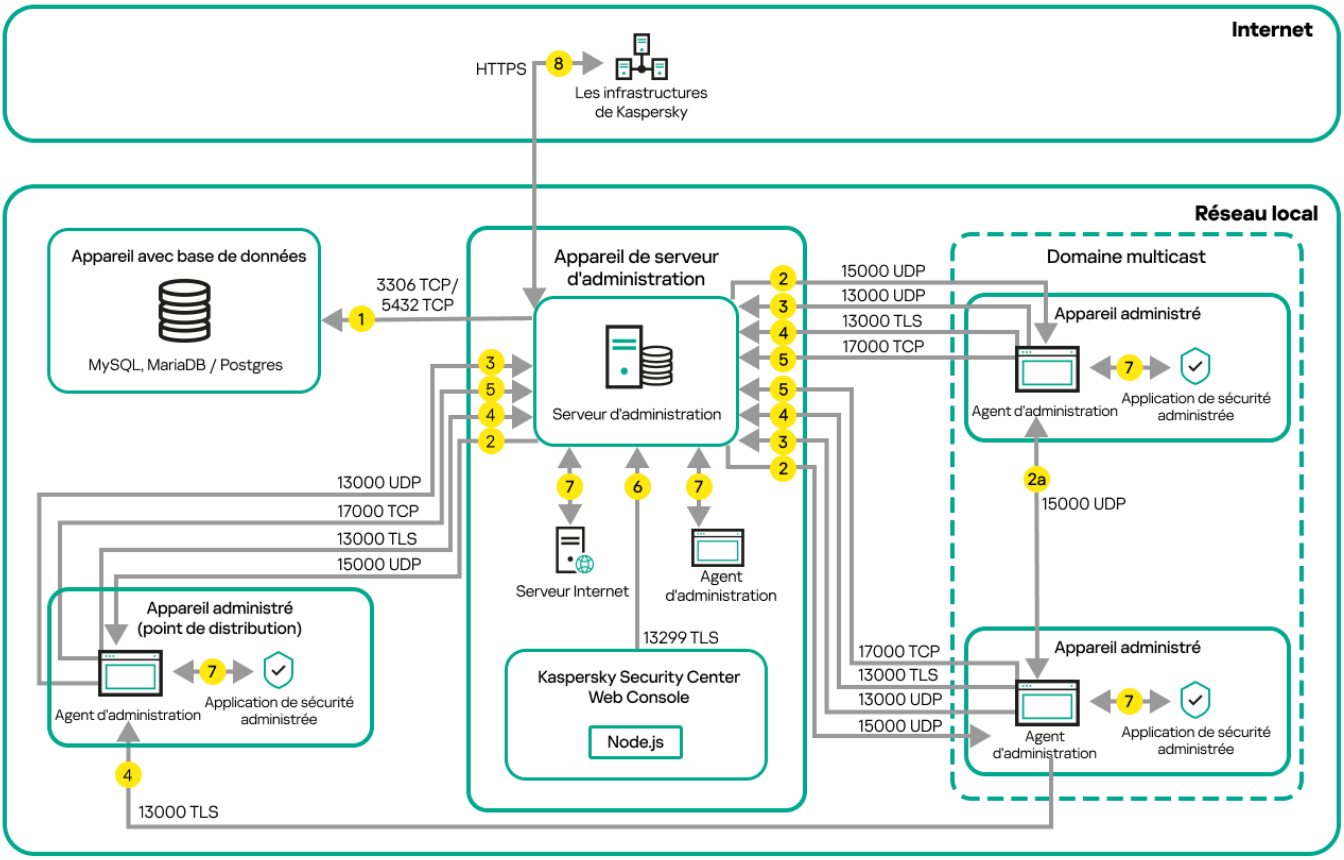
- Vous pouvez également utiliser des passerelles de connexion au sein du réseau. Par exemple, les points de distribution attribués automatiquement deviennent également des passerelles de connexion dans leur propre zone d'action. Cependant, au sein d'un réseau interne, les passerelles de connexion n'offrent 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.

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 Linux, 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 et MariaDB Server, ou le port 5432 pour PostgreSQL Server ou Postgres Pro 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.

   2a. Les Agents d'administration sur les appareils administrés non mobiles échangent des données sur d'autres Agents d'administration au sein du même domaine de diffusion (les données sont ensuite envoyées au Serveur d'administration).

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.

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. 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.

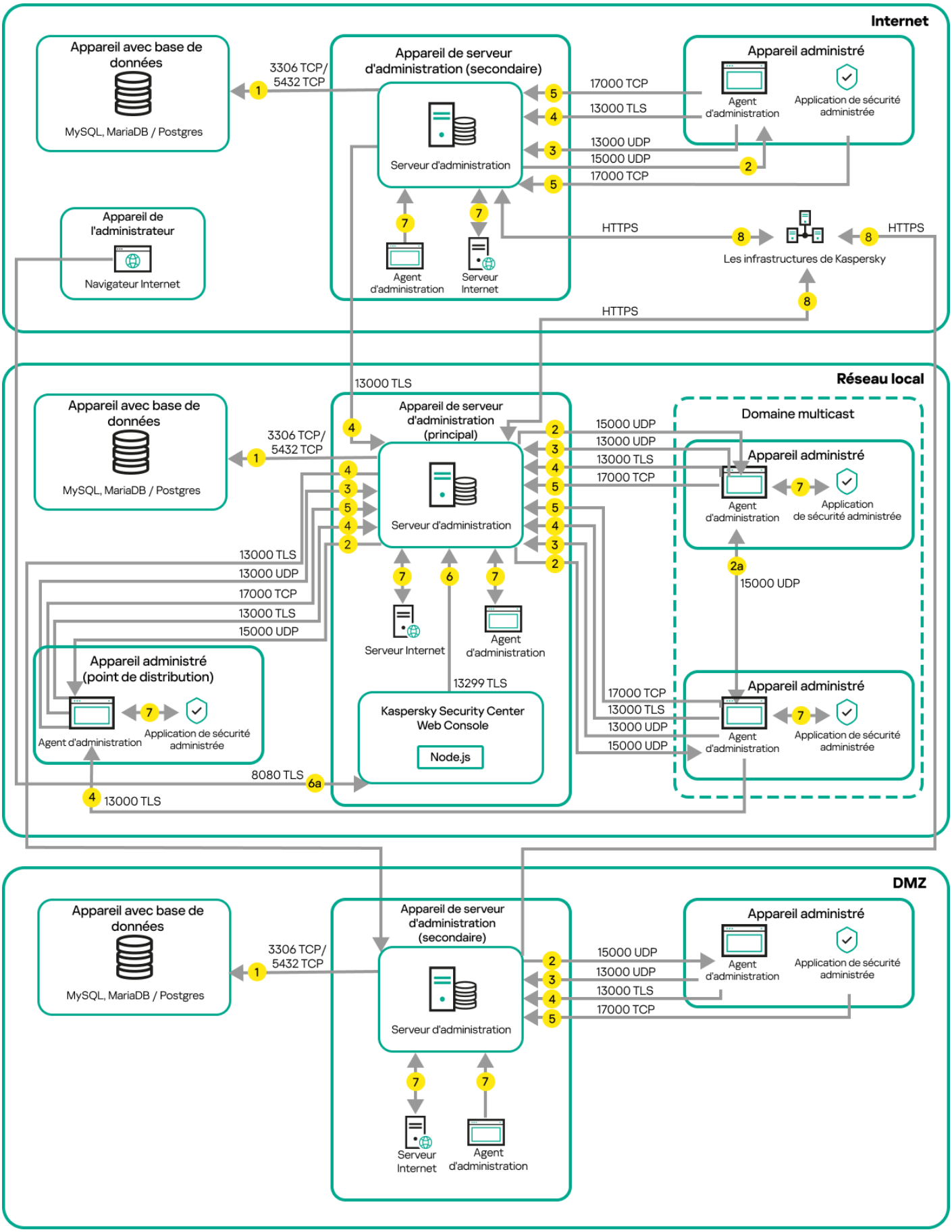
7. Les applications sur un seul appareil échangent du trafic local (sur le Serveur d'administration ou sur un appareil administré). Aucun port externe ne doit être ouvert.

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.

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 et MariaDB Server, ou le port 5432 pour PostgreSQL Server ou Postgres Pro 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 Linux 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.

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. 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.

   6a. 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.

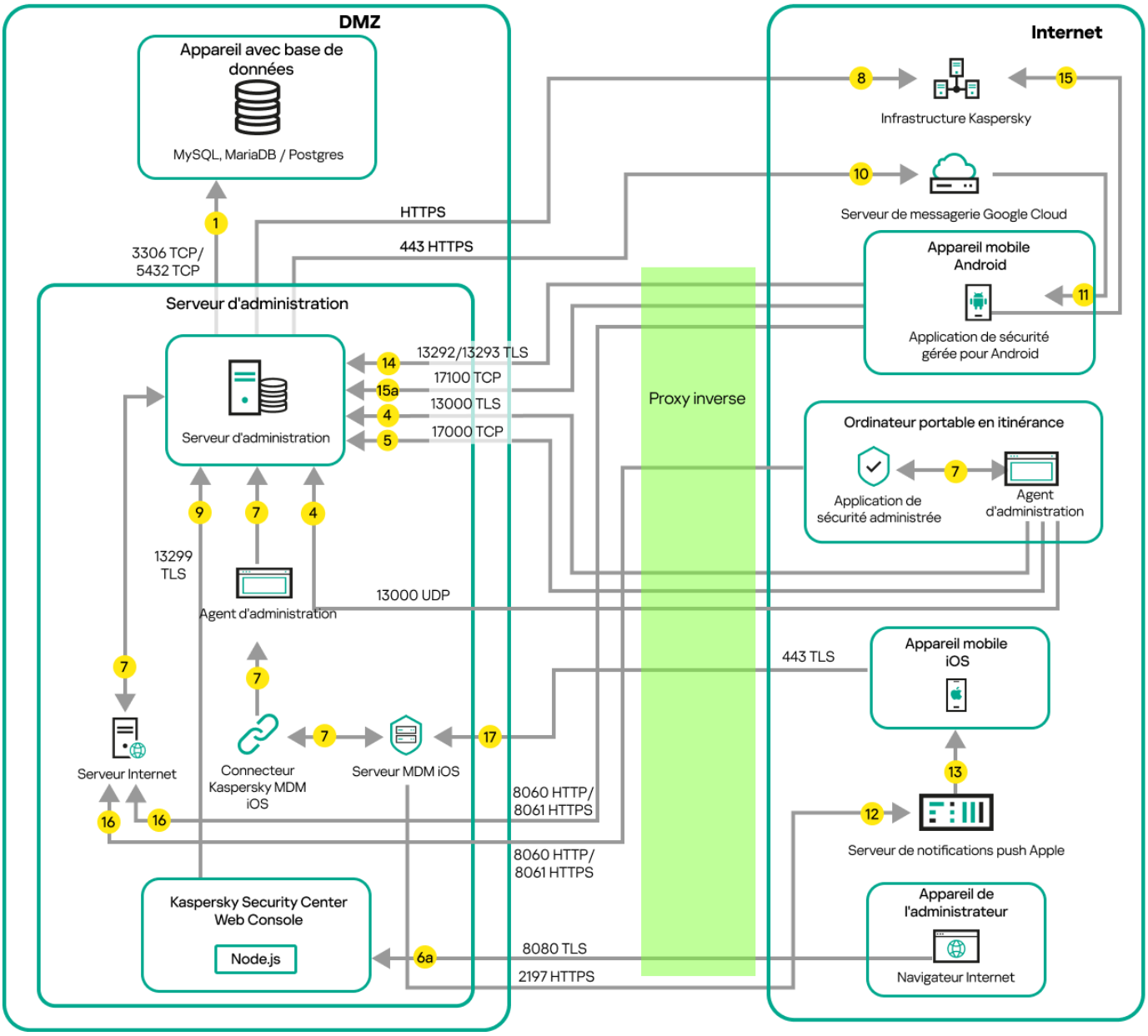
7. Les applications sur un seul appareil échangent du trafic local (sur le Serveur d'administration ou sur un appareil administré). Aucun port externe ne doit être ouvert.

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.

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 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 et MariaDB Server, ou le port 5432 pour PostgreSQL Server ou Postgres Pro 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 Linux 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.

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. 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.

   6a. 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.

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.

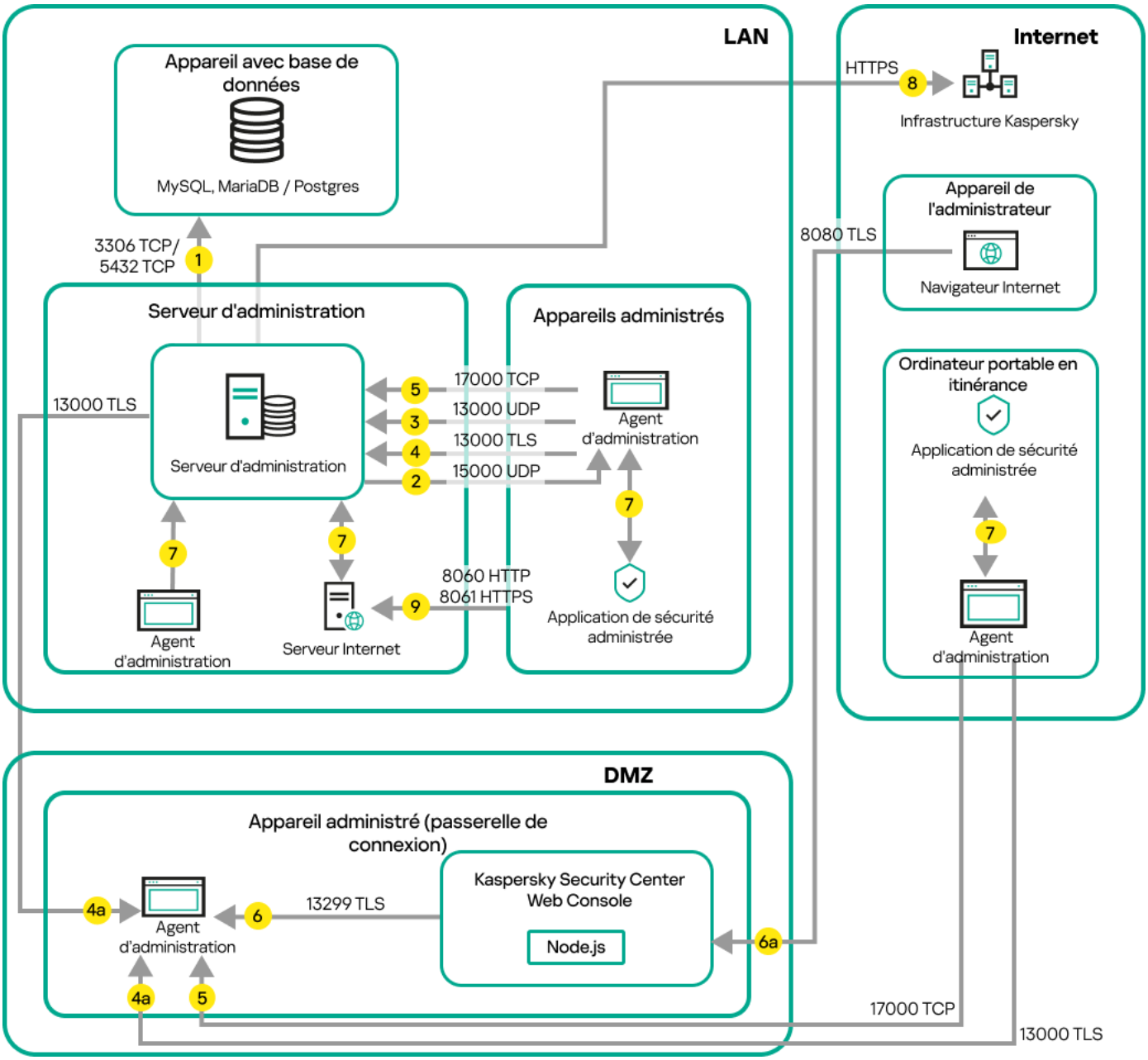
   Si vous ne voulez pas que votre Serveur d'administration accède à Internet, vous devez gérer ces données manuellement.

9. 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.

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 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 administrés 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 et MariaDB Server, ou le port 5432 pour PostgreSQL Server ou Postgres Pro 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 Linux 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.

   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. 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.

   6a. 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.

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.

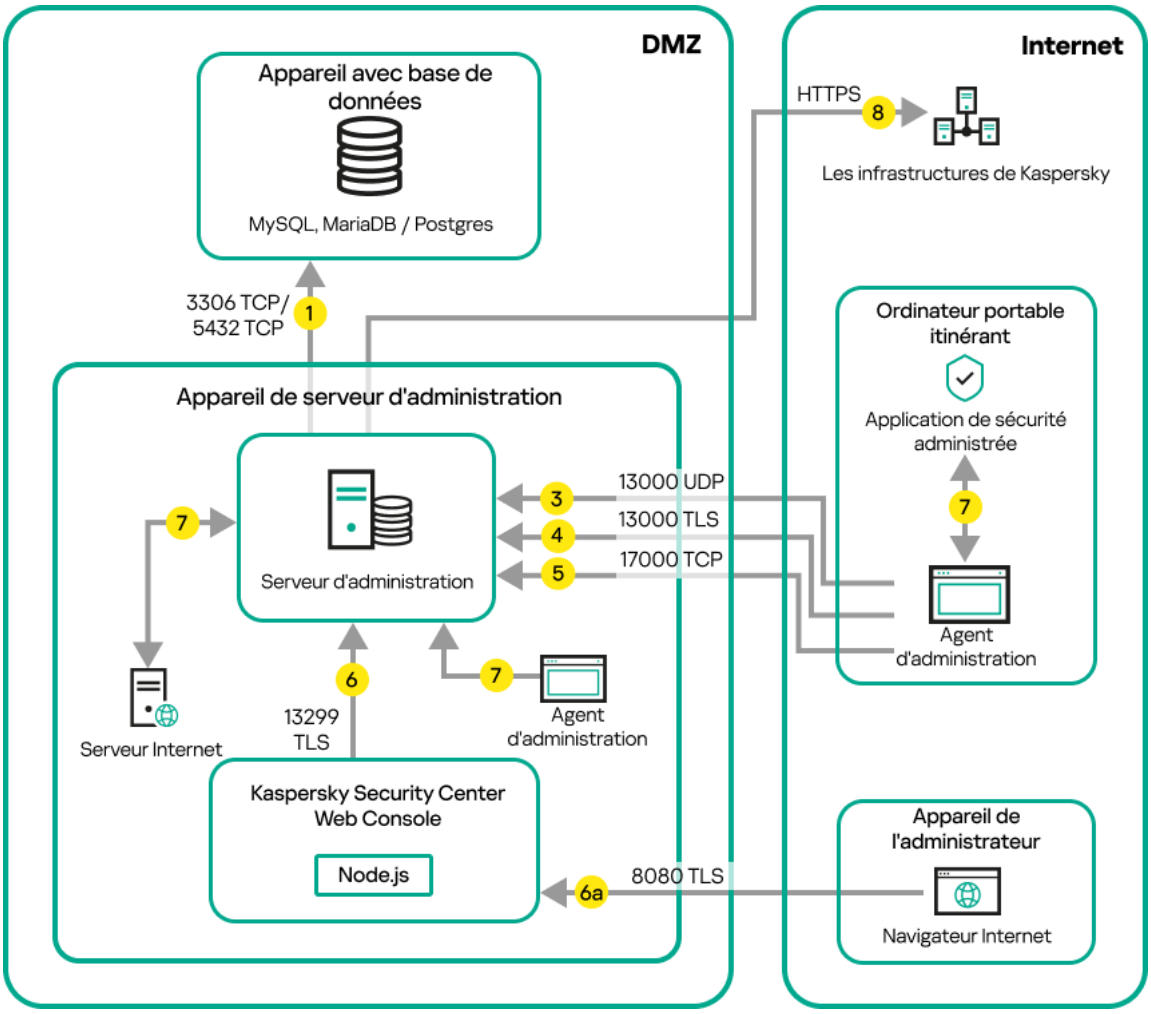
8. Le transfert des données du Serveur d'administration aux serveurs Kaspersky (telles que les données KSN ou les informations sur les licences) et le transfert des données des serveurs Kaspersky au Serveur d'administration (telles que les mises à jour d'applications et les mises à jour de bases de données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

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 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 et MariaDB Server, ou le port 5432 pour PostgreSQL Server ou Postgres Pro 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 Linux 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.

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. 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.

   6a. 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.

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

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

Cette section présente les schémas d'interaction entre les modules figurant dans Kaspersky Security Center Linux 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.

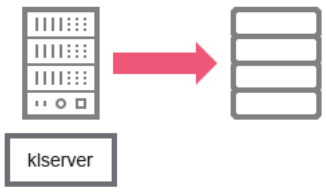
Conventions

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 famille Kaspersky Endpoint Security (ou une autre application de sécurité pouvant être administrée par Kaspersky Security Center Linux)
	Passerelle des connexions
	Point de distribution
	Navigateur sur l'appareil de l'utilisateur
klnagent	Processus exécuté sur l'appareil et ouvrant un port, quel qu'il soit
13000 TLS	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)
	Transport du SGBD
	Frontière de la zone démilitarisée

Serveur d'administration et SGBD

Les données du Serveur d'administration entrent dans la base de données.

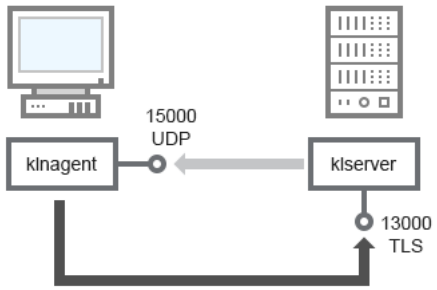


Serveur d'administration et SGBD

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 MariaDB). Veuillez vous référer à la documentation du SGBD pour les informations pertinentes.

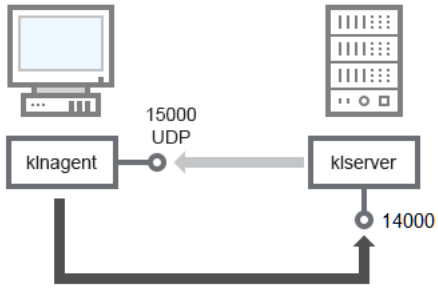
Serveur d'administration et appareil client : administration de l'application de sécurité

Le Serveur d'administration accepte la connexion depuis les Agents d'administration par le port TLS 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 Linux, 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 Linux prend aussi en charge la connexion depuis les Agents d'administration par le port 14000. Cependant, il est recommandé d'utiliser le port SSL 13000.



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

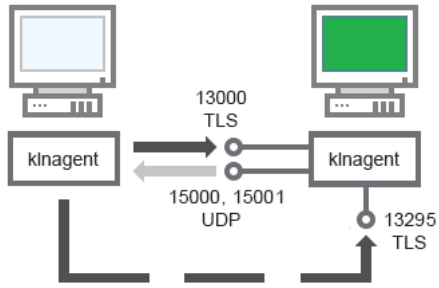
Pour avoir des explications sur les schémas, cf. tableau ci-après.

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	Destination du port
Agent d'administration	15000	klnagent	UDP	Diffusion multicast vers les Agents d'administration
Serveur d'administration	13000	klserver	TCP (TLS)	Réception des connexions des Agents d'administration
Serveur d'administration	14000	klserver	TCP	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.

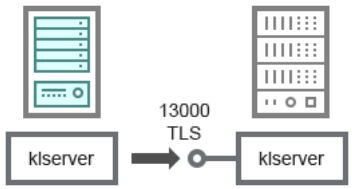
Mise à niveau du logiciel par un point de distribution (trafic)

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

Ensuite, après le regroupement des Serveurs d'administration dans une hiérarchie, vous pourrez administrer les deux Serveurs via Kaspersky Security Center Web Console connecté au Serveur d'administration primaire. Ainsi, seul le port 13299 du Serveur d'administration principal doit être accessible.



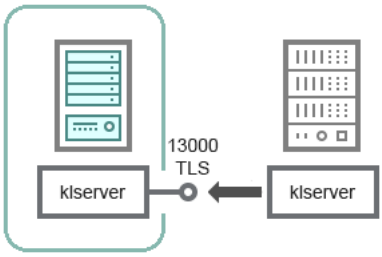
Hiérarchie des Serveurs d'administration : Serveur d'administration principal et Serveur d'administration secondaire

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	Destination du port
Serveur d'administration principal	13000	klserver	TCP (TLS)	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

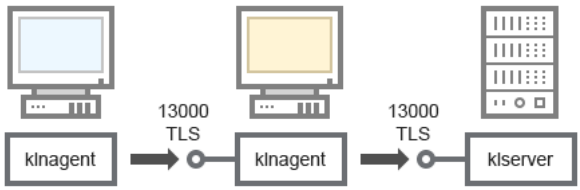
Le schéma illustre une hiérarchie de Serveurs d'administration dans laquelle le Serveur d'administration secondaire, situé dans la zone démilitarisée, reçoit une connexion d'un Serveur d'administration principal (les explications du schéma sont reprises dans le tableau ci-après). En cas de regroupement de Serveurs dans une hiérarchie, le port 13299 des deux Serveurs doit être accessible. Kaspersky Security Center Web Console se connecte au Serveur d'administration via le port 13299.

Ensuite, après le regroupement des Serveurs d'administration dans une hiérarchie, vous pourrez administrer les deux Serveurs via Kaspersky Security Center Web Console connecté au Serveur d'administration primaire. Ainsi, seul le port 13299 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	Destination du port
Serveur d'administration secondaire	13000	klserver	TCP (TLS)	Réception des connexions du Serveur d'administration principal

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



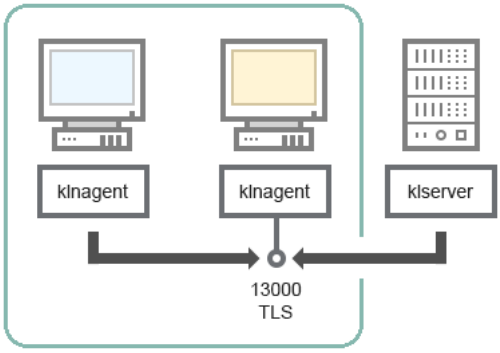
Serveur d'administration, passerelle de connexion dans un segment du réseau et appareil client

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	Destination du port
Serveur d'administration	13000	klserver	TCP (TLS)	Réception des connexions des Agents d'administration
Agent d'administration	13000	klnagent	TCP (TLS)	Réception des connexions des Agents d'administration

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



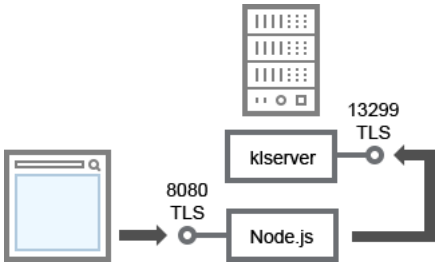
Serveur d'administration et passerelle de connexion et appareil client dans la zone démilitarisée

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	Destination du port
Agent d'administration	13000	klnagent	TCP (TLS)	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	Destination du port
Serveur d'administration	13299	klserver	TCP (TLS)	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 (TLS)	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.

Guide de démarrage

Suite à ce scénario, vous pouvez installer le Serveur d'administration de Kaspersky Security Center Linux et de Kaspersky Security Center Web Console, effectuer la configuration initiale du Serveur d'administration via l'Assistant de configuration initiale de l'application et installer les applications de Kaspersky sur les appareils administrés à l'aide de l'Assistant de déploiement de la protection.

Prérequis

Vous devez disposer d'une clé de licence (code d'activation) pour Kaspersky Endpoint Security for Business ou de clés de licence (codes d'activation) pour les applications de sécurité Kaspersky.

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

Étapes

Le scénario d'installation principal se déroule par étapes :

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

   Prenez connaissance des modules de Kaspersky Security Center Linux. 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).

   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.

2. **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.

3. **Installation d'un système de gestion de base de données (SGDB)**

   Installez le SGBD que Kaspersky Security Center Linux va utiliser ou utiliser le SGBD existant.

   Vous pouvez choisir parmi l'un des SGBDs pris en charge. Pour en savoir plus sur l'installation du SGBD sélectionné, consultez sa documentation.

   Si la distribution de votre système d'exploitation Linux ne contient pas de SGBD pris en charge, vous pouvez installer le SGBD depuis un stockage de paquets tiers. Si l'installation de distributions à partir de stockages tiers est interdite, vous pouvez installer le SGBD sur un appareil distinct.

   > 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.

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

Si vous souhaitez modifier le type de SGBD après l'installation, vous devez réinstaller Kaspersky Security Center Linux. Les données peuvent être transférées partiellement et manuellement dans une autre base de données.

4. **Configuration des ports**

   Assurez-vous que, pour l'interaction des composants 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.

5. **Installation de Kaspersky Security Center Linux**

   Sélectionnez un appareil Linux que vous souhaitez utiliser comme Serveur d'administration, assurez-vous que l'appareil possède la configuration logicielle et matérielle requise, puis installez Kaspersky Security Center Linux sur l'appareil. La version serveur de l'Agent d'administration est automatiquement installée avec le Serveur d'administration.

6. **Installation de Kaspersky Security Center Web Console et des plug-ins d'administration web**

   Sélectionnez un appareil Linux que vous comptez utiliser comme poste de travail de l'administrateur, assurez-vous que l'appareil possède la configuration logicielle et matérielle requise, puis installez Kaspersky Security Center Web Console sur l'appareil. Vous pouvez installer Kaspersky Security Center Web Console soit sur le même appareil où le Serveur d'administration est installé, soit sur un autre appareil.

   Téléchargez le plug-in Web d'administration de Kaspersky Endpoint Security for Linux puis installez-le sur le même appareil où Kaspersky Security Center Web Console est installé.

7. **Installation de Kaspersky Endpoint Security for Linux et de l'Agent d'administration sur l'appareil du Serveur d'administration**

   Par défaut, l'application ne considère pas l'appareil du Serveur d'administration comme un appareil administré. Pour protéger le Serveur d'administration des virus et autres menaces, et pour administrer l'appareil comme tout autre appareil administré, nous vous recommandons d' installer Kaspersky Endpoint Security for Linux et Agent d'administration pour Linux sur l'appareil du Serveur d'administration. Dans ce cas, l'Agent d'administration pour Linux est installé et fonctionne indépendamment de la version serveur de l'Agent d'administration que vous avez installé avec le Serveur d'administration.

8. **Configuration initiale**

   Après l'achèvement de l'installation du Serveur d'administration 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.

9. **Recherche d'appareils sur le réseau**

   Découvrez les appareils manuellement. Suite à cela, Kaspersky Security Center Linux 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 Linux des applications de Kaspersky et d'autres éditeurs sur les appareils détectées. Kaspersky Security Center Linux lance la recherche d'appareils régulièrement. Par conséquent, si de nouveaux appareils apparaissent sur le réseau, ils seront détectés automatiquement.

10. **Organisation des appareils dans les 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.

11. **Assignation des points de distribution**

    Les points de distribution pour les groupes d'administration sont assignés automatiquement mais, en cas de nécessité, vous pouvez les assigner manuellement. 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.

12. **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 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).

13. **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.

14. **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.

15. **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 Linux et de Kaspersky Security Center Web Console.

Configuration du serveur MariaDB x64 pour fonctionner avec Kaspersky Security Center Linux

Paramètres recommandés pour le fichier my.cnf

Pour plus de détails sur la configuration du SGBD, reportez-vous aussi à la procédure de configuration de compte utilisateur. Pour plus d'informations sur l'installation du SGBD, reportez-vous à la procédure d'installation du SGBD.

Pour configurer le fichier my.cnf :

1. Ouvrez le fichier my.cnf avec un éditeur de texte.

2. Saisissez les lignes suivantes dans la section [mysqld] du fichier my.cnf :

```
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=<value>
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
```

   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 10.6, 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`, `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. Assurez-vous 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 les valeurs `on`, alors les modules complémentaires d'optimisation sont activés.

   Si ces lignes manquent ou ont la valeurs `off`, vous devez effectuer les opérations suivantes :

   a. Ouvrez le fichier my.cnf avec un éditeur de texte.

b. Ajoutez les lignes suivantes dans le fichier my.cnf :

```
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 PostgreSQL ou Postgres Pro pour fonctionner avec Kaspersky Security Center Linux

Kaspersky Security Center Linux 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 Linux.

Le chemin d'accès par défaut au fichier de configuration est :
`/etc/postgresql/<VERSION>/main/postgresql.conf`

Paramètres recommandés pour PostgreSQL et Postgres Pro :

- `shared_buffers` = 25 % de la valeur de la mémoire RAM 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` = taille maximale de pile (exécutez la commande '`ulimit -s`' pour obtenir cette valeur en Ko) moins 1 Mo de marge de sécurité
- `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 un SGBD Postgres en cluster, indiquez le paramètre `max_connections` pour tous les serveurs SGBD ainsi que dans la configuration du cluster.

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.

Installation de Kaspersky Security Center Linux

Cette procédure décrit l'installation de Kaspersky Security Center Linux.

Avant l'installation :

- Installation d'un SGBD.
- Assurez-vous que l'appareil sur lequel vous voulez installer Kaspersky Security Center Linux fonctionne sur une des distributions Linux supportées.
- Assurez-vous que le serveur DNS est disponible sur le réseau.

Utiliser le fichier d'installation ksc64_[numéro_version]_amd64.deb ou ksc64-[numéro_version].x86_64.rpm correspondant à la distribution Linux installée sur votre appareil. Vous récupérez le fichier d'installation en le téléchargeant du site Web de Kaspersky.

Pour installer Kaspersky Security Center Linux, exécutez les commandes fournies dans les instructions ci-dessous sous un compte avec des privilèges root.

Pendant l'installation du Kaspersky Security Center Linux:

1. Si votre appareil fonctionne sous Astra Linux 1.8 ou une version ultérieure, exécutez les actions décrites à cette étape. Si votre appareil fonctionne sous un autre système d'exploitation, passez à l'étape suivante.

   a. Créez le répertoire /etc/systemd/system/kladminserver_srv.service.d et créez un fichier nommé override.conf avec le contenu suivant :

   ```
   [Service]
   User=
   User=ksc
   CapabilitiesParsec=PARSEC_CAP_PRIV_SOCK
   ExecStart=
   ExecStart=/opt/kaspersky/ksc64/sbin/klserver -d from_wd
   ```

   b. Créez un répertoire /etc/systemd/system/klwebsrv_srv.service.d et créez un fichier nommé override.conf avec le contenu suivant :

   ```
   [Service]
   User=
   User=ksc
   CapabilitiesParsec=PARSEC_CAP_PRIV_SOCK
   ExecStart=
   ExecStart=/opt/kaspersky/ksc64/sbin/klcsweb -d from_wd
   ```

2. Créez un groupe kladmins et un compte non privilégié ksc. Le compte doit être membre du groupe kladmins. Pour ce faire, exécutez les commandes suivantes en séquence :

   ```
   # adduser ksc
   # groupadd kladmins
   # gpasswd -a ksc kladmins
   # usermod -g kladmins ksc
   ```

3. Augmentez la limite par défaut des fichiers qui peuvent être ouverts (descripteurs de fichiers) pour les comptes utilisés pour la fonctionnalité des services du Serveur d'administration. Pour ce faire, ouvrez le fichier /etc/security/limits.conf, puis définissez les limites logicielles et matérielles des descripteurs de fichier comme suit :

```
ksc     soft    nofile  32768
ksc     hard    nofile  131072
```

4. Exécuter le fichier d'installation de Kaspersky Security Center Linux. En fonction de votre distribution Linux, exécutez l'une des commandes suivantes :

   - `# apt install /<path>/ksc64_[ version_number ]_amd64.deb`
   - `# yum install /<path>/ksc64-[ version_number ].x86_64.rpm -y`

5. Exécuter le fichier de configuration de Kaspersky Security Center Linux.

```
# /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
```

6. Lisez le Contrat de licence utilisateur final (CLUF) et la Politique de confidentialité. 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 les valeurs suivantes :

   a. 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 Kaspersky Security Center Linux, vous devez accepter les conditions du Contrat de licence utilisateur final.

   b. Saisissez `y` si vous comprenez et acceptez les conditions de la Politique de confidentialité et que vous acceptez que vos données soient traitées et transmises (y compris vers des pays tiers) comme décrit dans celle-ci. Saisissez `n` si vous n'acceptez pas les conditions de la Politique de confidentialité. Pour utiliser Kaspersky Security Center Linux, vous devez accepter les conditions de la Politique de confidentialité.

7. Lorsque vous y êtes invité, saisissez les paramètres suivants :

   a. Saisissez le nom DNS ou l'adresse IP statique du Serveur d'administration. Cette adresse sera utilisée par d'autres appareils pour se connecter au Serveur d'administration.

   b. Entrez le numéro de port SSL du Serveur d'administration. Le numéro de port est de 13000 par défaut.

   c. Estimez le nombre approximatif d'appareils que vous entendez administrer :

      - Si votre réseau prend en charge entre 1 et 100 appareils, saisissez 1.
      - Si votre réseau prend en charge entre 101 et 1 000 appareils, saisissez 2.
      - Si votre réseau prend en charge plus de 1 000 appareils, saisissez 3.

   d. Saisissez le nom du groupe de sécurité pour les services. Par défaut, le groupe `kladmins` est utilisé.

   e. Saisissez le nom du compte pour lancer le service Serveur d'administration. Le compte doit faire partie du groupe de sécurité saisi. Par défaut, le compte `ksc` est utilisé.

   f. Saisissez le nom du compte pour lancer d'autres services. Le compte doit faire partie du groupe de sécurité saisi. Par défaut, le compte `ksc` est utilisé.

   g. Sélectionnez le SGBD que vous avez installé pour fonctionner avec Kaspersky Security Center Linux:

      - Si vous avez installé MySQL ou MariaDB, saisissez 1.

- Si vous avez installé PostgreSQL ou Postgres Pro, saisissez 2.

h. Saisissez le nom DNS ou l'adresse IP de l'appareil sur lequel la base de données est installée. `127.0.0.1` par défaut pour une installation de base de données locale.

i. Saisissez le numéro de port de la base de données. Ce port sert à communiquer avec le Serveur d'administration. Par défaut, les ports suivants sont utilisés :

- Port `3306` pour MySQL ou MariaDB
- Port `5432` pour PostgreSQL ou Postgres Pro

j. Saisissez le nom de la base de données.

k. Saisissez l'identifiant de connexion du compte racine de la base de données que vous utilisez pour accéder à la base de données.

l. Saisissez le mot de passe du compte racine de la base de données que vous utilisez pour accéder à la base de données.

Attendez que les services soient ajoutés et lancés automatiquement :

- `klnagent_srv`
- `kladminserver_srv`
- `klactprx_srv`
- `klwebsrv_srv`

m. Créez un compte qui agira en tant qu'administrateur du Serveur d'administration. Saisissez le nom d'utilisateur et le mot de passe. Vous pouvez utiliser la commande suivante pour créer un nouvel utilisateur : `/opt/kaspersky/ksc64/sbin/kladduser -n ksc -p <password>`

Le mot de passe doit remplir 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 (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)

L'utilisateur est ajouté et Kaspersky Security Center Linux est installé.

Vérification du service

Utilisez les commandes suivantes pour vérifier si un service est en cours d'exécution ou non :

- `# systemctl status klnagent_srv.service`

- `# systemctl status kladminserver_srv.service`
- `# systemctl status klactprx_srv.service`
- `# systemctl status klwebsrv_srv.service`

Installation de Kaspersky Security Center Linux en mode silencieux

Vous pouvez installer Kaspersky Security Center Linux sur les appareils Linux en utilisant le fichier de réponses pour lancer l'installation en mode silencieux, c'est-à-dire sans la participation de l'utilisateur. Le fichier de réponses contient un ensemble personnalisé de paramètres d'installation : les variables et leurs valeurs respectives.

Avant l'installation :

- Installation d'un système de gestion de base de données (SGDB).
- Assurez-vous que l'appareil sur lequel vous voulez installer Kaspersky Security Center Linux fonctionne sur une des distributions Linux supportées.

Pour installer Kaspersky Security Center Linux en mode silencieux, procédez comme suit :

1. 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.
2. Si votre appareil fonctionne sous Astra Linux 1.8 ou une version ultérieure, exécutez les actions décrites à cette étape. Si votre appareil fonctionne sous un autre système d'exploitation, passez à l'étape suivante.

   a. Créez le répertoire /etc/systemd/system/kladminserver_srv.service.d et créez un fichier nommé override.conf avec le contenu suivant :
   ```
   [Service]
   User=
   User=ksc
   CapabilitiesParsec=PARSEC_CAP_PRIV_SOCK
   ExecStart=
   ExecStart=/opt/kaspersky/ksc64/sbin/klserver -d from_wd
   ```

   b. Créez un répertoire /etc/systemd/system/klwebsrv_srv.service.d et créez un fichier nommé override.conf avec le contenu suivant :
   ```
   [Service]
   User=
   User=ksc
   CapabilitiesParsec=PARSEC_CAP_PRIV_SOCK
   ExecStart=
   ExecStart=/opt/kaspersky/ksc64/sbin/klcsweb -d from_wd
   ```
3. Créez un groupe 'kladmins' et un compte non privilégié 'ksc', qui doit être membre du groupe 'kladmins'. Pour ce faire, exécutez les commandes suivantes sous un compte avec les privilèges root dans l'ordre :
   ```
   # adduser ksc
   # groupadd kladmins
   # gpasswd -a ksc kladmins
   # usermod -g kladmins ksc
   ```
4. Créez le fichier de réponses (au format TXT) et ajoutez dans le fichier de réponses une liste de variables au format `VARIABLE_NAME=variable_value`, chacune sur une ligne distincte. Le fichier de réponses doit inclure les variables répertoriées dans le tableau ci-dessous.

5. Définissez la valeur de la variable d'environnement `KLAUTOANSWERS` à la racine de l'environnement utilisateur contenant le nom complet du fichier de réponses incluant le chemin d'accès, par exemple, à l'aide de la commande suivante :

   ```
   export KLAUTOANSWERS=/tmp/ksc_install/answers.txt
   ```

6. Exécutez l'installation de Kaspersky Security Center Linux en mode silencieux — selon votre distribution Linux, exécutez une des commandes suivantes :

   Dans l'environnement racine :

   - `# apt install /<path>/ksc64_[ version_number ]_amd64.deb`
   - `# yum install /<path>/ksc64-[ version_number ].x86_64.rpm -y`

   Dans l'environnement utilisateur :

   - `$ sudo -E apt install /<chemin>/ksc64_[ version_number ]_amd64.deb`
   - `$ sudo -E yum install /<chemin>/ksc64-[ version_number ].x86_64.rpm -y`

7. Créez un utilisateur pour travailler avec Kaspersky Security Center Web Console. Pour ce faire, exécutez la commande suivante sous le compte avec les privilèges root :

   `/opt/kaspersky/ksc64/sbin/kladduser -n ksc -p < password >`, où le mot de passe doit contenir au moins 8 caractères.

Variables du fichier de réponses utilisées comme paramètres d'installation de Kaspersky Security Center Linux en mode silencieux

Nom de la variable	Requis	Description	Valeurs possibles
`EULA_ACCEPTED`	Oui	Confirme que vous comprenez et acceptez les termes du Contrat de licence utilisateur final.	`1`
`PP_ACCEPTED`	Oui	Confirme que vous avez compris et accepté les conditions de la Politique de confidentialité.	`1`
`KLSRV_UNATT_SERVERADDRESS`	Oui	Le nom DNS ou l'adresse IP statique du Serveur d'administration.	Nom DNS ou adresse IP
`KLSRV_UNATT_PORT_SRV`	Non	Le numéro de port du Serveur d'administration. Facultatif, la valeur par défaut est 14000.	Numéro de port
`KLSRV_UNATT_PORT_SRV_SSL`	Non	Le numéro de port SSL du Serveur d'administration. Facultatif, la valeur par défaut est égale à 13000.	Numéro de port
`KLSRV_UNATT_PORT_KLOAPI`	Non	Le numéro de port pour utiliser OpenAPI. Ce port est également utilisé pour recevoir les connexions de Kaspersky Security Center Web Console. Facultatif, la valeur par défaut est 13299.	Numéro de port
`KLSRV_UNATT_PORT_GUI`	Non	Le numéro du port pour travailler avec l'utilitaire klakaut. Facultatif, la valeur par défaut est égale à 13291. Ce port est fermé par défaut. Si vous souhaitez utiliser l'utilitaire klakaut pour automatiser le fonctionnement de Kaspersky Security Center Linux, ouvrez le port 13291 à l'aide de l'utilitaire klscflag.	Numéro de port
`KLSRV_UNATT_NETRANGETYPE`	Non	Le nombre approximatif d'appareils que vous entendez administrer. Facultatif, la valeur par défaut est égale à 1.	`1` pour 1 à 100 appareils en réseau. `2` pour 101 à 1 000 appareils en réseau. `3` pour plus de 1 000 appareils en réseau.

KLSRV_UNATT_DBMS_INSTANCE	Oui	L'adresse IP du serveur de base de données.	Adresse IP
KLSRV_UNATT_DBMS_PORT	Oui	Le port du serveur de base de données.	3306
KLSRV_UNATT_DB_NAME	Oui	Le nom de la base de données.	kav
KLSRV_UNATT_DBMS_LOGIN	Oui	Le nom d'utilisateur qui a accès à la base de données.	
KLSRV_UNATT_DBMS_PASSWORD	Oui	Le mot de passe d'un utilisateur qui a accès à la base de données.	
KLSRV_UNATT_KLADMINSGROUP	Oui	Le nom du groupe de sécurité pour les services.	kladmins
KLSRV_UNATT_KLSRVUSER	Oui	Le nom du compte pour lancer le service Serveur d'administration. Le compte doit être membre du groupe de sécurité spécifié dans la variable KLSRV_UNATT_KLADMINSGROUP.	ksc
KLSRV_UNATT_KLSVCUSER	Oui	Le nom du compte pour lancer d'autres services. Le compte doit être membre du groupe de sécurité spécifié dans la variable KLSRV_UNATT_KLADMINSGROUP.	ksc
Si le Serveur d'administration doit être déployé en tant que cluster de basculement Kaspersky Security Center Linux, le fichier de réponses doit inclure les variables supplémentaires suivantes :			
KLFOC_UNATT_NODE	Oui	Le numéro du nœud (1 ou 2).	1 ou 2
KLFOC_UNATT_STATE_SHARE_MOUNT_PATH	Oui	Point de montage du partage de l'état.	
KLFOC_UNATT_DATA_SHARE_MOUNT_PATH	Oui	Point de montage du partage de données.	
KLFOC_UNATT_CONN_MODE	Oui	Le mode de connectivité du cluster de basculement.	VirtualAdapter ou ExternalLoadBalancer
Si la variable KLFOC_UNATT_CONN_MODE a la valeur VirtualAdapter, le fichier de réponses doit inclure les variables supplémentaires suivantes :			
KLFOC_UNATT_CONN_MODE_VA_NAME	Oui	Nom de la carte réseau virtuelle.	
KLFOC_UNATT_CONN_MODE_VA_IPV4	L'une de ces variables est obligatoire	Adresse IP de la carte réseau virtuelle.	Adresse IP
KLFOC_UNATT_CONN_MODE_VA_IPV6		Adresse IPv6 de la carte réseau virtuelle.	Adresse IPv6

Installation de Kaspersky Security Center Linux sur Astra Linux dans un environnement logiciel fermé

Cette section décrit l'installation de Kaspersky Security Center Linux sur le système d'exploitation Astra Linux Special Edition.

Avant l'installation :

- Installer un SGBD.
- Téléchargez la clé de l'application kaspersky_astra_pub_key.gpg.

Utilisez le fichier d'installation ksc64_[version_number]_amd64.deb. Vous récupérez le fichier d'installation en le téléchargeant du site Web de Kaspersky.

Sous un compte disposant des privilèges root, exécutez les commandes indiquées dans cette instruction avec un haut niveau d'intégrité et sans aucune confidentialité.

Pour installer Kaspersky Security Center Linux sur les systèmes d'exploitation Astra Linux Special Edition (mise à jour opérationnelle 1.7.2) et Astra Linux Special Edition (mise à jour opérationnelle 1.6) :

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 dans le répertoire créé à l'étape précédente :

   ```
   cp kaspersky_astra_pub_key.gpg /etc/digsig/keys/legacy/kaspersky/
   ```

5. Mettez à jour l'image initiale du système de fichiers RAM pour tous les noyaux du système :

   ```
   update-initramfs -u -k all
   ```

   Redémarrez le système.

6. Si votre appareil fonctionne sous Astra Linux 1.8 ou une version ultérieure, exécutez les actions décrites à cette étape. Si votre appareil fonctionne sous un autre système d'exploitation, passez à l'étape suivante.

   a. Créez le répertoire /etc/systemd/system/kladminserver_srv.service.d et créez un fichier nommé override.conf avec le contenu suivant :

   ```
   [Service]
   User=
   User=ksc
   CapabilitiesParsec=PARSEC_CAP_PRIV_SOCK
   ExecStart=
   ExecStart=/opt/kaspersky/ksc64/sbin/klserver -d from_wd
   ```

   b. Créez un répertoire /etc/systemd/system/klwebsrv_srv.service.d et créez un fichier nommé override.conf avec le contenu suivant :

   ```
   [Service]
   User=
   User=ksc
   CapabilitiesParsec=PARSEC_CAP_PRIV_SOCK
   ExecStart=
   ExecStart=/opt/kaspersky/ksc64/sbin/klcsweb -d from_wd
   ```

7. Créez un groupe kladmins et un compte non privilégié ksc. Le compte doit être membre du groupe kladmins. Pour ce faire, exécutez les commandes suivantes en séquence :

   ```
   # adduser ksc
   # groupadd kladmins
   # gpasswd -a ksc kladmins
   # usermod -g kladmins ksc
   ```

8. Exécuter le fichier d'installation de Kaspersky Security Center Linux :

   ```
   # apt install /<path>/ksc64_[ version_number ]_amd64.deb
   ```

9. Exécuter le fichier de configuration de Kaspersky Security Center Linux.

```
# /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
```

10. Lisez le Contrat de licence utilisateur final (CLUF) et la Politique de confidentialité. Le texte s'affiche dans la fenêtre de ligne de commande. Appuyez sur la barre espace pour afficher le segment de texte suivant. Lorsque vous y êtes invité, saisissez les paramètres suivants :

    a. 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 Kaspersky Security Center Linux, vous devez accepter les conditions du Contrat de licence utilisateur final.

    b. Saisissez `y` si vous comprenez et acceptez les conditions de la Politique de confidentialité et que vous acceptez que vos données soient traitées et transmises (y compris vers des pays tiers) comme décrit dans celle-ci. Saisissez `n` si vous n'acceptez pas les conditions de la Politique de confidentialité. Pour utiliser Kaspersky Security Center Linux, vous devez accepter les conditions de la Politique de confidentialité.

11. Lorsque vous y êtes invité, saisissez les paramètres suivants :

    a. Saisissez le nom DNS ou l'adresse IP statique du Serveur d'administration.

    b. Entrez le numéro de port du Serveur d'administration. Le numéro de port est de 14000 par défaut.

    c. Entrez le numéro de port SSL du Serveur d'administration. Le numéro de port est de 13000 par défaut.

    d. Estimez le nombre approximatif d'appareils que vous entendez administrer :

    - Si votre réseau prend en charge entre 1 et 100 appareils, saisissez 1.
    - Si votre réseau prend en charge entre 101 et 1 000 appareils, saisissez 2.
    - Si votre réseau prend en charge plus de 1 000 appareils, saisissez 3.

    e. Saisissez le nom du groupe de sécurité pour les services. Par défaut, le groupe "kladmins" est utilisé.

    f. Saisissez le nom du compte pour lancer le service Serveur d'administration. Le compte doit faire partie du groupe de sécurité saisi. Par défaut, le compte "ksc" est utilisé.

    g. Saisissez le nom du compte pour lancer d'autres services. Le compte doit faire partie du groupe de sécurité saisi. Par défaut, le compte "ksc" est utilisé.

    h. Saisissez l'adresse IP de l'appareil sur lequel la base de données est installée.

    i. Saisissez le numéro de port de la base de données. Ce port sert à communiquer avec le Serveur d'administration. Le numéro de port est de 3306 par défaut.

    j. Saisissez le nom de la base de données.

    k. Saisissez l'identifiant de connexion du compte racine de la base de données que vous utilisez pour accéder à la base de données.

    l. Saisissez le mot de passe du compte racine de la base de données que vous utilisez pour accéder à la base de données.

    Attendez que les services soient ajoutés et lancés automatiquement :

    - `klnagent_srv`
    - `kladminserver_srv`

- `klactprx_srv`
- `klwebsrv_srv`

m. Créez un compte qui agira en tant qu'administrateur du Serveur d'administration. Saisissez le nom d'utilisateur et le mot de passe.

Le mot de passe doit remplir les conditions suivantes :

- Le mot de passe utilisateur doit comporter 8 caractères au moins et 16 caractères au maximum.
- 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 (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)

Kaspersky Security Center Linux est installé et l'utilisateur est ajouté.

Vérification du service

Utilisez les commandes suivantes pour vérifier si un service est en cours d'exécution ou non :

- `# systemctl status klnagent_srv.service`
- `# systemctl status kladminserver_srv.service`
- `# systemctl status klactprx_srv.service`
- `# systemctl status klwebsrv_srv.service`

Installation de Kaspersky Security Center Web Console

Cette section décrit comment installer Kaspersky Security Center Web Console Server (appelé aussi Kaspersky Security Center Web Console) sur des appareils qui fonctionnent avec un système d'exploitation Linux. Avant de lancer l'installation, vous devez installer un SGBD et le Serveur d'administration de Kaspersky Security Center Linux.

Si vous installez Kaspersky Security Center Web Console sur Astra Linux en mode environnement logiciel fermé, suivez les instructions spécifiques à Astra Linux.

Utilisez l'un des fichiers d'installation suivants qui correspond à la distribution Linux installée sur votre appareil :

- Pour Debian : ksc-web-console-[build_number].x86_64.deb
- Pour les systèmes d'exploitation basés sur RPM : ksc-web-console-[build_number].x86_64.rpm

- Pour ALT 8 SP : ksc-web-console-[build_number]-alt8p.x86_64.rpm

Vous récupérez le fichier d'installation en le téléchargeant du site Web de Kaspersky.

Installation de Kaspersky Security Center Web Console :

1. Assurez-vous que l'appareil sur lequel vous voulez installer Kaspersky Security Center Web Console fonctionne sur une des distributions Linux supportées.

2. Lisez le Contrat de licence utilisateur final (CLUF). Si le kit de distribution Kaspersky Security Center Linux ne contient pas de fichier TXT avec le texte du CLUF, vous pouvez télécharger le fichier depuis le site de Kaspersky. Si vous refusez les dispositions du Contrat de licence, n'installez pas l'application.

3. Créez un fichier de réponse qui contient les paramètres pour connecter Kaspersky Security Center Web Console au serveur d'administration. Nommez ce fichier ksc-web-console-setup.json et placez-le dans le répertoire suivant : /etc/ksc-web-console-setup.json.

   Exemple de fichier de réponse qui contient l'ensemble minimum de paramètres et l'adresse et le port par défaut :

   ```
   {
     "address": "127.0.0.1",
     "port": 8080,
     "trusted":
   "127.0.0.1|13299|/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer|KSC
   Server",
     "acceptEula": true
   }
   ```

   Nous vous recommandons d'indiquer les numéros de port supérieurs à 1024. Si vous souhaitez que Kaspersky Security Center Web Console fonctionne sur les ports inférieurs à 1024, après l'installation, vous devez exécuter la commande suivante :

   ```
   sudo setcap 'cap_net_bind_service=+ep' /var/opt/kaspersky/ksc-web-console/node
   ```

   Lorsque 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.

   Kaspersky Security Center Web Console ne peut être mise à jour par le même fichier d'installation .rpm. Si vous voulez modifier les paramètres d'un fichier de réponses et utiliser ce fichier pour réinstaller l'application, vous devez d'abord supprimer l'application, puis la réinstaller avec le nouveau fichier de réponses.

4. Dans un compte avec les privilèges racine, utilisez la ligne de commande pour exécuter le fichier de paramétrage avec l'extension .deb ou .rpm, selon votre distribution Linux.

   - Pour installer ou mettre à niveau Kaspersky Security Center Web Console à partir d'un fichier .deb, exécutez la commande suivante :
     ```
     $ sudo dpkg -i ksc-web-console-[build_number].x86_64.deb
     ```
   - Pour installer Kaspersky Security Center Web Console à partir d'un fichier .rpm, exécutez la commande suivante :
     ```
     $ sudo rpm -ivh --nodeps ksc-web-console-[build_number].x86_64.rpm
     ```
     ou
     ```
     $ sudo alien -i ksc-web-console-[build_number].x86_64.rpm
     ```

- Pour effectuer une mise à niveau à partir d'une version précédente de Kaspersky Security Center Web Console, exécutez une des commandes suivantes :

  - Pour les appareils exécutant un système d'exploitation basé sur RPM :
    ```
    $ sudo rpm -Uvh --nodeps --force ksc-web-console-[build_number].x86_64.rpm
    ```

  - Pour les appareils exécutant un système d'exploitation basé sur Debian :
    ```
    $ sudo dpkg -i ksc-web-console-[build_number].x86_64.deb
    ```

  Cette action lance la décompression du fichier d'installation. Veuillez patienter jusqu'à la fin de l'installation. Kaspersky Security Center Web Console est installée dans le répertoire suivant : /var/opt/kaspersky/ksc-web-console.

5. Redémarrez tous les services de Kaspersky Security Center Web Console en exécutant la commande suivante :
   ```
   $ sudo systemctl restart KSC*
   ```

Quand l'installation est terminée, vous pouvez utiliser un navigateur pour ouvrir et vous connecter à Kaspersky Security Center Web Console.

Paramètres d'installation de Kaspersky Security Center Web Console

Pour installer Kaspersky Security Center Web Console Server sur des appareils qui fonctionnent sous Linux, vous devez créer un fichier de réponse un fichier .json qui contient les paramètres pour connecter Kaspersky Security Center Web Console au Serveur d'administration.

Voici un exemple de fichier de réponse qui contient l'ensemble minimum de paramètres et l'adresse et le port par défaut :

```
{
  "address": "127.0.0.1",
  "port": 8080,
  "defaultLangId": 1049,
  "enableLog": false,
  "trusted": "127.0.0.1|13299|/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer|KSC
Server",
  "acceptEula": true,
  "certPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer",
  "webConsoleAccount": "Group1:User1",
  "managementServiceAccount": "Group1:User2",
  "serviceWebConsoleAccount": "Group1:User3",
  "pluginAccount": "Group1:User4",
  "messageQueueAccount": "Group1:User5"
}
```

Nous vous recommandons d'indiquer les numéros de port supérieurs à 1024. Si vous souhaitez que Kaspersky Security Center Web Console fonctionne sur les ports inférieurs à 1024, après l'installation, vous devez exécuter la commande suivante :

```
sudo setcap 'cap_net_bind_service=+ep' /var/opt/kaspersky/ksc-web-console/node
```

Lorsque 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 décrit les paramètres qui peuvent être spécifiés dans un fichier de réponse.

Paramètres d'installation de Kaspersky Security Center Web Console sur les appareils qui fonctionnent sous Linux

Paramètre	Description	Valeurs possibles
`address`	Adresse de Kaspersky Security Center Web Console Server (requis).	Valeur de chaîne.
`port`	Nombre de port utilisé par Kaspersky Security Center Web Console pour se connecter au Serveur d'administration (requis).	Valeur numérique.
`defaultLangId`	Langue de l'interface utilisateur (par défaut, `1033`).	Code numérique de la langue : • Allemand : `1031` • Anglais : `1033` • Espagnol : `3082` • Espagnol (Mexique) : `2058` • Français : `1036` • Japonais : `1041` • Kazakh : `1087` • Polonais : `1045` • Portugais (Brésil) : `1046` • Russe : `1049` • Turc : `1055` • Chinois simplifié : `4` • Chinois traditionnel : `31748` Si aucune valeur n'est spécifiée, c'est l'anglais en-US qui est utilisé.
`enableLog`	Pour activer ou pas le journal d'activité de Kaspersky Security Center Web Console.	Valeur booléenne : • `true` : le journal est activé (sélectionné par défaut). • `false` : le journal est désactivé.
`trusted`	Liste des Serveurs d'administration autorisés pour connecter Kaspersky Security Center Web Console. Chaque Serveur d'administration doit être défini avec les paramètres suivants : • Adresse du Serveur d'administration • Le port OpenAPI qui est utilisé par Kaspersky Security Center Web Console pour la connexion au serveur d'administration (par défaut, 13299) • Chemin vers le certificat du Serveur d'administration • Le nom du Serveur d'administration qui s'affiche dans la fenêtre de connexion	Valeur de chaîne au format suivant : `" adresse du serveur | port | chemin de certificat | nom du serveur "`. Exemple : `"X.X.X.X|13299|/cert/server-1.cer| Server 1 ||Y.Y.Y.Y|13299|/cert/server-2.cer| Server 2 "`.

	Les paramètres sont séparés par des barres verticales. Si plusieurs serveurs d'administration sont indiqués, séparez-les par deux barres verticales.	
`acceptEula`	Si vous acceptez ou pas les termes de l'Contrat de licence utilisateur final (CLUF). Le fichier des conditions du CLUF est téléchargé avec le fichier d'installation.	Valeur booléenne : • `vrai` : 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. • `false` : je n'accepte pas les conditions du Contrat de licence (sélectionné par défaut). Si aucune valeur n'est indiquée, le programme d'installation de Kaspersky Security Center Web Console affiche le CLUF et vous demande si vous acceptez ou non les conditions du CLUF.
`certDomain`	Si vous voulez générer un nouveau certificat, utilisez ce paramètre pour spécifier le nom de domaine pour lequel il faut générer un nouveau certificat.	Valeur de chaîne.
`certPath`	Si vous voulez utiliser un certificat existant, utilisez ce paramètre pour spécifier le chemin vers le fichier de certificat.	Valeur de chaîne. Spécifiez le chemin `"/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"` pour utiliser le certificat existant. Pour un certificat personnalisé, spécifiez le chemin où ce certificat personnalisé est stocké.
`keyPath`	Si vous voulez utiliser un certificat existant, utilisez ce paramètre pour spécifier le chemin vers le fichier clé.	Valeur de chaîne.
`webConsoleAccount`	Nom du compte à partir duquel le service Kaspersky Security Center Web Console est exécuté.	Valeur de chaîne au format suivant : `" group name : user name "`. Exemple : `" Group1 : User1 "`. Si aucune valeur n'est indiquée, le programme d'installation de Kaspersky Security Center Web Console crée un nouveau compte avec le nom par défaut `user_management_%uid%`.
`managementServiceAccount`	Nom du compte privilégié à partir duquel le service d'administration de Kaspersky Security Center Web Console est exécuté.	Valeur de chaîne au format suivant : `" group name : user name "`. Exemple : `" Group1 : User1 "`. Si aucune valeur n'est indiquée, le programme d'installation de Kaspersky Security Center Web Console crée un nouveau compte avec le nom par défaut `user_nodejs_%uid%`.
`serviceWebConsoleAccount`	Nom du compte à partir duquel le service Kaspersky Security Center Web Console est exécuté.	Valeur de chaîne au format suivant : `" group name : user name "`. Exemple : `" Group1 : User1 "`. Si aucune valeur n'est indiquée, le programme d'installation de Kaspersky Security Center Web Console crée un nouveau compte avec le nom par défaut `user_svc_nodejs_%uid%`.
`pluginAccount`	Nom du compte à partir duquel le service Plug-ins des produits de Kaspersky Security Center est exécuté.	Valeur de chaîne au format suivant : `" group name : user name "`. Exemple : `" Group1 : User1 "`. Si aucune valeur n'est indiquée, le programme d'installation de Kaspersky Security Center Web Console crée un nouveau compte avec le nom par défaut `user_web_plugin_%uid%`.
`messageQueueAccount`	Nom du compte à partir duquel le service File d'attente des messages de Kaspersky Security Center Web Console est exécuté.	Valeur de chaîne au format suivant : `" group name : user name "`. Exemple : `" Group1 : User1 "`. Si aucune valeur n'est indiquée, le programme d'installation de Kaspersky Security Center Web Console crée un nouveau compte avec le nom par défaut `user_message_queue_%uid%`.

Si vous spécifiez les paramètres `webConsoleAccount`, `managementServiceAccount`, `serviceWebConsoleAccount`, `pluginAccount` ou `messageQueueAccount`, assurez-vous que les comptes utilisateurs personnalisés appartiennent au même groupe de sécurité. Si ces paramètres ne sont pas spécifiés, le programme d'installation de Kaspersky Security Center Web Console crée un groupe de sécurité par défaut, puis crée des comptes utilisateurs avec des noms par défaut dans ce groupe.

Installation de Kaspersky Security Center Web Console sur Astra Linux à l'aide de l'environnement logiciel fermé

Cette section décrit comment installer le Serveur de Kaspersky Security Center Web Console (également appelé Kaspersky Security Center Web Console) sur le système d'exploitation Astra Linux Special Edition. Avant de lancer l'installation, vous devez installer un SGBD et le Serveur d'administration de Kaspersky Security Center Linux.

Installation de Kaspersky Security Center Web Console :

1. Assurez-vous que l'appareil sur lequel vous voulez installer Kaspersky Security Center Web Console fonctionne sur une des distributions Linux supportées.

2. Lisez le Contrat de licence utilisateur final (CLUF). Si le kit de distribution Kaspersky Security Center Linux ne contient pas de fichier TXT avec le texte du CLUF, vous pouvez télécharger le fichier depuis le site de Kaspersky. Si vous refusez les dispositions du Contrat de licence, n'installez pas l'application.

3. Créez un fichier de réponse qui contient les paramètres pour connecter Kaspersky Security Center Web Console au serveur d'administration. Nommez ce fichier ksc-web-console-setup.json et placez-le dans le répertoire suivant : /etc/ksc-web-console-setup.json.

   Exemple de fichier de réponse qui contient l'ensemble minimum de paramètres et l'adresse et le port par défaut :

   ```
   {
     "address": "127.0.0.1",
     "port": 8080,
     "trusted":
   "127.0.0.1|13299|/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer|KSC
   Server",
     "acceptEula": true
   }
   ```

4. Ouvrez le fichier `/etc/digsig/digsig_initramfs.conf`, puis définissez le paramètre suivant :

   ```
   DIGSIG_ELF_MODE=1
   ```

5. Dans la ligne de commande, exécutez la commande suivante pour installer le paquet de compatibilité :

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

6. Créez un répertoire pour la clé de l'application :

   ```
   mkdir -p /etc/digsig/keys/legacy/kaspersky/
   ```

7. Placez la clé de l'application `/opt/kaspersky/ksc64/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 Kaspersky Security Center Linux 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.

8. Mettez à jour les disques RAM :

   ```
   update-initramfs -u -k all
   ```

   Redémarrez le système.

9. Sous un compte avec les privilèges root, utilisez la ligne de commande pour exécuter le fichier d'installation. Vous récupérez le fichier d'installation en le téléchargeant du site de Kaspersky.

   - Pour installer ou mettre à jour Kaspersky Security Center Web Console, exécutez la commande suivante :

     ```
     $ sudo dpkg -i ksc-web-console-[build_number].x86_64.deb
     ```

   - Pour effectuer une mise à niveau à partir d'une version précédente de Kaspersky Security Center Web Console, exécutez la commande suivante :

     ```
     $ sudo dpkg -i ksc-web-console-[build_number].x86_64.deb
     ```

   Cette action lance la décompression du fichier d'installation. Veuillez patienter jusqu'à la fin de l'installation. Kaspersky Security Center Web Console est installée dans le répertoire suivant : `/var/opt/kaspersky/ksc-web-console`.

10. Redémarrez tous les services de Kaspersky Security Center Web Console en exécutant la commande suivante :

    ```
    $ sudo systemctl restart KSC*
    ```

Quand l'installation est terminée, vous pouvez utiliser un navigateur pour ouvrir et vous connecter à Kaspersky Security Center Web Console.

Si votre appareil fonctionne sous Astra Linux 1.8, vous devez modifier les privilèges de l'utilisateur après l'installation de Kaspersky Security Center Web Console.

Nous vous recommandons d'effectuer les étapes de l'instruction pour chaque service séparément.

Pour ignorer les privilèges de l'utilisateur, procédez comme suit :

1. Ouvrez les fichiers suivants :

   - /etc/systemd/system/ KSCSvcWebConsole.service
   - /etc/systemd/system/ KSCWebConsole.service
   - /etc/systemd/system/ KSCWebConsoleManagement.service
   - /etc/systemd/system/ KSCWebConsoleMessageQueue.service
   - /etc/systemd/system/ KSCWebConsolePlugin.service

2. Copiez la chaîne `User= value` depuis les fichiers.

   Les valeurs sont différentes pour chaque service et sont générées lors de l'installation de Kaspersky Security Center Web Console.

3. Créez les répertoires suivants :

- /etc/systemd/system/ KSCSvcWebConsole.service.d
- /etc/systemd/system/ KSCWebConsole.service.d
- /etc/systemd/system/ KSCWebConsoleManagement.service.d
- /etc/systemd/system/ KSCWebConsoleMessageQueue.service.d
- /etc/systemd/system/ KSCWebConsolePlugin.service.d

4. Dans chaque répertoire, créez un fichier nommé `override.conf`, puis insérez la chaîne que vous avez copiée à l'étape 2 dans le fichier. Le fichier `override.conf` doit présenter le contenu suivant :

   - for **/etc/systemd/system/ KSCSvcWebConsole.service.d**

     ```
     [Service]

     User=

     User= value

     CapabilitiesParsec=PARSEC_CAP_PRIV_SOCK

     ExecStart=

     ExecStart=/usr/bin/env /var/opt/kaspersky/ksc-web-console/node
     /var/opt/kaspersky/ksc-web-console/pm.service-console.js
     ```

   - for **/etc/systemd/system/ KSCWebConsole.service.d**

     ```
     [Service]

     User=

     User= value

     CapabilitiesParsec=PARSEC_CAP_PRIV_SOCK

     ExecStart=

     ExecStart=/usr/bin/env /var/opt/kaspersky/ksc-web-console/node
     /var/opt/kaspersky/ksc-web-console/pm.js
     ```

   - for **/etc/systemd/system/ KSCWebConsoleManagement.service.d**

```
[Service]

User=

User= value

CapabilitiesParsec=PARSEC_CAP_PRIV_SOCK

ExecStart=

ExecStart=/usr/bin/env /var/opt/kaspersky/ksc-web-console/node
/var/opt/kaspersky/ksc-web-console/pm.updates-manager.js
```

- for /etc/systemd/system/ KSCWebConsoleMessageQueue.service.d

```
[Service]

User=

User= value

CapabilitiesParsec=PARSEC_CAP_PRIV_SOCK

ExecStart=

ExecStart=/usr/bin/env /var/opt/kaspersky/ksc-web-console/vendor/nsqd -tls-
cert=../nsq-server.crt -tls-key=../nsq-server.key -tls-required=1 -tls-min-
version=tls1.2 -tls-root-ca-file=../KLRootCA.crt -max-msg-size=10485760 -mem-
queue-size=100 -sync-every=0 -sync-timeout=24h -http-address=127.0.0.1:4151 -
https-address=127.0.0.1:4152 -tcp-address=127.0.0.1:4150 -tls-client-auth-
policy=require-verify
```

- for /etc/systemd/system/ KSCWebConsolePlugin.service.d

```
[Service]

User=

User= value

CapabilitiesParsec=PARSEC_CAP_PRIV_SOCK

ExecStart=

ExecStart=/usr/bin/env /var/opt/kaspersky/ksc-web-console/node
/var/opt/kaspersky/ksc-web-console/pm.plugin.js
```

où `User= value` est la chaîne que vous avez copiée à l'étape 2. Par exemple, `User=user_svc_nodejs_rjvyyf-xkg`.

5. Redémarrez le service.

Installation de Kaspersky Security Center Web Console connecté au Serveur d'administration installé sur les nœuds du cluster de basculement Kaspersky Security Center Linux

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 Linux. Avant d'installer Kaspersky Security Center Web Console, installez un SGBD et le Serveur d'administration Kaspersky Security Center Linux sur les nœuds du cluster de basculement Kaspersky Security Center Linux.

Pour installer Kaspersky Security Center Web Console connecté au Serveur d'administration installé sur les nœuds du cluster de basculement Kaspersky Security Center Linux :

1. Effectuez les étapes 1 et 2 de l'installation de Kaspersky Security Center Web Console.

2. À l'étape 3, dans le fichier de réponses, indiquez le paramètre d'installation `de confiance` pour permettre au cluster de basculement Kaspersky Security Center Linux de se connecter à Kaspersky Security Center Web Console. La valeur de chaîne de ce paramètre a le format suivant :
   `"trusted": "server address|port|certificate path|server name"`

   Spécifiez les modules du paramètre d'installation de `trusted` :

   - **Adresse du Serveur d'administration**. Si vous avez créé la carte réseau virtuelle lors de la préparation des nœuds du cluster, utilisez l'adresse IP de la carte comme adresse du cluster de basculement Kaspersky Security Center Linux. Dans le cas contraire, indiquez l'adresse IP du répartiteur de charge tiers que vous utilisez.

   - **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 Linux. Chemin d'accès par défaut au fichier du certificat est : <shared data folder>\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.

   - **Nom du Serveur d'administration**. Nom du cluster de basculement Kaspersky Security Center Linux qui s'affichera dans la fenêtre de connexion de Kaspersky Security Center Web Console.

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.

Vous pouvez accéder à **Découverte et déploiement** → **Appareils non définis** pour consulter les informations sur les nœuds du cluster et le serveur de fichiers.

Déploiement du cluster de basculement Kaspersky Security Center Linux

Cette section contient à la fois des informations générales à propos du cluster de basculement Kaspersky Security Center Linux, et des instructions à propos de la préparation et du déploiement du cluster de basculement Kaspersky Security Center Linux sur votre réseau.

Scénario : Déploiement du cluster de basculement Kaspersky Security Center Linux

Un cluster de basculement Kaspersky Security Center Linux assure la haute disponibilité de Kaspersky Security Center Linux 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 Linux 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.

Le déploiement des applications Kaspersky se déroule par étapes :

1. **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 Linux. Assurez-vous que le serveur de fichiers répond aux exigences matérielles et logicielles, créez deux dossiers partagés pour les données de Kaspersky Security Center Linux 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 Linux

2. **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 Linux

3. **Création des comptes pour les services Kaspersky Security Center Linux**

   Exécutez les étapes suivantes sur le nœud actif, le nœud passif et le serveur de fichiers :

   1. Créez un groupe portant le nom " kladmins " et attribuez le même GID aux trois groupes.
   2. Créez un compte utilisateur portant le nom " ksc " et attribuez le même UID aux trois comptes utilisateur. Définissez le groupe principal sur 'kladmins' pour les comptes créés.
   3. Créez un compte utilisateur avec le nom " rightless " et attribuez le même UID aux trois comptes utilisateur. Définissez le groupe principal sur 'kladmins' pour les comptes créés.

4. **Installation du Système de gestion de base de données (SGBD)**

   Vous avez deux options :

   - Si vous souhaitez utiliser MariaDB Galera Cluster, vous n'avez pas besoin d'un appareil dédié au SGBD. Installez MariaDB Galera Cluster sur chacun des nœuds.
   - Si vous souhaitez utiliser un autre SGBD pris en charge, installez le SGBD sélectionné sur un appareil dédié.

5. **Installation de Kaspersky Security Center Linux**

Installez Kaspersky Security Center Linux en mode cluster de basculement sur les deux nœuds. Vous devez d'abord installer Kaspersky Security Center Linux sur le nœud actif, puis l'installer sur le nœud passif.

De plus, vous pouvez installer Kaspersky Security Center Web Console sur un appareil distinct qui n'est pas un nœud de cluster.

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 Linux 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 Linux est déployé. Veuillez prendre connaissance des événements qui conduisent au basculement entre les nœuds actifs et passifs.

À propos du cluster de basculement Kaspersky Security Center Linux

Un cluster de basculement Kaspersky Security Center Linux assure la haute disponibilité de Kaspersky Security Center Linux 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 Linux 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.

Dans un cluster de basculement de Kaspersky Security Center Linux, tous les services de Kaspersky Security Center Linux sont administrés automatiquement. N'essayez pas de redémarrer les services manuellement.

Configurations logicielle et matérielle

Pour déployer un cluster de basculement Kaspersky Security Center Linux, vous devez disposer du matériel suivant :

- Deux appareils présentant des caractéristiques matérielles et logicielles identiques. Ces appareils agiront en tant que nœuds actifs et passifs.
- Un serveur de fichiers sous Linux, avec le système de fichiers EXT4. Vous devez fournir un appareil dédié qui fera office de serveur de fichiers.

  Assurez-vous d'avoir fourni une bande passante réseau élevée entre le serveur de fichiers et les nœuds actifs et passifs.

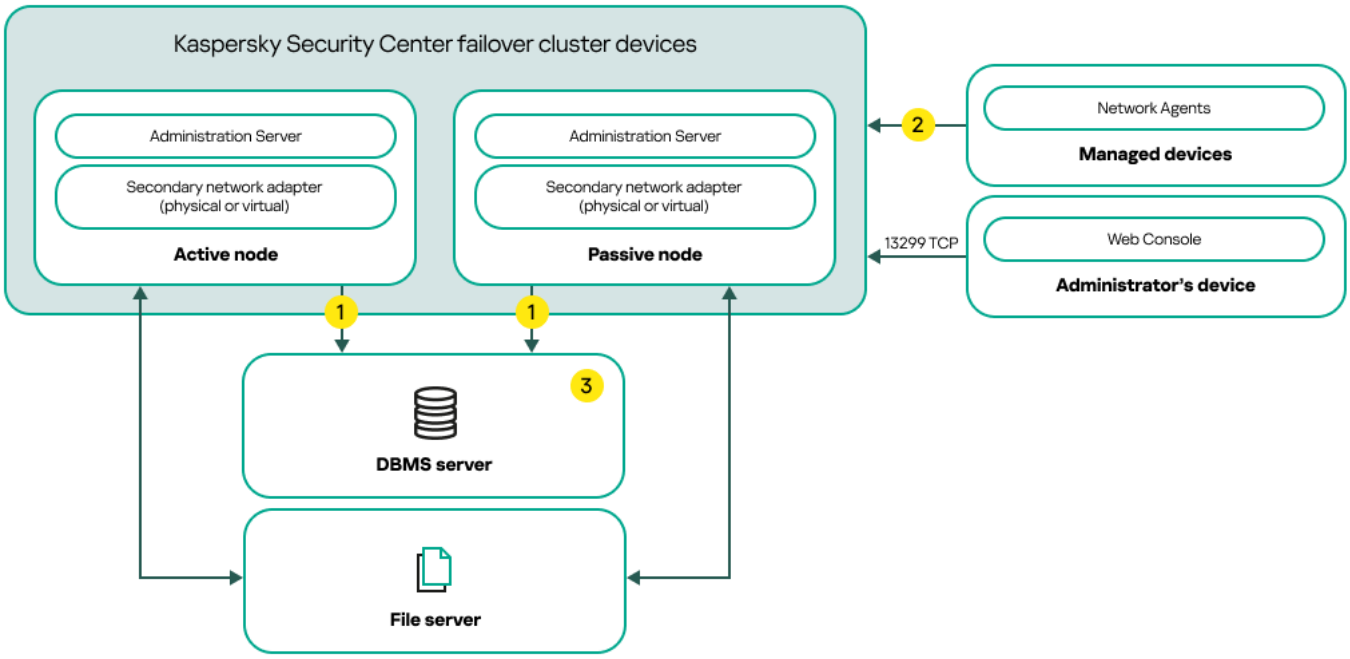
- Un appareil avec un Système de gestion de base de données (SGBD) pris en charge. Si vous utilisez MariaDB Galera Cluster comme SGBD, un appareil dédié à cet effet n'est pas nécessaire.

Le déploiement du cluster de basculement échoue lorsque vous avez installé à la fois les paquets arping et iputils-arping ou uniquement le paquet arping. Avant de déployer un cluster de basculement, assurez-vous que seul le paquet iputils-arping est installé sur les deux nœuds.

Schémas de déploiement

Vous pouvez choisir l'un des schémas suivants pour déployer le cluster de basculement Kaspersky Security Center Linux :

- Un schéma qui utilise une carte réseau secondaire.
- Un schéma qui utilise un équilibreur de charge tiers.



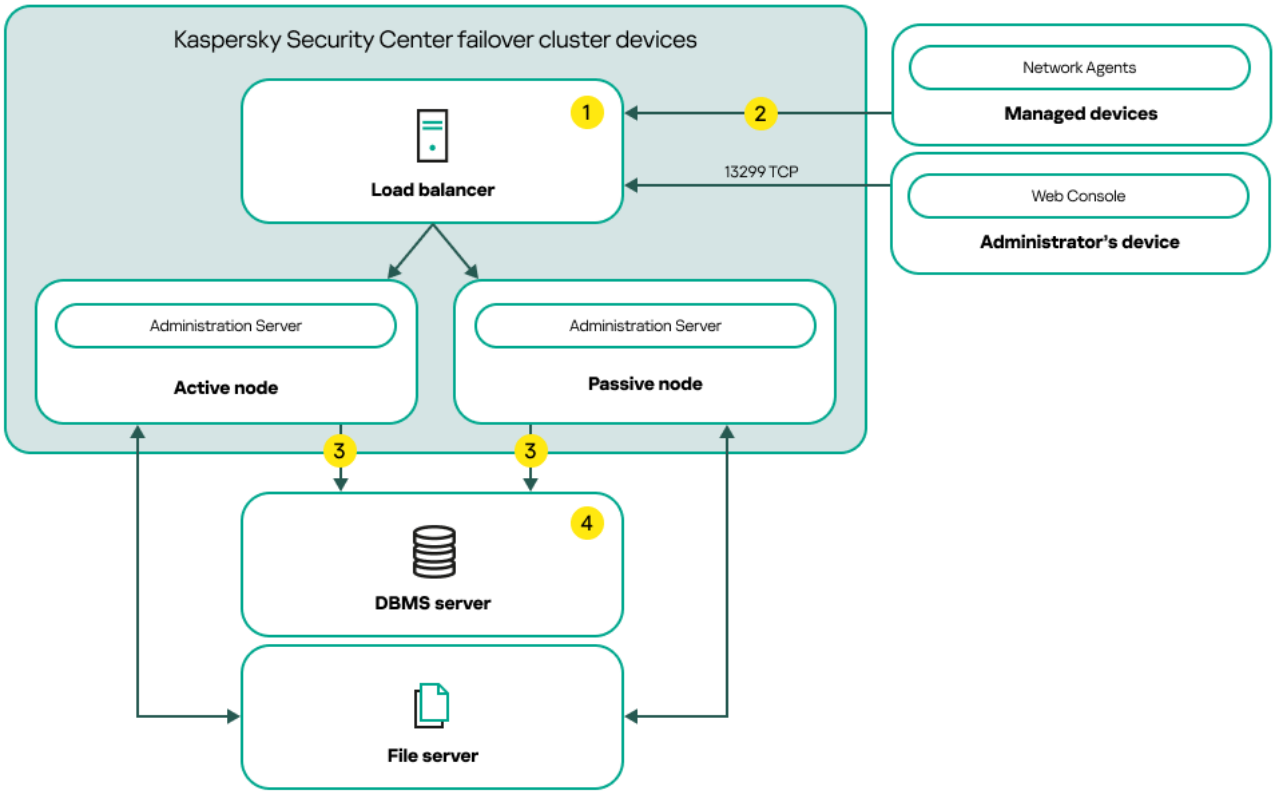
Un schéma qui utilise une carte réseau secondaire.

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 5432 pour PostgreSQL ou Postgres Pro. 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.

3 Un appareil avec le Système de gestion de base de données (SGBD). Si vous utilisez MariaDB Galera Cluster comme SGBD, un appareil dédié à cet effet n'est pas nécessaire. Installez MariaDB Galera Cluster sur chacun des nœuds.



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 5432 pour PostgreSQL ou Postgres Pro. Veuillez vous référer à la documentation du SGBD pour les informations pertinentes.

4 Un appareil avec le Système de gestion de base de données (SGBD). Si vous utilisez MariaDB Galera Cluster comme SGBD, un appareil dédié à cet effet n'est pas nécessaire. Installez MariaDB Galera Cluster sur chacun des nœuds.

Conditions de basculement

Le cluster de basculement bascule l'administration de la protection des équipements clients du nœud actif vers le 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 Linux a échoué ou a été délibérément interrompu par l'utilisateur. Les services de Kaspersky Security Center Linux 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.

Préparation d'un serveur de fichiers pour un cluster de basculement Kaspersky Security Center Linux

Un serveur de fichiers fonctionne comme un module obligatoire d'un cluster de basculement Kaspersky Security Center Linux.

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. Installez et configurez un serveur NFS :
   - L'accès au serveur de fichiers doit être activé pour les deux nœuds dans les paramètres du serveur NFS.
   - Le protocole NFS doit avoir la version 4.0 ou 4.1.
   - Configuration minimale requise pour le noyau Linux :
     - 3.19.0-25, si vous utilisez NFS 4.0
     - 4.4.0-176, si vous utilisez NFS 4.1
3. Sur le serveur de fichiers, créez deux dossiers et partagez-les à l'aide de NFS. 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 Linux. Vous indiquerez les chemins d'accès aux dossiers partagés lors de la configuration de l'installation de Kaspersky Security Center Linux.

   En fonction de votre distribution Linux, installez soit le paquet nfs-utils, soit le paquet nfs-kernel-server à l'aide de la commande correspondante :

   ```
   sudo yum install nfs-utils
   sudo apt install nfs-kernel-server
   ```

   Exécutez les commande suivantes :

   ```
   sudo mkdir -p /mnt/KlFocStateShare
   sudo mkdir -p /mnt/KlFocDataShare_klfoc
   sudo chown ksc:kladmins /mnt/KlFocStateShare
   sudo chown ksc:kladmins /mnt/KlFocDataShare_klfoc
   sudo chmod -R 777 /mnt/KlFocStateShare /mnt/KlFocDataShare_klfoc
   sudo sh -c "echo /mnt/KlFocStateShare *\(rw,sync,no_subtree_check,no_root_squash\) >>
   /etc/exports"
   sudo sh -c "echo /mnt/KlFocDataShare_klfoc *\
   (rw,sync,no_subtree_check,no_root_squash\) >> /etc/exports"
   sudo exportfs -a
   sudo systemctl start rpcbind
   sudo service nfs start
   ```

   Activez le démarrage automatique en exécutant la commande suivante :

   ```
   sudo systemctl enable rpcbind
   ```

4. Redémarrez le serveur de fichiers.

Le serveur de fichiers est préparé. Pour déployer le cluster de basculement Kaspersky Security Center Linux, suivez les instructions supplémentaires de ce scénario.

Préparation des nœuds pour un cluster de basculement Kaspersky Security Center Linux

Préparez deux appareils qui fonctionneront en tant que nœuds actifs et passifs d'un cluster de basculement Kaspersky Security Center Linux.

Pour préparer des nœuds pour un cluster de basculement Kaspersky Security Center Linux, 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. En fonction de votre distribution Linux, installez soit le paquet nfs-utils, soit le paquet nfs-kernel-server sur chaque nœud à l'aide de la commande correspondante :
   ```
   sudo yum install nfs-utils
   sudo apt install nfs-kernel-server
   ```

3. Créez des points de montage en exécutant les commandes suivantes :
   ```
   sudo mkdir -p /mnt/KlFocStateShare
   sudo mkdir -p /mnt/KlFocDataShare_klfoc
   ```

4. Faites correspondre les points de montage et les dossiers partagés :
   ```
   sudo sh -c "echo {server}:{chemin d'accès au dossier KlFocStateShare}
   /mnt/KlFocStateShare nfs vers=4,soft,timeo=50,retrans=2,auto,user,rw 0 0 >>
   /etc/fstab"
   sudo sh -c "echo {serveur}:{chemin d'accès au dossier KlFocDataShare_klfoc}
   /mnt/KlFocDataShare_klfoc nfs vers=4,noauto,user,rw,exec 0 0 >> /etc/fstab"
   ```
   Ici, `{serveur}:{chemin d'accès au dossier KlFocStateShare}` et `{serveur}:{chemin d'accès au dossier KlFocDataShare_klfoc}` sont les chemins d'accès réseau aux dossiers partagés sur le serveur de fichiers.

5. Montez les dossiers partagés en exécutant les commandes suivantes :
   ```
   monter /mnt/KlFocStateShare
   monter /mnt/KlFocDataShare_klfoc
   ```

6. Assurez-vous que les autorisations d'accès aux dossiers partagés appartiennent à ksc:kladmins.

   Exécutez la commande suivante :
   ```
   sudo ls -la /mnt/
   ```

7. 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.

   Exécutez une des actions suivantes :

   - Utilisez une carte réseau virtuelle.

     a. Utilisez la commande suivante pour vérifier que NetworkManager est utilisé pour administrer l'adaptateur physique :
        ```
        nmcli device status
        ```

Si la carte physique apparaît comme non administrée dans la sortie, configurez NetworkManager pour gérer la carte physique. Les étapes de configuration exactes dépendent de votre distribution.

b. Utilisez la commande suivante pour identifier les interfaces :

```
ip a
```

c. Créez un profil de configuration :

```
nmcli connection add type macvlan dev <interface physique> mode bridge
ifname <interface virtuelle> ipv4.addresses <masque d'adresse> ipv4.method
manual autoconnect no
```

- Utilisez une carte réseau physique ou un hyperviseur. Dans ce scénario, désactivez le logiciel NetworkManager.

a. Supprimez les connexions NetworkManager pour l'interface cible :

```
nmcli con del <nom de la connexion>
```

Utilisez la commande suivante pour vérifier si l'interface cible dispose de connexions :

```
nmcli con show
```

b. Modifiez le fichier NetworkManager.conf. Recherchez la section keyfile et affectez l'interface cible au paramètre unmanaged-devices.

```
[keyfile]
unmanaged-devices=interface-name:<nom de l'interface>
```

c. Redémarrez NetworkManager :

```
systemctl reload NetworkManager
```

Utilisez la commande suivante pour vérifier que l'interface cible n'est pas administrée :

```
nmcli dev status
```

- 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.

Les nœuds sont préparés. Pour déployer le cluster de basculement Kaspersky Security Center Linux, suivez les instructions supplémentaires du scénario.

Installation de Kaspersky Security Center Linux sur les nœuds du cluster de basculement Kaspersky Security Center Linux

Cette procédure décrit l'installation de Kaspersky Security Center Linux sur les nœuds du cluster de basculement de Kaspersky Security Center Linux. Kaspersky Security Center Linux est installé séparément sur les deux nœuds du cluster de basculement Kaspersky Security Center Linux. 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.

Utiliser le fichier d'installation ksc64_[numéro_version]_amd64.deb ou ksc64-[numéro_version].x86_64.rpm correspondant à la distribution Linux installée sur votre appareil. Vous récupérez le fichier d'installation en le téléchargeant du site Web de Kaspersky.

Installation sur le nœud primaire (actif)

Pour installer Kaspersky Security Center Linux sur le nœud primaire :

1. Assurez-vous que l'appareil sur lequel vous voulez installer Kaspersky Security Center Linux fonctionne sur une des distributions Linux supportées.

2. Dans la ligne de commande, exécutez les commandes fournies dans cette instruction.

3. Exécuter le fichier d'installation de Kaspersky Security Center Linux. En fonction de votre distribution Linux, exécutez l'une des commandes suivantes :

   - `sudo apt install /<path>/ksc64_[ version_number ]_amd64.deb`
   - `sudo yum install /<path>/ksc64-[ version_number ].x86_64.rpm -y`

4. Exécuter le fichier de configuration de Kaspersky Security Center Linux.

   ```
   sudo /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
   ```

5. Lisez le Contrat de licence utilisateur final (CLUF) et la Politique de confidentialité. 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 les valeurs suivantes :

   a. 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 Kaspersky Security Center Linux, vous devez accepter les conditions du Contrat de licence utilisateur final.

   b. Saisissez `y` si vous comprenez et acceptez les conditions de la Politique de confidentialité et que vous acceptez que vos données soient traitées et transmises (y compris vers des pays tiers) comme décrit dans celle-ci. Saisissez `n` si vous n'acceptez pas les conditions de la Politique de confidentialité. Pour utiliser Kaspersky Security Center Linux, vous devez accepter les conditions de la Politique de confidentialité.

6. Sélectionnez **Nœud de cluster primaire** comme mode d'installation du Serveur d'administration.

7. Lorsque vous y êtes invité, saisissez les paramètres suivants :

   a. Saisissez le chemin d'accès local au point de montage du partage d'état.

   b. Saisissez le chemin d'accès local au point de montage du partage de données.

   c. Choisissez un mode de connectivité de cluster de basculement : via une carte réseau secondaire ou un équilibreur de charge externe.

   d. Si vous utilisez une carte réseau secondaire, saisissez son nom.

e. Lorsque vous êtes invité à saisir le nom DNS ou l'adresse IP statique du Serveur d'administration, saisissez l'adresse IP de la carte réseau secondaire ou l'adresse IP de l'équilibreur de charge externe.

f. Entrez le numéro de port SSL du Serveur d'administration. Le numéro de port est de 13000 par défaut.

g. Estimez le nombre approximatif d'appareils que vous entendez administrer :

- Si votre réseau prend en charge entre 1 et 100 appareils, saisissez 1.
- Si votre réseau prend en charge entre 101 et 1 000 appareils, saisissez 2.
- Si votre réseau prend en charge plus de 1 000 appareils, saisissez 3.

h. Saisissez le nom du groupe de sécurité pour les services. Par défaut, le groupe kladmins est utilisé.

i. Saisissez le nom du compte pour lancer le service Serveur d'administration. Le compte doit faire partie du groupe de sécurité saisi. Par défaut, le compte "ksc" est utilisé.

j. Saisissez le nom du compte pour lancer d'autres services. Le compte doit faire partie du groupe de sécurité saisi. Par défaut, le compte "ksc" est utilisé.

k. Sélectionnez le SGBD que vous avez installé pour fonctionner avec Kaspersky Security Center Linux:

- Si vous avez installé MySQL ou MariaDB, saisissez 1.
- Si vous avez installé PostgreSQL ou Postgres Pro, saisissez 2.

l. Saisissez le nom DNS ou l'adresse IP de l'appareil sur lequel la base de données est installée.

m. Saisissez le numéro de port de la base de données. Ce port sert à communiquer avec le Serveur d'administration. Par défaut, les ports suivants sont utilisés :

- Port 3306 pour MySQL ou MariaDB
- Port 5432 pour PostgreSQL ou Postgres Pro

n. Saisissez le nom de la base de données.

o. Saisissez l'identifiant de connexion du compte racine de la base de données que vous utilisez pour accéder à la base de données.

p. Saisissez le mot de passe du compte racine de la base de données que vous utilisez pour accéder à la base de données.

8. Attendez que les services soient ajoutés et lancés automatiquement :

- klfocsvc_klfoc
- kladminserver_klfoc
- klwebsrv_klfoc
- klactprx_klfoc
- klnagent_klfoc

9. Créez un compte qui agira en tant qu'administrateur du Serveur d'administration. Saisissez le nom d'utilisateur et le mot de passe. Le mot de passe utilisateur ne doit pas comporter moins de 8 ni plus de 16 caractères.

L'utilisateur est ajouté et Kaspersky Security Center Linux est installé sur le nœud primaire.

Installation sur le nœud secondaire (passif)

Pour installer Kaspersky Security Center Linux sur le nœud secondaire :

1. Assurez-vous que l'appareil sur lequel vous voulez installer Kaspersky Security Center Linux fonctionne sur une des distributions Linux supportées.

2. Dans la ligne de commande, exécutez les commandes fournies dans cette instruction.

3. Exécuter le fichier d'installation de Kaspersky Security Center Linux. En fonction de votre distribution Linux, exécutez l'une des commandes suivantes :

   - `sudo apt install /<path>/ksc64_[ version_number ]_amd64.deb`
   - `sudo yum install /<path>/ksc64-[ version_number ].x86_64.rpm -y`

4. Exécuter le fichier de configuration de Kaspersky Security Center Linux.

   ```
   sudo /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
   ```

5. Lisez le Contrat de licence utilisateur final (CLUF) et la Politique de confidentialité. 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 les valeurs suivantes :

   a. 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 Kaspersky Security Center Linux, vous devez accepter les conditions du Contrat de licence utilisateur final.

   b. Saisissez `y` si vous comprenez et acceptez les conditions de la Politique de confidentialité et que vous acceptez que vos données soient traitées et transmises (y compris vers des pays tiers) comme décrit dans celle-ci. Saisissez `n` si vous n'acceptez pas les conditions de la Politique de confidentialité. Pour utiliser Kaspersky Security Center Linux, vous devez accepter les conditions de la Politique de confidentialité.

6. Sélectionnez **Nœud de cluster secondaire** comme mode d'installation du Serveur d'administration.

7. Lorsque vous y êtes invité, saisissez le chemin d'accès local au point de montage du partage d'état.

Kaspersky Security Center Linux est installé sur le nœud secondaire.

Vérification du service

Utilisez les commandes suivantes pour vérifier si un service est en cours d'exécution ou non :

- `systemctl status klnagent_srv.service`
- `systemctl status kladminserver_srv.service`
- `systemctl status klactprx_srv.service`

- `systemctl status klwebsrv_srv.service`

Maintenant, vous pouvez tester le cluster de basculement Kaspersky Security Center Linux 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 Linux 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 /opt/kaspersky/ksc64/sbin.
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 maintenir, accédez à /opt/kaspersky/ksc64/sbin.
3. Ouvrez la ligne de commande, puis détachez le nœud du cluster en exécutant la commande `detach_node.sh`.
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 été maintenu, accédez à /opt/kaspersky/ksc64/sbin.
8. Ouvrez la ligne de commande, puis attachez le nœud au cluster en exécutant la commande `attach_node.sh`.
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.

Comptes pour travailler avec le SGBD

Pour installer le Serveur d'administration et l'utiliser, vous avez besoin d'un compte SGBD interne. Ce compte permet d'accéder au SGBD et requiert des privilèges spécifiques. Un ensemble de droits requis dépend des critères suivants :

- Type de SGBD :
  - MySQL ou MariaDB
  - PostgreSQL ou Postgres Pro
- 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 de Serveur d'administration (ci-après également appelée base de données du Serveur) à l'aide du programme d'installation du Serveur d'administration (le programme d'installation).
  - **Manuel**. Vous pouvez utiliser une application tierce 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 SGBD que vous devez accorder aux comptes avant d'installer et de démarrer le Serveur d'administration.

MySQL et MariaDB

Si vous choisissez MySQL ou MariaDB comme SGBD, créez un compte utilisateur interne du SGBD pour accéder au SGBD, puis accordez à ce compte les privilèges requis. Notez que la méthode de création de la base de données n'affecte pas l'ensemble des privilèges. Les droits requis sont énumérés ci-dessous :

- 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 plus d'informations sur la configuration des privilèges du compte, consultez Configuration du compte SGBD pour l'utilisation avec 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.

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 SGBD pour l'utilisation avec PostgreSQL ou Postgres Pro.

Privilèges du rôle Postgres

Création automatique de la base de données		Création manuelle de la base de données
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, le rôle Postgres utilisé pour accéder au SGBD doit avoir les droits de propriétaire sur la base de données du Serveur d'administration.

Configuration du compte SGBD pour travailler avec MySQL et MariaDB

Prérequis

Avant d'attribuer des droits au compte SGBD, effectuez 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.

Configurer le compte SGBD pour installer le Serveur d'administration

Pour configurer le compte SGBD pour l'installation du Serveur d'administration :

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.

   Pour créer un compte SGBD avec un mot de passe, exécutez la commande suivante :

```
/* Créez un utilisateur nommé KSCAdmin et spécifiez le mot de passe pour KSCAdmin */
CREATE USER 'KSCAdmin' IDENTIFIED BY '<password>';
```

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 '<password>';
  ```

- Pour modifier l'authentification d'un compte SGBD existant, exécutez la commande suivante :

  ```
  ALTER USER 'KSCAdmin'@'%' IDENTIFIED WITH mysql_native_password BY '<password>';
  ```

3. Accordez les privilèges suivants au compte SGBD créé :

   - 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 accorder les privilèges requis au compte SGBD créé, exécutez le script suivant :

   ```
   /* 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'`.

4. Pour afficher la liste des privilèges accordés au compte SGBD, exécutez la commande suivante :

   ```
   SHOW grants for 'KSCAdmin';
   ```

5. 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.

6. Installez le 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.

Configuration des comptes SGBD pour l'utilisation avec PostgreSQL et Postgres Pro

Prérequis

Avant d'attribuer des droits au compte SGBD, effectuez 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.

Configuration des comptes SGBD pour installer le Serveur d'administration (création automatique de la base de données du Serveur d'administration)

Pour configurer le compte SGBD pour l'installation du Serveur d'administration :

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.

     Par défaut, l'utilisateur *Postgres* n'a pas de mot de passe. Cependant, le mot de passe est nécessaire pour installer Kaspersky Security Center Linux. Pour définir le mot de passe de l'utilisateur *Postgres*, exécutez le script suivant :

     ```
     ALTER USER "user_name" WITH PASSWORD '<password>';
     ```

   - 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. Installez le 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 SGBD pour installer le Serveur d'administration (création manuelle de la base de données du Serveur d'administration).

Pour configurer le compte SGBD pour l'installation du Serveur d'administration :

1. Exécutez un environnement pour l'utilisation avec Postgres.

2. Créez un rôle Postgres et une base de données du Serveur d'administration. Ensuite, accordez tous les privilèges au rôle dans la base de données du Serveur d'administration. Pour ce faire, connectez-vous sous l'utilisateur *Postgres* dans la base de données *Postgres* et exécutez le script suivant (dans ce script, le rôle est *KSCAdmin*, le nom de la base de données du Serveur d'administration est *KAV*) :

   ```
   CREATE USER "KSCAdmin" WITH PASSWORD '<mot de passe>';
   CREATE DATABASE "KAV" ENCODING 'UTF8' OWNER "KSCAdmin";
   GRANT ALL PRIVILEGES ON DATABASE "KAV" TO "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";`

3. 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";
   ```

4. Installez le 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.

Certificats pour l'utilisation de Kaspersky Security Center Linux

Cette section contient des informations sur les certificats de Kaspersky Security Center Linux et décrit comment émettre et remplacer des certificats pour 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.

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 du Serveur Web
- 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 via la section des propriétés du Serveur d'administration dans Kaspersky Security Center Web Console, selon le 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.
- C—certificat commun de réserve pour les ports 13000 et 13291.

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 aux fins suivantes :

- Authentification du Serveur d'administration lors de la connexion à Kaspersky Security Center Web Console
- Interaction sécurisée entre le Serveur d'administration et l'Agent d'administration sur les appareils administrés
- Authentification lorsque les Serveurs d'administration primaires sont connectés aux Serveurs d'administration secondaires

Le certificat de Serveur d'administration est automatiquement créé en cours de l'installation du module Serveur d'administration et sauvegardé dans le dossier /var/opt/kaspersky/klnagent_srv/1093/cert/. Vous indiquez le certificat du Serveur d'administration lors de la création du fichier de réponses pour l'installation de Kaspersky Security Center Web Console. Ce certificat est appelé certificat commun ("C").

Le certificat du Serveur d'administration est valable 397 jours. Kaspersky Security Center génère automatiquement un certificat de réserve commune ("CR") 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.

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

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. 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.

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 définissez le certificat mobile dans les propriétés du Serveur d'administration.

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"). De plus, dans les propriétés du Serveur d'administration, vous pouvez spécifier 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 Web

Le Serveur Web, un module du Serveur d'administration de Kaspersky Security Center, utilise un type de certificat spécial. 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. Pour cela, le Serveur Web peut utiliser différents certificats.

Le Serveur Web utilise l'un des certificats suivants, par ordre de priorité :

1. Certificat de serveur Web personnalisé que vous avez spécifié manuellement à l'aide de Kaspersky Security Center Web Console

2. Certificat commun du Serveur d'administration ("C")

Certificat de Kaspersky Security Center Web Console

Le Serveur de Kaspersky Security Center Web Console (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.

Conditions requises pour les certificats personnalisés utilisés dans Kaspersky Security Center Linux

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

Conditions requises pour les certificats de Kaspersky Security Center Linux

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 la 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 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 Internet 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 Internet 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.

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.

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 la Console Web est auto-signé et généré automatiquement par Kaspersky Security Center Linux. 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 Kaspersky Security Center 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 réémettre le certificat expiré de Kaspersky Security Center Web Console, procédez comme suit :

Réinstallez Kaspersky Security Center Web Console en effectuant l'une des opérations suivantes :

- Si vous souhaitez utiliser le même fichier d'installation de Kaspersky Security Center Web Console, supprimez Kaspersky Security Center Web Console, puis installez la même version de Kaspersky Security Center Web Console.
- Si vous souhaitez utiliser un fichier d'installation d'une version mise à jour, exécutez la commande de mise à jour.

Le certificat de Kaspersky Security Center Web Console est réémis pour une autre durée de validité de 397 jours.

Remplacement de certificat pour Kaspersky Security Center Web Console

Par défaut, lorsque vous installez le serveur de Kaspersky Security Center Web Console (appelé également Kaspersky Security Center Web Console), un certificat de navigateur de 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 par un certificat personnalisé :

1. Créez un nouveau fichier de réponses requis pour l'installation de Kaspersky Security Center Web Console.
2. Dans ce fichier, indiquez les chemins d'accès au fichier de certificat personnalisé et au fichier de clé à l'aide des paramètres `certPath` et `keyPath`.
3. Réinstallez Kaspersky Security Center Web Console en indiquant le nouveau fichier de réponses. Exécutez une des actions suivantes :
   - Si vous souhaitez utiliser le même fichier d'installation de Kaspersky Security Center Web Console, supprimez Kaspersky Security Center Web Console, puis installez la même version de Kaspersky Security Center Web Console.
   - Si vous souhaitez utiliser un fichier d'installation d'une version mise à jour, exécutez la commande de mise à jour.

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 Linux :

1. Dans un utilitaire multiplateforme basé sur OpenSSL, exécutez les commandes suivantes :

```
openssl pkcs12 -in <filename.pfx> -clcerts -nokeys | sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > server.crt
```

```
openssl pkcs12 -in <filename.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.

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

Le nouveau certificat doit être créé au format PKCS#12 (par exemple, au moyen de la PKI de l'organisation) et doit être émis par une autorité de certification (CA) de confiance. De plus, le nouveau certificat doit inclure toute la chaîne de confiance et une clé privée, qui doit être stockée dans le fichier avec l'extension pfx ou p12. Pour le nouveau certificat, les exigences énumérées ci-dessous doivent être remplies.

Type de certificat : certificat commun, certificat de réserve commun (" C ", " CR ")

Conditions :

- 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 ", mais ne peut pas être inférieure à 1.

- Utilisation des clés :
  - Signature numérique
  - Signature du certificat
  - Chiffrement de la 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.

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.

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> {-i <inputfile> [-p <password>] [-o <chkopt>] | -g <dnsname>}][-f <time>][-r <calistfile>]
[-l <logfile>]
```

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

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>`	Le type de certificat à remplacer. Valeurs possibles du paramètre `<type>` : • `C` — remplacer le certificat commun pour les ports 13000 et 13291. • `CR` — remplacer certificat commun de réserve pour les ports 13000 et 13291.
`-f <time>`	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 <inputfile>`	Le conteneur où se trouve le certificat et une clé privée au format PKCS#12 (fichier avec extension .p12 ou .pfx).
`-p <password>`	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 <chkopt>`	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:< key length >` dans l'utilitaire klsetsrvcert, où le paramètre `< key length >` correspond à la valeur de la longueur de clé requise. Sinon, la longueur de clé actuelle du certificat est utilisée.
`-g <dnsname>`	Un certificat est créé pour le nom DNS indiqué.
`-r <calistfile>`	Liste des autorités de certification racine de confiance, format PEM.
`-l <logfile>`	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 <inputfile> -p <password> -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 -t CR -i <inputfile> -p <password> -o NoCA
   ```

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

   ```
   klsetsrvcert -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

Vous pouvez utiliser l'utilitaire klmover pour restaurer la connexion des appareils non contrôlés au Serveur d'administration, par exemple, après une panne du Serveur d'administration, s'il n'est pas possible de le restaurer à partir d'une sauvegarde.

Pour restaurer la connexion, exécutez l'utilitaire klmover à partir de la ligne de commande :

- Pour Linux :
  - Pour les systèmes 32 bits : `/opt/kaspersky/klnagent/bin/klmover [-address adresse du serveur >] [-pn numéro de port >] [-ps numéro de port SSL >] [-nossl] [-cert chemin d'accès au fichier de certificat >]`
  - Pour les systèmes 64 bits : `/opt/kaspersky/klnagent64/bin/klmover [-address adresse du serveur >] [-pn numéro de port >] [-ps numéro de port SSL >] [-nossl] [-cert chemin d'accès au fichier de certificat >]`
- Pour les appareils Windows :
  - Pour les systèmes 32 bits : `< chemin >\klmover.exe [-adresse < adresse du serveur >] [-pn < numéro de port >] [-ps < numéro de port SSL >] [-nossl] [-cert < chemin d'accès au fichier de certificat >]`
  - Pour les systèmes 64 bits : `< chemin >\klmover.exe [-adresse < adresse du serveur >] [-pn < numéro de port >] [-ps < numéro de port SSL >] [-nossl] [-cert < chemin d'accès au fichier de certificat >]`

où `chemin >` est le chemin d'installation par défaut de l'Agent d'administration ou le chemin d'installation que vous avez spécifié dans les paramètres du paquet 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.

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 Linux, vous ne pouvez pas supprimer l'Agent d'administration à l'aide de l'utilitaire klmover ou de la ligne 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.

L'utilitaire klmover requiert des droits d'administrateur local.

L'activation de l'option **Utiliser un mot de passe de désinstallation** sur les appareils Windows 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 <server address>`	Adresse du Serveur d'administration pour la connexion. Vous pouvez spécifier une adresse IP ou un nom DNS.
`-pn <port number>`	Numéro de port à utiliser pour une connexion non sécurisée au Serveur d'administration. Le numéro de port par défaut est 14000.
`-ps <SSL port number>`	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.
`-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 <path to certificate file>`	Utilise le fichier de certificat spécifié pour l'authentification, afin d'accéder au Serveur d'administration.

Désignation du dossier partagé

Après l'installation du Serveur d'administration, vous pouvez indiquer l'emplacement du dossier partagé dans les propriétés du Serveur d'administration. Par défaut, le dossier partagé est créé sur l'appareil doté du Serveur d'administration. 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.

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.

Pour vous connecter à Kaspersky Security Center Web Console, procédez comme suit :

1. Dans votre navigateur web, accédez à <adresse Internet du Serveur d'administration>:<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 Serveur d'administration, la liste des Serveurs d'administration n'est pas vérouillée.

3. Exécutez une des actions suivantes :

   - Pour se connecter au Serveur d'administration avec un compte utilisateur du domaine, il faut saisir 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`

     > 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 se connecter au Serveur d'administration à l'aide des nom d'utilisateur et mot de passe de l'administrateur, il faut saisir le nom d'utilisateur et le mot de passe de l'utilisateur interne.
   - 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.

4. Cliquez sur le bouton **Se connecter**.

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 Linux.

Déconnexion

Pour vous déconnecter de Kaspersky Security Center Web Console,

Dans le menu principal, allez dans les paramètres de votre compte et puis sélectionnez **Se déconnecter**.

Kaspersky Security Center Web Console se ferme, et la page de connexion s'affiche.

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, allez dans les paramètres de votre compte et sélectionnez **Langue**.
2. Sélectionnez une des langues de localisation prises en charge.

Configuration du serveur MySQL x64 pour fonctionner avec Kaspersky Security Center Linux

Si vous utilisez le serveur 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.cnf

Pour plus de détails sur la configuration du SGBD, reportez-vous aussi à la procédure de configuration de compte utilisateur. Pour plus d'informations sur l'installation du SGBD, reportez-vous à la procédure d'installation du SGBD.

Pour configurer le fichier my.cnf :

1. Ouvrez le fichier my.cnf 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`.

Assistant de configuration initiale de l'application

L'application Kaspersky Security Center Linux 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'envoi par email des notifications d'événements survenus pendant le fonctionnement du Serveur d'administration et des applications administrées.
- 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**.
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 à Internet pour utiliser Kaspersky Security Network et télécharger les mises à jour des bases antivirus pour Kaspersky Security Center Linux et les applications Kaspersky administrées.

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 Linux à Internet.

- Numéro de port

  Numéro du port via lequel la connexion proxy à Kaspersky Security Center Linux 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.

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.

Sélectionnez les options :

- Zone

  Vous pouvez sélectionner les zones de protection suivantes :

  - **Postes de travail**
  - **Serveurs de fichiers et systèmes de stockage de données**
  - **Virtualisation**
  - **Systèmes embarqués**
  - **Réseaux industriels**
  - **Terminaux industriels**

- 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.

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.

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 Linux 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. 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 Linux.

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 Linux. S'il n'existe pas de paquet de distribution de l'application pour la langue de Kaspersky Security Center Linux, le paquet de distribution anglais est sélectionné.

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.

Étape 7. Configuration de Kaspersky Security Network

Indiquer les paramètres du transfert des informations sur le fonctionnement de Kaspersky Security Center Linux 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 Linux 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 Linux 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 8. Sélection de la méthode d'activation de l'application

Choisissez une des options suivantes pour activer Kaspersky Security Center Linux :

- **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 Linux. 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 **Déployer 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 plus tard dans la section **Opérations → Licence → Licences pour les logiciels de Kaspersky** du menu principal.

- **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.

  Vous recevez le fichier clé à l'adresse email que vous avez indiquée après l'achat de Kaspersky Security Center.

  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 **Déployer 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 plus tard dans la section **Opérations → Licence → Licences pour les logiciels de Kaspersky** du menu principal.

- Reportez l'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 9. 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.

Étape 10. 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.

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 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**.

Étape 11. Fin de l'Assistant de configuration initiale de l'application

Cliquez sur **Terminer** pour terminer le travail de l'Assistant.

Une fois que vous avez terminé l'Assistant de configuration initiale de l'application, vous pouvez exécuter l'Assistant de déploiement de la protection pour installer automatiquement les applications antivirus ou l'Agent d'administration sur les appareils de votre réseau.

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

Vous pouvez démarrer manuellement l'Assistant de déploiement de la protection à tout moment.

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.

  Le seul moyen d'installer une application pour Windows (y compris l'Agent d'administration pour Windows) sur un appareil sur lequel l'Agent d'administration n'est pas installé est d'utiliser un point de distribution Windows. Par conséquent, lorsque vous installez une application Windows :

  - Sélectionnez cette option.
  - Assurez-vous qu'un point de distribution est attribué aux appareils clients cibles.
  - Assurez-vous que le point de distribution est basé sur 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.

Étape 7. 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 Linux 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 8. 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 9. 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 Linux 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 Linux. 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 10. 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.

Mise à jour de Kaspersky Security Center Linux

Vous pouvez installer le Serveur d'administration version 15 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, tous les données et les paramètres de la version précédente du Serveur d'administration sont conservées.

Avant la mise à jour de Kaspersky Security Center Linux, assurez-vous que vous utilisez les versions du système d'exploitation et du SGBD prises en charge par la version 15 du Serveur d'administration. Si nécessaire, vous pouvez déplacer le Serveur d'administration sur un autre appareil avec les versions ultérieures du système d'exploitation et du SGBD.

Vous pouvez mettre à niveau une version du Serveur d'administration à l'aide de l'une des méthodes suivantes :

- En utilisant le fichier d'installation de Kaspersky Security Center Linux
- En créant la sauvegarde des données du Serveur d'administration, en installant une nouvelle version du Serveur d'administration et en restaurant les données du Serveur d'administration à partir de la sauvegarde

Lors de la mise à jour, l'utilisation simultanée du SGBD par le Serveur d'administration et une autre application est strictement interdite.

Si votre réseau comprend plusieurs Serveurs d'administration, vous devez mettre à jour chaque Serveur manuellement. Kaspersky Security Center Linux ne prend pas en charge la mise à jour centralisée.

De plus, vous devez mettre à jour Kaspersky Security Center Web Console vers une nouvelle version.

Lors de la mise à jour de Kaspersky Security Center Linux à partir d'une version précédente, tous les plug-ins installés des applications Kaspersky prises en charge sont conservés. Le plug-in Serveur d'administration et le plug-in Agent d'administration sont mis à niveau automatiquement. Avant de lancer la mise à jour, il est conseillé de créer une copie de sauvegarde des données du Serveur d'administration.

Mise à niveau de Kaspersky Security Center Linux à l'aide du fichier d'installation

Pour mettre à niveau le Serveur d'administration d'une version précédente (à partir de la version 13) vers la version 15.2, vous pouvez installer une nouvelle version sur une version antérieure à l'aide du fichier d'installation de Kaspersky Security Center Linux.

Pour mettre à niveau une version antérieure du Serveur d'administration vers la version 15.2 à l'aide du fichier d'installation :

1. Téléchargez le fichier d'installation de Kaspersky Security Center Linux avec un paquet complet pour la version 15.2 depuis le site de Kaspersky :
   - Pour les appareils exécutant un système d'exploitation basé sur RPM : ksc64-<version number>.x86_64.rpm
   - Pour les appareils exécutant un système d'exploitation basé sur Debian : ksc64_<version number>_amd64.deb

2. Mettez à niveau le paquet d'installation à l'aide du gestionnaire de paquets que vous utilisez sur votre Serveur d'administration. Par exemple, vous pouvez utiliser les commandes suivantes dans le terminal de ligne de commande sous un compte doté des privilèges root :

   - Pour les appareils exécutant un système d'exploitation basé sur RPM :
     ```
     $ sudo rpm -Uvh --nodeps --force ksc64-<version number>.x86_64.rpm
     ```
   - Pour les appareils exécutant un système d'exploitation basé sur Debian :
     ```
     $ sudo dpkg -i ksc64_<version number>_amd64.deb
     ```

   Une fois que la commande a été exécutée avec succès, le script /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl est créé. Le message à ce sujet s'affiche dans le terminal.

3. Sous un compte disposant des privilèges root, exécutez le script /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl pour configurer le Serveur d'administration mis à jour.

4. Lisez le Contrat de licence et la Politique de confidentialité qui s'affichent dans le terminal de ligne de commande. Si vous acceptez tous les termes du Contrat de licence et de la Politique de confidentialité :

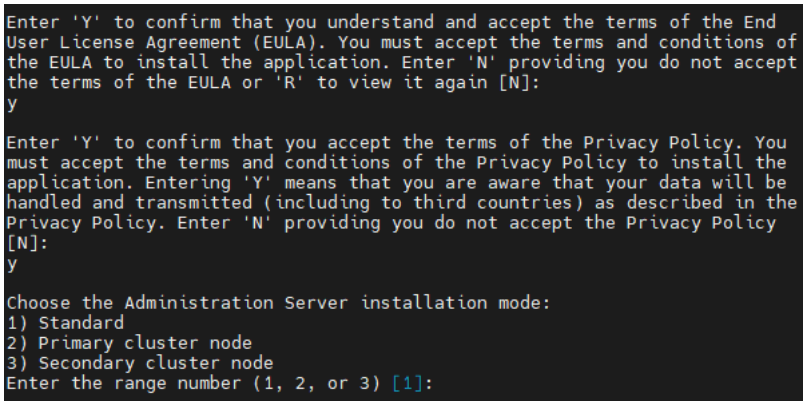
   a. Saisissez " Y " pour confirmer que vous avez entièrement lu, compris et accepté les termes et conditions du CLUF.

   b. Saisissez à nouveau le " Y " pour confirmer que vous avez entièrement lu, compris et accepté la politique de confidentialité qui décrit le traitement des données.

   L'installation de l'application sur votre appareil se poursuivra une fois que vous aurez entré deux fois 'Y'.

5. Saisissez " 1 " pour sélectionner le mode d'installation standard du Serveur d'administration.

   L'image ci-dessous montre les deux dernières étapes.



Acceptation des conditions du CLUF et de la Politique de confidentialité et sélection du mode d'installation standard du Serveur d'administration dans le terminal de ligne de commande

   Ensuite, le script configure et termine la mise à jour du Serveur d'administration. Lors de la mise à jour, vous ne pouvez pas modifier les paramètres du Serveur d'administration ajustés avant la mise à jour.

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 Linux.

   Une fois la tâche d'installation à distance terminée, la version de l'Agent d'administration est mise à jour.

Mise à niveau de Kaspersky Security Center Linux via la sauvegarde

Pour mettre à jour le Serveur d'administration d'une version précédente (à partir de la version 13) vers la version 15, vous pouvez créer une sauvegarde des données du Serveur d'administration et restaurer ces données après l'installation de Kaspersky Security Center Linux d'une nouvelle version. En cas de problèmes lors de l'installation, vous pouvez restaurer la version précédente du Serveur d'administration, en utilisant la sauvegarde des données du Serveur créée avant la mise à jour.

Pour mettre à jour une version antérieure du Serveur d'administration vers la version 15 via la sauvegarde, procédez comme suit :

1. Avant la mise à jour, sauvegardez les données du Serveur d'administration avec une version antérieure de l'application.
2. Désinstallez l'ancienne version de Kaspersky Security Center Linux.
3. Installez Kaspersky Security Center version 15 sur l'ancien Serveur d'administration.
4. Restaurez les données du Serveur d'administration à partir de la sauvegarde créée avant la mise à jour.
5. 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 Linux.

   Une fois la tâche d'installation à distance terminée, la version de l'Agent d'administration est mise à jour.

Mise à jour de Kaspersky Security Center sur les nœuds du cluster de basculement Kaspersky Security Center Linux

Vous pouvez installer la version 15 du Serveur d'administration sur chaque nœud du cluster de basculement Kaspersky Security Center Linux sur lequel le Serveur d'administration est installé avec une version antérieure (à partir de la version 14). Lors de la mise à jour jusqu'à la version 15, tous les données et les paramètres de la version précédente du Serveur d'administration sont conservées.

> Si vous avez déjà installé Kaspersky Security Center Linux localement sur les appareils, vous pouvez également mettre à niveau Kaspersky Security Center Linux sur ces appareils à l'aide du fichier d'installation ou via une sauvegarde.

Pour mettre à jour Kaspersky Security Center sur les nœuds du cluster de basculement Kaspersky Security Center Linux :

1. Téléchargez le fichier d'installation de Kaspersky Security Center Linux avec un paquet complet pour la version 15 depuis le site de Kaspersky :
   - Pour les appareils exécutant un système d'exploitation basé sur RPM—ksc64-<version number>-<build number>.x86_64.rpm

- Pour les appareils exécutant un système d'exploitation basé sur Debian—ksc64_<version number>-<build number>_amd64.deb

2. Arrêter le cluster.

3. Sur le nœud actif du cluster, mettez à niveau le paquet d'installation à l'aide du gestionnaire de paquets que vous utilisez sur votre Serveur d'administration.

   Par exemple, vous pouvez utiliser les commandes suivantes dans le terminal de ligne de commande sous un compte doté des privilèges root :

   - Pour les appareils exécutant un système d'exploitation basé sur RPM :
     ```
     $ sudo rpm -Uvh --nodeps --force ksc64-<version number>-<build number>.x86_64.rpm
     ```
   - Pour les appareils exécutant un système d'exploitation basé sur Debian :
     ```
     $ sudo dpkg -i ksc64_<version number>-<build number>_amd64.deb
     ```

   Une fois que la commande a été exécutée avec succès, le script /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl est créé. Le message à ce sujet s'affiche dans le terminal.

4. Sous un compte disposant des privilèges root, exécutez le script /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl pour configurer le Serveur d'administration mis à jour.

5. Lisez le Contrat de licence et la Politique de confidentialité qui s'affichent dans le terminal de ligne de commande. Si vous acceptez tous les termes du Contrat de licence et de la Politique de confidentialité :

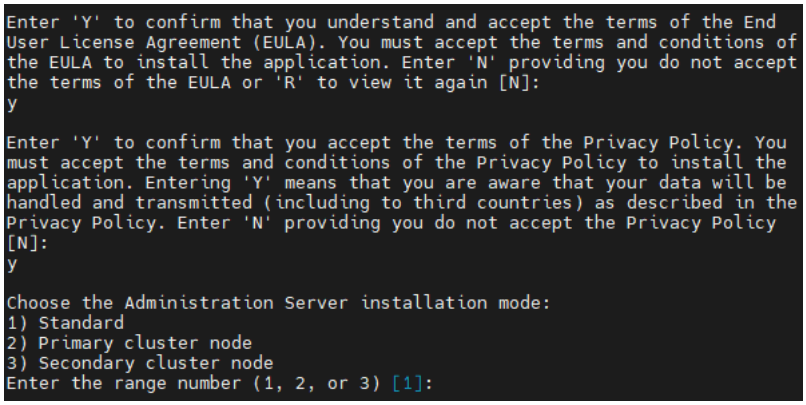
   a. Saisissez " Y " pour confirmer que vous avez entièrement lu, compris et accepté les termes et conditions du CLUF.

   b. Saisissez à nouveau le " Y " pour confirmer que vous avez entièrement lu, compris et accepté la politique de confidentialité qui décrit le traitement des données.

   L'installation de l'application sur votre appareil se poursuivra une fois que vous aurez entré deux fois 'Y'.

6. Sélectionnez le nœud sur lequel vous effectuez la mise à niveau en saisissant " 2 ".

   L'image ci-dessous montre les deux dernières étapes.



Acceptation des conditions du CLUF et de la Politique de confidentialité et sélection du mode d'installation dans le terminal de ligne de commande

   Ensuite, le script configure et termine la mise à jour du Serveur d'administration. Lors de la mise à jour, vous ne pouvez pas modifier les paramètres du Serveur d'administration ajustés avant la mise à jour.

7. Effectuez les étapes 3 à 5 sur le nœud passif.

   À l'étape 6, saisissez " 3 " pour sélectionner le nœud.

8. Démarrer le cluster.

   Notez que vous pouvez démarrer le cluster sur n'importe quel nœud. Si vous démarrez le cluster sur le nœud passif, il devient le nœud actif.

   Par conséquent, vous avez installé le Serveur d'administration de la dernière version sur les nœuds du cluster de basculement de Kaspersky Security Center Linux.

Mise à niveau de Kaspersky Security Center Web Console

Cet article décrit comment mettre à jour Kaspersky Security Center Web Console Server (appelé aussi Kaspersky Security Center Web Console) sur des appareils qui fonctionnent avec un système d'exploitation Linux.

Si vous devez mettre à jour Kaspersky Security Center Web Console sur Astra Linux en mode environnement logiciel fermé, suivez les instructions spécifiques à Astra Linux.

Utilisez l'un des fichiers d'installation suivants qui correspond à la distribution Linux installée sur votre appareil :

- Pour Debian : ksc-web-console-[build_number].x86_64.deb
- Pour les systèmes d'exploitation basés sur RPM : ksc-web-console-[build_number].x86_64.rpm
- Pour ALT 8 SP : ksc-web-console-[build_number]-alt8p.x86_64.rpm

Vous récupérez le fichier d'installation en le téléchargeant du site Web de Kaspersky.

Pour mettre à jour Kaspersky Security Center Web Console, procédez comme suit :

1. Assurez-vous que l'appareil sur lequel vous voulez mettre à jour Kaspersky Security Center Web Console fonctionne sur une des distributions Linux supportées.

2. Lisez et acceptez le Contrat de licence utilisateur final (CLUF). Si le kit de distribution Kaspersky Security Center Linux ne contient pas de fichier TXT avec le texte du CLUF, vous pouvez télécharger le fichier depuis le site de Kaspersky. Si vous n'acceptez pas les conditions du Contrat de licence, ne mettez pas à jour Kaspersky Security Center Web Console à l'aide du fichier d'installation.

3. Utilisez le même fichier de réponses que vous avez préparé avant d'installer Kaspersky Security Center Web Console. Le nom du fichier de réponses est ksc-web-console-setup.json et l'emplacement du fichier est /etc/ksc-web-console-setup.json.

   Si le fichier de réponses n'existe pas, créez un nouveau fichier de réponses qui contient les paramètres de connexion de Kaspersky Security Center Web Console au Serveur d'administration. Nommez le fichier ksc-web-console-setup.json, puis placez-le dans le répertoire /etc.

   Exemple de fichier de réponse qui contient l'ensemble minimum de paramètres et l'adresse et le port par défaut :

   ```
   {
     "address": "127.0.0.1",
     "port" : 8080,
     "trusted":
     "127.0.0.1|13299|/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer|KSC
     Server",
   ```

```
  "acceptEula": true
}
```

Si vous souhaitez mettre à jour Kaspersky Security Center Web Console connect au Serveur d'administration installé sur les nœuds du cluster de basculement Kaspersky Security Center Linux, dans le fichier de réponses, indiquez le paramètre de l'installation de `confiance` pour permettre au cluster de basculement Kaspersky Security Center Linux de se connecter à Kaspersky Security Center Web Console. La valeur de chaîne de ce paramètre a le format suivant :

```
"trusted": "server address|port|certificate path|server name"
```

Spécifiez les modules du paramètre d'installation de `trusted` :

- **Adresse du Serveur d'administration**. Si vous avez créé la carte réseau virtuelle lors de la préparation des nœuds du cluster, utilisez l'adresse IP de la carte comme adresse du cluster de basculement Kaspersky Security Center Linux. Dans le cas contraire, indiquez l'adresse IP du répartiteur de charge tiers que vous utilisez.
- **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 Linux. Chemin d'accès par défaut au fichier du certificat est : <shared data folder>\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.
- **Nom du Serveur d'administration**. Nom du cluster de basculement Kaspersky Security Center Linux qui s'affichera dans la fenêtre de connexion de Kaspersky Security Center Web Console.

Kaspersky Security Center Web Console ne peut pas être mis à jour à l'aide du même fichier d'installation .rpm. Si vous voulez modifier les paramètres d'un fichier de réponses et utiliser ce fichier pour réinstaller l'application, vous devez d'abord supprimer l'application, puis la réinstaller avec le nouveau fichier de réponses.

4. Dans un compte avec les privilèges racine, utilisez la ligne de commande pour exécuter le fichier de paramétrage avec l'extension .deb ou .rpm, selon votre distribution Linux.

   Pour effectuer une mise à niveau à partir d'une version précédente de Kaspersky Security Center Web Console, exécutez une des commandes suivantes :

   - Pour les appareils exécutant un système d'exploitation basé sur RPM :
     ```
     $ sudo rpm -Uvh --nodeps --force ksc-web-console-[build_number].x86_64.rpm
     ```
   - Pour les appareils exécutant un système d'exploitation basé sur Debian :
     ```
     $ sudo dpkg -i ksc-web-console-[build_number].x86_64.deb
     ```

   Cette action lance la décompression du fichier d'installation. Veuillez patienter jusqu'à la fin de l'installation.

5. Redémarrez tous les services de Kaspersky Security Center Web Console en exécutant la commande suivante :
   ```
   $ sudo systemctl restart KSC*
   ```

Quand la mise à jour est terminée, vous pouvez utiliser un navigateur pour ouvrir et vous connecter à Kaspersky Security Center Web Console.

Mise à jour de Kaspersky Security Center Web Console sur Astra Linux en mode environnement logiciel fermé

Cet article décrit comment mettre à jour le Serveur de Kaspersky Security Center Web Console (également appelé Kaspersky Security Center Web Console) sur le système d'exploitation Astra Linux Special Edition.

Pour mettre à jour Kaspersky Security Center Web Console, procédez comme suit :

1. Assurez-vous que l'appareil sur lequel vous voulez mettre à jour Kaspersky Security Center Web Console fonctionne sur une des distributions Linux supportées.

2. Lisez et acceptez le Contrat de licence utilisateur final (CLUF). Si le kit de distribution Kaspersky Security Center Linux ne contient pas de fichier TXT avec le texte du CLUF, vous pouvez télécharger le fichier depuis le site de Kaspersky. Si vous n'acceptez pas les conditions du Contrat de licence, ne mettez pas à jour Kaspersky Security Center Web Console à l'aide du fichier d'installation.

3. Utilisez le même fichier de réponses que vous avez préparé avant d'installer Kaspersky Security Center Web Console. Le nom du fichier de réponses est ksc-web-console-setup.json et l'emplacement du fichier est /etc/ksc-web-console-setup.json.

   Si le fichier de réponses n'existe pas, créez un nouveau fichier de réponses qui contient les paramètres de connexion de Kaspersky Security Center Web Console au Serveur d'administration. Nommez le fichier ksc-web-console-setup.json, puis placez-le dans le répertoire /etc.

   Exemple de fichier de réponse qui contient l'ensemble minimum de paramètres et l'adresse et le port par défaut :

   ```
   {
     "address": "127.0.0.1",
     "port": 8080,
     "trusted":
   "127.0.0.1|13299|/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer|KSC
   Server",
     "acceptEula": true
   }
   ```

4. Assurez-vous que dans le fichier `/etc/digsig/digsig_initramfs.conf`, le paramètre `DIGSIG_ELF_MODE` est spécifié comme suit :

   ```
   DIGSIG_ELF_MODE=1
   ```

5. Assurez-vous que le paquet de compatibilité `astra-digsig-oldkeys` est installé.

   Si ce paquet n'est pas installé, exécutez la commande suivante :

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

6. Créez un répertoire pour la clé de l'application s'il n'existe pas :

   ```
   mkdir -p /etc/digsig/keys/legacy/kaspersky/
   ```

7. Placez la clé de l'application /opt/kaspersky/ksc64/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 Kaspersky Security Center Linux 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.

8. Mettez à jour les disques RAM :

   ```
   update-initramfs -u -k all
   ```

   Redémarrez le système.

9. Sous un compte avec les privilèges root, utilisez la ligne de commande pour exécuter le fichier d'installation. Vous récupérez le fichier d'installation en le téléchargeant du site de Kaspersky.

   Pour effectuer une mise à niveau à partir d'une version précédente de Kaspersky Security Center Web Console, exécutez la commande suivante :

   ```
   $ sudo dpkg -i ksc-web-console-[build_number].x86_64.deb
   ```

   Cette action lance la décompression du fichier d'installation. Veuillez patienter jusqu'à la fin de l'installation.

10. Redémarrez tous les services de Kaspersky Security Center Web Console en exécutant la commande suivante :

    ```
    $ sudo systemctl restart KSC*
    ```

Quand la mise à jour est terminée, vous pouvez utiliser un navigateur pour ouvrir et vous connecter à Kaspersky Security Center Web Console.

Migration vers Kaspersky Security Center Linux

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.

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.

Avant de commencer, informez-vous sur les fonctionnalités et les limites de Kaspersky Security Center Linux :

- Différences fonctionnelles entre Kaspersky Security Center Windows et Kaspersky Security Center Linux
- Liste d'applications Kaspersky prises en charge par Kaspersky Security Center Linux

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. **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 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.

4. **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
- 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
- Désigner et configurer les points de distribution

  Si vous déplacez un appareil qui agit comme point de distribution vers un autre Serveur d'administration, les appareils inclus dans la portée du point de distribution ne sont pas déplacés automatiquement. Vous devez déplacer chaque appareil individuellement. Si un point de distribution agit comme passerelle, vous devez exécuter le script `# /opt/kaspersky/klnagent64/bin/setup/postinstall.pl` afin que le point de distribution ne serve plus de passerelle.

5. **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.

6. **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.

7. **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, il existe d'autres méthodes pour transférer vos objets actuels, mais ces méthodes vous permettent de transférer uniquement les stratégies et les tâches :

- 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. Sélectionnez **Migrer vers Kaspersky Security Center Linux ou Kaspersky Single Management Platform** pour lancer l'Assistant et suivre ses étapes.

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*.
- 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**).

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.

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

Par défaut, les connexions à Kaspersky Security Center Linux sont autorisées depuis n'importe quel appareil. Par exemple, vous pouvez installer Kaspersky Security Center Web Console Server sur n'importe quel appareil qui satisfait à la configuration requise et le Kaspersky Security Center Web Console Server communiquera avec Kaspersky Security Center Linux. Cependant, vous pouvez configurer le Serveur d'administration pour que les connexions soient autorisées uniquement à partir des appareils utilisant les adresses IP que vous spécifiez. Dans ce cas, si un intrus tente de se connecter à Kaspersky Security Center Linux 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 Linux.

L'adresse IP est vérifiée lorsqu'un utilisateur se connecte à Kaspersky Security Center Linux ou exécute une application qui interagit avec le Serveur d'administration via Kaspersky Security Center Linux OpenAPI. À ce moment, une application sur un appareil 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 :

- Serveur de Kaspersky Security Center Web Console

  Si vous vous connectez à Kaspersky Security Center Linux via Kaspersky Security Center Web Console, vous pouvez configurer un pare-feu sur l'appareil où Kaspersky Security Center Web Console Server est installé à l'aide du système d'exploitation standard. Ensuite, si quelqu'un essaie de se connecter à Kaspersky Security Center Linux sur un appareil et Kaspersky Security Center Web Console Server est installé sur un autre appareil, un pare-feu permet d'empêcher les intrus d'intervenir.

- 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 Linux :

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 Linux (généralement, /opt/kaspersky/ksc64/sbin).
3. Sous le compte root, saisissez la commande suivante :
   `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 Syslog 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. Sous le compte root, saisissez la commande suivante à l'invite de commande :
   ```
   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.

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 Linux 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 Linux à Internet.

   - **Numéro de port**

     Numéro du port via lequel la connexion proxy à Kaspersky Security Center Linux 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.

Hiérarchie des Serveurs d'administration

Certaines entreprises clientes, par exemple MSP, peuvent exécuter plusieurs Serveurs d'administration. L'administration de plusieurs serveurs hétérogènes n'est pas pratique et pour cette raison, il est utile de les regrouper dans une hiérarchie. Dans la hiérarchie, un Serveur d'administration basé sur Linux peut fonctionner à la fois comme Serveur primaire et comme Serveur secondaire. Le Serveur primaire basé sur Linux peut gérer à la fois les Serveurs secondaires Linux et Windows. Un Serveur Windows primaire peut administrer un Serveur Linux secondaire.

La configuration " primaire/secondaire " entre deux Serveurs d'administration offre les possibilités suivantes :

- Un Serveur d'administration secondaire hérite des stratégies, des tâches, des rôles d'utilisateur et des paquets d'installation du Serveur d'administration primaire, évitant ainsi la duplication des paramètres.
- 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.
- Un Serveur d'administration principal peut être utilisé comme source de mises à jour pour un Serveur d'administration secondaire.

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.

Création d'une hiérarchie des Serveurs d'administration : ajout d'un Serveur d'administration secondaire

Dans la hiérarchie, un Serveur d'administration basé sur Linux peut fonctionner à la fois comme Serveur primaire et comme Serveur secondaire. Le Serveur primaire basé sur Linux peut gérer à la fois les Serveurs secondaires Linux et Windows. Un Serveur Windows primaire peut administrer un Serveur Linux 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, cliquez 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. Dans 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 :

   - **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.

   - **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, 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.

   - **Utiliser un serveur proxy**

Sélectionnez cette option si vous utilisez un serveur proxy pour vous connecter au Serveur d'administration secondaire.

Dans ce cas, vous devez également indiquer les paramètres suivants du serveur proxy :

- **Adresse**
- **Nom d'utilisateur**
- **Mot de passe**

7. 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.
8. Saisissez les identifiants de l'utilisateur qui dispose des droits d'accès sur le futur Serveur d'administration secondaire.

Assurez-vous que la vérification en deux étapes est désactivée pour le compte que vous spécifiez. Si la vérification en deux étapes est activée pour ce compte, vous pouvez créer la hiérarchie à partir du futur Serveur secondaire uniquement (voir les instructions ci-dessous). Il s'agit d'un problème connu.

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 désignez manuellement le certificat du futur Serveur secondaire.

La connexion peut également échouer, car le futur Serveur secondaire est authentifié à l'aide d'un certificat auto-signé qui a été généré automatiquement par Kaspersky Security Center Linux. Par conséquent, le navigateur peut bloquer le téléchargement du certificat auto-signé. Si tel est le cas, vous pouvez effectuer l'une des opérations suivantes :

- Pour le futur Serveur secondaire, créez un certificat de confiance dans votre infrastructure et qui répond aux exigences des certificats personnalisés.
- Ajoutez le certificat auto-signé du futur Serveur secondaire 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. Pour en savoir plus sur l'ajout d'un certificat à la liste des certificats de confiance, consultez la documentation de votre navigateur.

Une fois l'exécution de l'Assistant terminée, la hiérarchie "primaire/secondaire" est établie. 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 ou parce que le fichier de certificat du Serveur d'administration secondaire est auto-signé), vous pouvez toujours 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 primaire, dans /var/opt/kaspersky/klnagent_srv/1093/cert/.

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 primaire 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 de Kaspersky Security Center Web Console correspondant à la distribution Linux installée sur votre appareil sous 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.

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.

   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.
6. 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 de Kaspersky Security Center Web Console correspondant à la distribution Linux installée sur votre appareil sous 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.

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 **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 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 Linux, 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.

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 /var/opt/kaspersky/klnagent_srv/logs/sc.syslog.

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 sur les événements rejetés sont écrites dans le journal du système d'exploitation. Les nouveaux événements sont placés dans une file d'attente et enregistrés dans la base de données dès que la suppression est terminée. Par défaut, la file d'attente des événements est limitée à 20 000 événements. Vous pouvez personnaliser la limite de la file d'attente en modifiant la valeur de l'indicateur KLEVP_MAX_POSTPONED_CNT.

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.

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.

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. Installez le Serveur d'administration sur le nouvel appareil.

   Notez que si vous déplacez le serveur de base de données vers un autre appareil, indiquez l'adresse locale comme adresse IP de l'appareil sur lequel la base de données est installée (le " h " dans les instructions Installation de Kaspersky Security Center Linux). Si vous devez conserver le serveur de base de données sur l'appareil précédent, saisissez l'adresse IP de l'appareil précédent dans la case " h " de l'instruction Installation de Kaspersky Security Center Linux.

7. Une fois l'installation terminée, restaurez les données du Serveur d'administration sur le nouvel appareil à l'aide de l'utilitaire klbackup.

8. Ouvrez Kaspersky Security Center Web Console et connectez-vous au Serveur d'administration.

9. Vérifiez que tous les appareils administrés sont connectés au Serveur d'administration.

10. Désinstallez le Serveur d'administration et le serveur de base de données de l'appareil précédent.

Modification des informations d'identification du SGBD

Parfois, 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 informations d'identification de SGBD dans un environnement Linux à l'aide de l'utilitaire klsrvconfig :

1. Lancez une ligne de commande Linux.

2. Spécifiez l'utilitaire klsrvconfig dans la fenêtre de ligne de commande ouverte :

   ```
   sudo /opt/kaspersky/ksc64/sbin/klsrvconfig -set_dbms_cred
   ```

3. Indiquez un nouveau nom de compte. Vous devez spécifier les identifiants d'un compte qui existe dans le SGBD.

4. Saisissez un nouveau mot de passe.

5. Indiquez le nouveau mot de passe pour confirmation.

Les informations d'identification de SGBD sont modifiées.

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. La sauvegarde permet de restaurer les données lors du déplacement de la base de données du Serveur d'administration vers un autre appareil ou lors de la mise à jour vers une version plus récente de Kaspersky Security Center Linux (le déplacement des données du Serveur d'administration 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.

Vous pouvez créer une copie de sauvegarde des données du Serveur d'administration à l'aide d'une des options suivantes :

- En créant et en exécutant une tâche de sauvegarde des données via Kaspersky Security Center Web Console.
- 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 (généralement, /opt/kaspersky/ksc64/sbin/klbackup).

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.

La restauration des données du Serveur d'administration est possible uniquement à l'aide de l'utilitaire klbackup.

Création d'une tâche de copie de sauvegarde des données du Serveur d'administration

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.

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.

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. Parcourez les étapes de l'Assistant à l'aide du bouton **Suivant**.
3. Dans la liste **Application**, sélectionnez **Kaspersky Security Center 15**, et dans la liste **Type de tâche**, sélectionnez **Sauvegarde des données du Serveur d'administration**.
4. A l'étape correspondante, indiquez les informations suivantes :
   - Dossier pour le stockage des copies de sauvegarde
   - Mot de passe pour la sauvegarde (facultatif)
   - Nombre maximum de copies de sauvegarde à enregistrer
5. Si, à l'étape **Fin de la création de la tâche**, vous activez l'option **Ouvrir les détails de la tâche à la fin de la création**, vous pouvez modifier les paramètres de la tâche par défaut. 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 **Terminer**.

La tâche est créée et s'affiche dans la liste des tâches.

Sauvegarde et restauration des données à l'aide de l'utilitaire 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'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.

Si vous avez sauvegardé les données du Serveur d'administration inclus dans Kaspersky Security Center Linux 15 ou toute version antérieure en utilisant le SGBD MariaDB d'une version antérieure, et que vous récupérez ensuite les données sur un appareil avec une version ultérieure de MariaDB, une erreur peut se produire. Pour en savoir plus, consultez l'article Comment restaurer des données du Serveur d'administration à partir d'une sauvegarde créée sur une version antérieure du SGBD.

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.

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.

Syntaxe de l'utilitaire :

```
klbackup -path BACKUP_PATH [-linux_path LINUX_PATH][-node_cert CERT_PATH] [-logfile
LOGFILE] [-use_ts]|[-restore] [-password PASSWORD]
```

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 BACKUP_PATH` : enregistre les données dans le dossier BACKUP_PATH ou les utilise pour la restauration à partir du dossier BACKUP_PATH (paramètre obligatoire).
- `-linux_path LINUX_PATH` : chemin d'accès local du dossier contenant les données de sauvegarde du SGBD.

  Le compte utilisateur du serveur de base de données et l'outil klbackup doivent posséder les droits pour modifier les données dans le dossier LINUX_PATH.
- `-node_cert CERT_PATH` : fichier de certificat de serveur pour configurer le nœud de cluster de basculement inactif après la récupération. S'il n'est pas défini, il est automatiquement récupéré sur le Serveur.
- `-logfile LOGFILE` : enregistre un rapport sur la sauvegarde ou la restauration des données du Serveur d'administration.

  Le compte utilisateur du serveur de base de données et l'outil klbackup doivent posséder les droits pour modifier les données dans le dossier BACKUP_PATH.
- `-use_ts` — Lors de l'enregistrement des données, copiez les informations dans le dossier BACKUP_PATH, 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 BACKUP_PATH.

  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 `/tmp/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 BACKUP_PATH. Si aucune clé n'est disponible, la copie de sauvegarde des données s'opère dans le dossier BACKUP_PATH.
- `-password PASSWORD` : 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. Pour restaurer les données du Serveur d'administration à partir d'une sauvegarde, nous vous recommandons de lancer l'utilitaire sur un Serveur d'administration récemment installé.

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 PostgreSQL comme SGBD) :
  - 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 prend en charge les versions MariaDB 10.3 et ultérieures. Si vous utilisez MariaDB version 10.2 ou antérieure, les administrateurs doivent administrer eux-mêmes ce SGBD.

La tâche Maintenance du Serveur d'administration est créée automatiquement lors de l'installation de Kaspersky Security Center Linux. 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 **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.

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.

Accès aux serveurs DNS publics

Si l'accès aux serveurs Kaspersky via le système DNS n'est pas possible, Kaspersky Security Center Linux 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 Linux 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 la ligne de commande, puis remplacez votre répertoire actuel par celui contenant l'utilitaire klscflag. L'utilitaire klsclag se trouve dans le répertoire dans lequel le Serveur d'administration est installé. Le chemin d'installation par défaut est /opt/kaspersky/ksc64/sbin.

2. Pour désactiver l'utilisation du DNS public, exécutez la commande suivante sous le compte root :

   ```
   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 sous le compte root :

   ```
   klscflag -fset -pv ".core/.independent" -s Transport -n ForceUseSystemDNS -t d -v 0
   ```

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 l'option **Afficher le chiffrement et la protection des données**.

3. Cliquez sur **Enregistrer**.

Après cela, la section **Opérations** → **Chiffrement et protection des données** apparaît dans le menu principal.

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. Kaspersky Security Center Linux 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 Linux utilise des certificats auto-signés. Vous pouvez également utiliser vos propres certificats. Les experts de Kaspersky recommande d'utiliser des certificats émis par des autorités de certification de confiance.

Pour configurer les protocoles de chiffrement et les suites cryptographiques sur le Serveur d'administration :

1. Exécutez la ligne de commande, puis remplacez votre répertoire actuel par celui contenant l'utilitaire klscflag. L'utilitaire klsclag se trouve dans le répertoire dans lequel le Serveur d'administration est installé. Le chemin d'installation par défaut est /opt/kaspersky/ksc64/sbin.

2. Utilisez l'indicateur SrvUseStrictSslSettings pour configurer les protocoles de chiffrement et les suites de chiffrement autorisés sur le Serveur d'administration. Sous le compte root, exécutez la commande suivante dans la ligne de commande :

   ```
   klscflag -fset -pv ".core/.independent" -s Transport -n SrvUseStrictSslSettings -
   v <value> -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 Linux). 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 (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 Linux suivants :

   - Serveur d'administration
   - Serveur Web
   - Proxy d'activation

En conséquence, 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 la ligne de commande, puis remplacez votre répertoire actuel par celui contenant l'utilitaire klscflag. L'utilitaire klsclag se trouve dans le répertoire dans lequel le Serveur d'administration est installé. Le chemin d'installation par défaut est /opt/kaspersky/ksc64/sbin.

2. Dans la ligne de commande sous le compte root, exécutez une des commandes suivantes :

   - 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 <value> -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 <value> -t d
     ```

   Spécifiez le paramètre <value> de l'indicateur :

   - `1` : Pour activer la prise en charge du protocole TLS.
   - `0` : Pour désactiver la prise en charge du protocole TLS.

Liste globale des sous-réseaux

Pour chaque Serveur d'administration que vous utilisez, vous pouvez créer une liste globale des sous-réseaux dans laquelle seront stockées les informations relatives aux sous-réseaux de votre réseau. 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.

Pour ajouter un sous-réseau à la liste globale des sous-réseaux :

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. **GénéralSous-réseaux globaux**Sous l'onglet Général, sélectionnez la section Certificats.

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

   Nouveau sous-réseau La fenêtre Nouveau sous-réseau s'ouvre.

4. Remplissez les champs suivants :

   - **Nom**
   - **Adresse de sous-réseau**
   - **Masque de sous-réseau**
   - **Description**

5. Cliquez sur **Enregistrer**.

La fenêtre se ferme et le sous-réseau apparaît dans la liste des sous-réseaux.

Si nécessaire, vous pouvez effectuer les opérations suivantes dans la liste des sous-réseaux globaux :

- Supprimez des sous-réseaux de la liste en sélectionnant le sous-réseau requis et en cliquant sur le bouton **Supprimer** .
- Modifiez les propriétés des sous-réseaux en cliquant sur le lien portant le nom du sous-réseau requis, puis en exécutant les actions décrites aux étapes 4 à 5.

Recherche d'appareils en réseau

Cette section décrit les outils de recherche et de découverte des appareils du réseau.

Kaspersky Security Center Linux 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. Lorsque tous les appareils en réseau sont découverts, vous pouvez obtenir des informations à leur sujet et les administrer par des stratégies. Des sondages réseau réguliers sont nécessaires pour déterminer s'il existe de nouveaux appareils et si les appareils précédemment découverts sont toujours sur le réseau.

La découverte des appareils en réseau se déroule par étapes :

1. **Recherche d'appareils initiale**

   Une fois que vous avez terminé l'Assistant de démarrage rapide, effectuez la découverte de l'appareil manuellement.

2. **Configuration des prochains sondages**

   Assurez-vous que le sondage des plages IP est activé et que la planification du sondage répond aux besoins de votre organisation. Lors de la configuration de la planification du sondage, utilisez les recommandations de fréquence de sondage du réseau.

   Vous pouvez également activer le sondage Zeroconf si votre réseau inclut des appareils IPv6.

   Si des appareils en réseau sont inclus dans un domaine, il est recommandé d'utiliser le sondage du contrôleur de domaine.

3. **Configuration de règles pour l'ajout d'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 automatique pour déplacer ces appareils vers le groupe **Appareils administrés**. Vous pouvez aussi définir des règles de conservation.

   Si vous ignorez cette étape de définition des règles, tous les appareils détectés sont placés dans le groupe **Appareils non définis** et y restent. 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 de chaque appareil et décider si vous voulez le déplacer vers un groupe d'administration, et si oui, choisir le groupe.

Résultats

La réalisation du scénario donne les résultats suivants :

- Le Serveur d'administration de Kaspersky Security Center Linux 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**).

Sondage des plages IP

Kaspersky Security Center Linux tente d'effectuer une résolution de nom inversée pour chaque adresse IPv4 de la plage spécifiée vers un nom DNS à l'aide de requêtes DNS standard. Si cette opération réussit, le serveur envoie une `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 Linux. La résolution de nom inverse est nécessaire pour exclure les appareils réseau qui ne peuvent avoir d'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. Si cette zone n'est pas configurée, le sondage du sous-réseau IP ne donnera aucun résultat.

Au début, Kaspersky Security Center Linux 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 Linux inclut automatiquement le réseau 192.168.0.0/24 dans la liste des adresses de sondage. Kaspersky Security Center Linux sonde dans ce cas toutes les adresses entre 192.168.0.1 et 192.168.0.254.

Si seul le sondage des plages IP est activé, Kaspersky Security Center Linux ne détecte que les appareils dotés d'une adresse IPv4. Si votre réseau inclut des appareils IPv6, activez le sondage Zeroconf des appareils.

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 Linux 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 Linux inclut automatiquement le réseau 192.168.0.0/24 dans la liste des adresses de sondage. Kaspersky Security Center Linux 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 Linux 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**. 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.

Kaspersky Security Center Linux peut sonder les réseaux qui ont des appareils avec des adresses IPv6. Dans ce cas, les plages IP ne sont pas spécifiées et Kaspersky Security Center Linux 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 l'appareil Linux qui sonde les réseaux : le Serveur d'administration ou un point de distribution.

Pour activer le sondage Zeroconf :

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, Kaspersky Security Center Linux commence à sonder votre réseau. Dans ce cas, les plages IP spécifiées sont ignorées.

Sondage du contrôleur de domaine

Kaspersky Security Center Linux prend en charge le sondage d'un contrôleur de domaine Microsoft Active Directory et d'un contrôleur de domaine Samba. 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.

Le serveur envoie des demandes d'écho ICMP (identiques à la commande ping) lors d'un sondage de Microsoft Active Directory.

Conditions préalables

Avant d'interroger un contrôleur de domaine, assurez-vous d'autoriser 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.
- Protocole LDAPS (Lightweight Directory Access Protocol over Secure Sockets)

  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

Sondage du contrôleur de domaine à l'aide du Serveur d'administration

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 **Sonder les domaines indiqués**, cliquez sur **Ajouter**, puis spécifiez l'adresse et les informations d'identification de l'utilisateur du contrôleur de domaine.
5. Si nécessaire, dans la fenêtre **Paramètres de sondage du contrôleur de domaine**, spécifiez la planification 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 Linux 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 interroger un contrôleur de domaine 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, le Serveur d'administration ou un 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` and `KLNAG_LDAP_SSL_CACERT`). Vous pouvez configurer les indicateurs de l'Agent d'administration à l'aide de klsclag comme décrit dans cet article.

La connexion initiale à un contrôleur de domaine se déroule comme suit :

1. Le Serveur d'administration ou un point de distribution 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, le Serveur d'administration ou un point de distribution tente de se connecter au contrôleur de domaine via une connexion TCP non chiffrée en utilisant SASL (DIGEST-MD5).

Authentification et connexion au contrôleur de domaine lors de l'authentification d'un utilisateur du domaine auprès du Serveur d'administration

Quand un utilisateur du domaine s'authentifie sur le Serveur d'administration, le Serveur d'administration identifie le protocole pour établir la connexion avec le contrôleur de domaine.

La connexion à un contrôleur de domaine se déroule comme suit :

1. Le Serveur d'administration tente de se connecter au contrôleur de domaine via LDAPS.

   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, une erreur de connexion au contrôleur de domaine se produit, et les autres protocoles de connexion ne sont pas utilisés.

Configuration des indicateurs

Vous pouvez utiliser l'utilitaire klscflag pour configurer les indicateurs.

Exécutez la ligne de commande, puis remplacez votre répertoire actuel par celui contenant l'utilitaire klscflag. Sur l'appareil du Serveur d'administration, l'utilitaire klsclag se trouve dans le répertoire d'installation. Le chemin d'installation par défaut est /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 Linux 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 Linux 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.

Si vous voulez sonder correctement un contrôleur de domaine Samba, vous devez spécifier le `netbios name` et les paramètres de `workgroup` dans le fichier `/etc/samba/smb.conf`.

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 Linux 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 s'afficher dans Kaspersky Security Center Web Console.

Pour éviter de conserver des données relatives à des machines virtuelles qui n'existent pas, Kaspersky Security Center Linux 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 le menu principal, accédez à **Découverte et déploiement** → **Déploiement et attribution** → **Paquets d'installation**.
2. Dans le menu contextuel du paquet d'installation de l'Agent d'administration, sélectionnez l'option **Propriétés**.

   La fenêtre **Propriétés** s'ouvre.
3. Dans la fenêtre **Propriétés**, 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.

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. Accédez à **Ressources (Appareils)** → **Règles de déplacement**.
2. Cliquez sur **Ajouter**.
3. Sous l'onglet **Conditions de la règle**, sélectionnez l'onglet **Machines virtuelles**.
4. Définissez la règle **Est une machine virtuelle** sur **Oui** et **Membre d'une Virtual Desktop Infrastructure** sur **Oui**.
5. Cliquez sur le bouton **Enregistrer**.

Bonnes pratiques de déploiement

Kaspersky Security Center Linux est une application distribuée. Kaspersky Security Center Linux 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.
- Kaspersky Security Center Web Console : l'outil de base pour l'administrateur. Vous pouvez installer Kaspersky Security Center Web Console soit sur le même appareil où le Serveur d'administration est installé, soit sur un autre appareil.
- 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 Linux dans le réseau de l'entreprise se réalise comme suit :

- Installation du Serveur d'administration
- Installation de Kaspersky Security Center Web Console 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

Kaspersky Security Center Linux est conçu pour l'exécution centralisée des tâches d'administration et de maintenance de base sur le réseau d'une organisation. L'application permet à l'administrateur d'accéder aux informations détaillées sur le niveau de sécurité du réseau de l'entreprise. Kaspersky Security Center Linux permet de configurer tous les modules de protection créés à l'aide des applications de Kaspersky.

Le Serveur d'administration de Kaspersky Security Center Linux 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 Linux 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 Linux 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 modules de Kaspersky Security Center Linux 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 Linux, 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.

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.

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

Lors du déploiement du Serveur d'administration, il est nécessaire de créer deux comptes non privilégiés. Les services inclus dans le Serveur d'administration fonctionneront sous ces comptes non privilégiés. Suivez le principe du moindre privilège lorsque vous accordez des droits et des autorisations aux comptes. Évitez d'inclure des comptes inutiles dans le groupe kladmins.

Vous devez également créer un compte interne dans le SGBD. Le Serveur d'administration utilise ce compte SGBD interne pour accéder au SGBD sélectionné.

L'ensemble des comptes requis et leurs privilèges dépendent du type de SGBD sélectionné et de la méthode de création de la base de données du Serveur d'administration.

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.

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.

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

Par défaut, l'utilisateur peut se connecter à Kaspersky Security Center Linux depuis n'importe quel appareil sur lequel Kaspersky Security Center Web Console est installé. 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.

Comptes et authentification

Avant d'exécuter les étapes ci-dessous, créez une copie de sauvegarde du Serveur d'administration de Kaspersky Security Center Linux 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 Linux propose une vérification en deux étapes pour les utilisateurs de Kaspersky Security Center Web Console 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, vous entrez votre nom d'utilisateur, votre mot de passe et un code de sécurité à usage unique supplémentaire. 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.

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.

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 16 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 Linux 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.

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.

Restrictions de l'attribution du rôle Administrateur primaire

L'utilisateur créé par l'utilitaire kladduser se voit attribuer le rôle Administrateur primaire dans la liste de contrôle d'accès (ACL) du Serveur d'administration. Nous vous recommandons d'éviter l'attribution du rôle Administrateur primaire à un grand nombre d'utilisateurs.

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 Linux 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.

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.

- Produits de sécurité recommandés. 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 produits 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 Kaspersky Security Center Web Console.

Par défaut, le Serveur d'administration utilise le port 13299 pour recevoir les connexions de Kaspersky Security Center Web Console. Nous vous recommandons de limiter le nombre d'appareils à partir desquels le Serveur d'administration peut être administré à l'aide de ce port.

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 dans un paquet d'installation, la clé de licence est accessible par tous les utilisateurs disposant de droits de lecture sur ce dossier (directement ou via le serveur Web intégré au Serveur d'Administration).

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'attribution 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.

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 Linux (Agent d'administration, Kaspersky Endpoint Security for Windows, Kaspersky Endpoint Security for Linux, 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

Nous vous recommandons vivement d'activer la protection par mot de passe pour empêcher les intrus de désactiver ou de désinstaller les applications de sécurité de Kaspersky. Sur les plateformes prenant en charge la protection par mot de passe, vous pouvez définir le mot de passe, par exemple, pour Kaspersky Endpoint Security, pour l'Agent d'administration et pour d'autres applications de Kaspersky. Après avoir activé la protection par mot de passe, nous vous recommandons de verrouiller les paramètres correspondants 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. L'utilitaire klmover se trouve 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.

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 Linux, vous ne pouvez pas supprimer l'Agent d'administration à l'aide de l'utilitaire klmover ou de la ligne 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.

L'activation de l'option **Utiliser un mot de passe de désinstallation** sur les appareils Windows 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 avec les contrôleurs de domaine et spécifiez des plages d'adresses IP pour découvrir 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.

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 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 d'audit

Kaspersky Security Center Linux 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.

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**

   Exécutez la commande suivante :

```
openssl genrsa 1024 > ca-key.pem

openssl req -new -x509 -nodes -days 365 -key ca-key.pem -config myssl.cnf > ca-cert.pem

openssl req -newkey rsa:1024 -days 365 -nodes -keyout server-key.pem -config myssl.cnf
> server-req.pem

openssl x09 -req -in server-req.pem -days 365 -CA ca-cert.pem -CAkey ca-key.pem -
set_serial 01 > server-cert.pem
```

2. **Créez un fichier indicateur de serveur**

   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. L'utilitaire klsclag se trouve dans le répertoire dans lequel le Serveur d'administration est installé. Le chemin d'installation par défaut est /opt/kaspersky/ksc64/sbin.

   ```
   klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_CA -v <path to ca-cert.pem> -t d
   ```

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**

   À l'aide de l'utilitaire klsclag, créez les indicateurs de serveur et indiquez comme valeurs le chemin d'accès aux fichiers de certificat :

   ```
   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
   ```

   L'utilitaire klsclag se trouve dans le répertoire dans lequel le Serveur d'administration est installé. Le chemin d'installation par défaut est /opt/kaspersky/ksc64/sbin.

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=".../mysqlcerts/ca-cert.pem"
   ```

```
ssl-cert=".../mysqlcerts/server-cert.pem"
ssl-key=".../mysqlcerts/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.

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**

   Exécutez les commande 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 mydb myuser 192.168.1.0/16 scram-sha-256
   ```

   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 la ligne de commande, puis remplacez votre répertoire actuel par celui contenant l'utilitaire klscflag. L'utilitaire klsclag se trouve dans le répertoire dans lequel le Serveur d'administration est installé. Le chemin d'installation par défaut est /opt/kaspersky/ksc64/sbin.

   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 la ligne de commande, puis remplacez votre répertoire actuel par celui contenant l'utilitaire klscflag. L'utilitaire klsclag se trouve dans le répertoire dans lequel le Serveur d'administration est installé. Le chemin d'installation par défaut est /opt/kaspersky/ksc64/sbin.

   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**

Préparatifs du déploiement

Cette section décrit les étapes à suivre absolument avant de pouvoir déployer Kaspersky Security Center Linux.

Planification du déploiement de Kaspersky Security Center Linux

Cette section contient des informations sur les options optimales de déploiement des modules de Kaspersky Security Center Linux 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 :

- Déploiement d'un système de protection à l'aide de 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 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 ne prend pas en charge le déploiement à l'aide des stratégies de groupe Microsoft Active Directory®.

À propos de la planification du déploiement de Kaspersky Security Center Linux dans le réseau de l'entreprise

Un serveur d'administration peut prendre en charge jusqu'à 50 000 appareils (avec PostgreSQL ou Postgres Pro comme SGBD). Si le total des appareils sur le réseau de l'entreprise est supérieur à 50 000, 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 Linux " reprend des descriptions détaillées des configurations typiques de Kaspersky Security Center Linux. 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 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 Linux

Cette section présente les configurations typiques suivantes pour le déploiement des modules de Kaspersky Security Center Linux 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 prendre en charge jusqu'à 50 000 appareils (avec PostgreSQL ou Postgres Pro comme SGBD). Envisagez la possibilité d'augmenter le nombre d'appareils administrés dans un avenir proche : il peut être utile de connecter un nombre légèrement inférieur d'appareils à un seul 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. Notez que 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 une tâche *Télécharger les mises à jour sur les stockages des points de distribution* pour les 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. Reportez-vous à la section suivante pour plus de détails : Activation d'un serveur push.

Choix d'un SGBD

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
MySQL (voir versions supportées)	Utilisez ce SGBD si vous prévoyez d'utiliser un seul Serveur d'administration pour moins de 20 000 appareils.
MariaDB (voir versions supportées)	Utilisez ce SGBD si vous prévoyez d'utiliser un seul Serveur d'administration pour moins de 20 000 appareils.
PostgreSQL, Postgres Pro (cf. les versions compatibles)	Utilisez ce SGBD si vous prévoyez d'utiliser un seul Serveur d'administration pour moins de 50 000 appareils.

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

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.

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.

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

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.

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 le Serveur d'administration effectue 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.

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.

Notez que Kaspersky Security Center Linux ne prend pas en charge le déploiement à l'aide des stratégies de groupe de Microsoft Windows.

Vous pouvez utiliser des points de distribution situés sur le réseau de l'organisation. 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 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).

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 distribuer des mises à jour qui peuvent être récupérées soit depuis le Serveur d'administration, soit depuis les serveurs Kaspersky. Dans ce dernier cas, configurez le téléchargement des mises à jour pour un point de distribution.

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=<soft_resource_limit>:<hard_resource_limit>`

   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_proc_id>/limits
   ```

   où le paramètre `<nagent_proc_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
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.

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.

Paramètres réseau pour l'interaction avec des services externes

Kaspersky Security Center Linux utilise les paramètres réseau suivants pour interagir avec les services externes.

Paramètres réseau

Paramètres réseau	Adresse	Description
Port : 443	activation-v2.kaspersky.com/activationservice/activationservice.svc	Activation des applications.

Protocole : HTTPS		
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 Linux 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.
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	Mise à jour des bases de données, des modules logiciels et des applications de Kaspersky.

	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	
Port : 443 Protocole : HTTPS	ds.kaspersky.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.
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 Linux 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 la ligne de commande, puis remplacez votre répertoire actuel par celui contenant l'utilitaire klscflag. L'utilitaire klsclag se trouve dans le répertoire dans lequel le Serveur d'administration est installé. Le chemin d'installation par défaut est /opt/kaspersky/ksc64/sbin.

2. Si vous souhaitez télécharger les mises à jour via le protocole HTTP, exécutez une des commandes suivantes sous le compte root :

   - Sur l'appareil sur lequel le Serveur d'administration est installé :

     ```
     klscflag -fset -pv klserver -s Updater -n DisableKLHttps -t d -v 1
     ```

   - Sur un point de distribution :

     ```
     klscflag -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 sous le compte root :

- Sur l'appareil sur lequel le Serveur d'administration est installé :

  ```
  klscflag -fset -pv klserver -s Updater -n DisableKLHttps -t d -v 0
  ```

- Sur un point de distribution :

  ```
  klscflag -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 Linux sur les appareils de l'entreprise commence d'habitude par l'installation de l'Agent d'administration sur ceux-ci.

Sous Microsoft Windows XP, l'Agent d'administration peut ne pas exécuter correctement les opérations suivantes : télécharger les mises à jour directement depuis les serveurs Kaspersky (en tant que point de distribution) et fonctionner en tant que serveur proxy KSN (en tant que point de distribution).

Déploiement initial

Pour administrer les appareils de l'entreprise, il faut installer l'Agent d'administration sur les appareils.

Les méthodes suivantes peuvent être utilisées pour l'installation initiale de l'Agent d'administration sur un appareil administré par Linux :

- 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.

Les méthodes suivantes peuvent être utilisées pour l'installation initiale de l'Agent d'administration sur un appareil administré par Windows :

- En exécutant la tâche d'installation à distance sur le point de distribution Windows.
- À l'aide du paquet Windows Installer (MSI) pour l'Agent d'administration, avec des outils tiers d'installation à distance d'applications.
- En exécutant le programme d'installation de l'application sur l'appareil administré.
- Via l'envoi aux utilisateurs des appareils de liens vers les paquets autonomes créés par Kaspersky Security Center Linux. Les paquets autonomes sont des modules exécutables qui contiennent la distribution des applications sélectionnés avec des paramètres prédéfinis.

Les méthodes suivantes peuvent être utilisées pour l'installation initiale de l'Agent d'administration sur un appareil administré par macOS :

- 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 Linux. 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 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 la connexion à distance avec l'appareil administré et de lancer l'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 Linux qu'à l'aide de la majorité des outils tiers. Ce moyen prévoit la création dans Kaspersky Security Center Linux 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).

- À partir du fichier d'archive ZIP, CAB, TAR ou TAR.GZ 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 Kaspersky Security Center Web Console lors de la création du paquet d'installation. En cas d'installation à distance des applications via les outils de Kaspersky Security Center Linux, 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 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 Linux dans un sous-dossier dédié du dossier partagé.

N'indiquez pas dans les paramètres des paquets d'installation les données des comptes utilisateur privilégiés.

Le déploiement à l'aide des stratégies de groupe de Microsoft Windows n'est pas pris en charge.

Directement après l'installation de Kaspersky Security Center Linux, 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.

À propos des tâches d'installation à distance des applications de Kaspersky Security Center Linux

Kaspersky Security Center Linux propose les méthodes d'installation à distance d'applications les plus diverses, présentées sous la forme de tâches d'installation à distance des applications. Vous pouvez créer une tâche d'installation à distance à la fois pour un groupe d'administration spécifié et pour des appareils spécifiques ou une sélection d'appareils (ces tâches apparaissent dans Kaspersky Security Center Web Console, 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 Linux.

   Pour capturer et installer des images de disque, utilisez des outils tiers disponibles dans l'organisation.

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 :

- 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 à partir des appareils.

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 dans Kaspersky Security Center Web Console comme un seul appareil. Ce problème survient parce que la procédure de clonage fait que les nouveaux appareils conservent des données internes identiques, ce qui permet au Serveur d'administration d'associer un appareil à son propre enregistrement dans Kaspersky Security Center Web Console.

Le *mode spécial de clonage de disque de l'Agent d'administration* vous permet d'éviter les problèmes liés à l'affichage incorrect des nouveaux appareils dans Kaspersky Security Center Web Console après le clonage. 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 un seul enregistrement dans Kaspersky Security Center Web Console. Une fois le clonage de l'image de l'appareil étalon terminé, les nouveaux appareils s'affichent correctement dans Kaspersky Security Center Web Console (sous les enregistrements individuels).

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 `klmover -cloningmode 1` dans la ligne de commande Windows.

   L'Agent d'administration passe au mode de clonage du disque.

3. Pour connaître l'état actuel du mode de clonage du disque, saisissez `klmover -cloningmode` dans la ligne de commande.

   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 `klmover -cloningmode 0` dans la ligne de commande.

Déploiement forcé à l'aide d'une tâche d'installation à distance des applications de Kaspersky Security Center Linux

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 Linux, 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. 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 Linux 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 Linux 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 Linux, 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 Linux

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 de tels cas, vous pouvez créer un fichier exécutable commun appelé *paquet d'installation autonome* via Kaspersky Security Center Linux, en utilisant les paquets d'installation avec les paramètres d'installation appropriés préparés par l'administrateur. Le paquet d'installation autonome se place dans le dossier partagé de Kaspersky Security Center Linux.

Kaspersky Security Center Linux 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 Linux. 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.

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 /var/opt/kaspersky/klnagent_srv/1093/.working/. 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 reçues par les points de distribution sont enregistrées dans le dossier /var/opt/kaspersky/klnagent_srv/1103/.

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 Kaspersky Security Center Web Console. La modification des paramètres du paquet d'installation dans Kaspersky Security Center Web Console oblige le Serveur d'administration à mettre à jour l'image du paquet dans le cache préparé pour le transfert sur les appareils.

Le serveur envoie des requêtes Echo ICMP (identiques à la commande ping) à l'appareil cible lors de l'installation à distance.

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 Linux, 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.

Surveillance du déploiement

Pour surveiller le déploiement de Kaspersky Security Center Linux et vous assurer qu'une application de sécurité et un Agent d'administration sont installés sur les appareils administrés, utilisez la fonctionnalité de surveillance et de reporting :

- Utilisez le widget de déploiement du tableau de bord pour surveiller le déploiement en temps réel.

- Utilisez des rapports pour obtenir des informations détaillées.

Configuration des paramètres des programmes d'installation

La section contient des informations sur les fichiers des programmes d'installation de Kaspersky Security Center Linux 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 modules Linux de Kaspersky Security Center pour les appareils Windows reposent sur la technologie 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.

Paramètres d'installation du Serveur d'administration

Le tableau ci-dessous décrit les propriétés que vous pouvez configurer lors de l'installation de Kaspersky Security Center Linux en mode silencieux.

Paramètres d'installation du Serveur d'administration en mode silencieux

Nom de la variable	Requis	Description	Valeurs possibles
`EULA_ACCEPTED`	Oui	Confirme que vous comprenez et acceptez les termes du Contrat de licence utilisateur final.	`1`
`PP_ACCEPTED`	Oui	Confirme que vous avez compris et accepté les conditions de la Politique de confidentialité.	`1`
`KLSRV_UNATT_SERVERADDRESS`	Oui	Le nom DNS ou l'adresse IP statique du Serveur d'administration.	Nom DNS ou adresse IP
`KLSRV_UNATT_PORT_SRV`	Non	Le numéro de port du Serveur d'administration. Facultatif, la valeur par défaut est 14000.	Numéro de port
`KLSRV_UNATT_PORT_SRV_SSL`	Non	Le numéro de port SSL du Serveur d'administration. Facultatif, la valeur par défaut est égale à 13000.	Numéro de port
`KLSRV_UNATT_PORT_KLOAPI`	Non	Le numéro de port du Serveur d'administration KLOAPI. Facultatif, la valeur par défaut est égale à 13299.	Numéro de port
`KLSRV_UNATT_PORT_GUI`	Non	Le numéro de port de l'interface graphique du Serveur d'administration. Facultatif, la valeur par défaut est égale à 14000.	Numéro de port
`KLSRV_UNATT_NETRANGETYPE`	Non	Le nombre approximatif d'appareils que vous entendez administrer. Facultatif, la valeur par défaut est égale à 1.	`1` pour 1 à 100 appareils en réseau. `2` pour 101 à 1 000 appareils en réseau. `3` pour plus de 1 000 appareils en réseau.

`KLSRV_UNATT_DBMS_TYPE`	Oui	Le type de système de gestion de base de données : MySQL (MariaDB) ou Postgres.	`mysql`
			ou
			`postgres`

`KLSRV_UNATT_DBMS_INSTANCE`	Oui	L'adresse IP du serveur de base de données.	Adresse IP

KLSRV_UNATT_DBMS_PORT	Oui	Le port du serveur de base de données. La valeur par défaut pour MySQL (MariaDB) est 3306 ; la valeur par défaut pour Postgres est 5432.	3306 ou 5432
KLSRV_UNATT_DB_NAME	Oui	Le nom de la base de données.	kav
KLSRV_UNATT_DBMS_LOGIN	Oui	Le nom d'utilisateur qui a accès à la base de données.	
KLSRV_UNATT_DBMS_PASSWORD	Oui	Le mot de passe d'un utilisateur qui a accès à la base de données.	
KLSRV_UNATT_KLADMINSGROUP	Oui	Le nom du groupe de sécurité pour les services.	kladmins
KLSRV_UNATT_KLSRVUSER	Oui	Le nom du compte pour lancer le service Serveur d'administration. Le compte doit être membre du groupe de sécurité spécifié dans la variable KLSRV_UNATT_KLADMINSGROUP.	ksc
KLSRV_UNATT_KLSVCUSER	Oui	Le nom du compte pour lancer d'autres services. Le compte doit être membre du groupe de sécurité spécifié dans la variable KLSRV_UNATT_KLADMINSGROUP.	ksc
Si le Serveur d'administration doit être déployé en tant que cluster de basculement Kaspersky Security Center Linux, le fichier de réponses doit inclure les variables supplémentaires suivantes :			
KLFOC_UNATT_NODE	Oui	Le numéro du nœud (1 ou 2).	1 ou 2
KLFOC_UNATT_STATE_SHARE_MOUNT_PATH	Oui	Point de montage du partage de l'état.	
KLFOC_UNATT_DATA_SHARE_MOUNT_PATH	Oui	Point de montage du partage de données.	
KLFOC_UNATT_CONN_MODE	Oui	Le mode de connectivité du cluster de basculement.	VirtualAdapter ou ExternalLoadBalancer
Si la variable KLFOC_UNATT_CONN_MODE a la valeur VirtualAdapter, le fichier de réponses doit inclure les variables supplémentaires suivantes :			
KLFOC_UNATT_CONN_MODE_VA_NAME	Oui	Nom de la carte réseau virtuelle.	
KLFOC_UNATT_CONN_MODE_VA_IPV4	L'une de ces variables est obligatoire	Adresse IP de la carte réseau virtuelle.	Adresse IP
KLFOC_UNATT_CONN_MODE_VA_IPV6		Adresse IPv6 de la carte réseau virtuelle.	Adresse IPv6

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.
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	• 1 : activer.

	Infrastructure (VDI)	• 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 Linux 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 Linux 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 Linux 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 Kaspersky Security Center Web Console.

Prise en charge des machines virtuelles dynamiques

Kaspersky Security Center Linux 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 Linux 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.

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 Linux 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 Linux.

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 Linux, les seuls scénarios critiques sont ceux où un logiciel tiers sur les appareils dotés de l'Agent d'administration touche le répertoire /var/opt/kaspersky/klnagent. 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 Linux, 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 Linux, 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 répertoire /var/opt/kaspersky/klnagent 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 Linux prend aussi en charge la possibilité d'installation locale des applications à l'aide du paquet d'installation autonome. Kaspersky Security Center Linux ne prend pas en charge l'installation de toutes les applications de Kaspersky.

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.

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 version>.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 version>.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 version>.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 version>_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 version>_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 version>_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 de l'Agent d'administration pour Windows en mode interactif

Pour installer l'Agent d'administration sur l'appareil localement, procédez comme suit :

1. Sur l'appareil, exécutez le fichier ksc_<version number>.<build number>_full_<localization language>.exe dans le paquet de distribution téléchargé à partir d'Internet.

   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 15** pour démarrer l'Assistant d'installation de l'Agent d'administration. Suivez les instructions de l'assistant.

Pendant le fonctionnement de l'Assistant d'installation, vous pouvez configurer les paramètres avancés de l'Agent d'administration (cf. ci-dessous).

3. Pour utiliser l'appareil en tant que passerelle des connexions pour le groupe d'administration choisi, choisissez l'option **Utiliser l'Agent d'administration en tant que passerelle de connexion en DMZ** dans la fenêtre **Passerelle de connexion**.

4. Pour configurer l'Agent d'administration lors de l'installation sur une la machine virtuelle, procédez comme suit :

   a. Si vous avez l'intention de créer des machines virtuelles dynamiques au départ de l'image de la machine virtuelle, activez le mode dynamique de l'Agent d'administration pour Virtual Desktop Infrastructure (VDI). Pour ce faire, dans la fenêtre **Paramètres avancés** de l'Assistant d'installation, sélectionnez l'option **Activer le mode dynamique pour VDI**.

      Passez cette étape si vous n'avez pas l'intention de créer des machines virtuelles dynamiques au départ de l'image de la machine virtuelle.

   b. Optimisez le fonctionnement de l'Agent d'administration pour le VDI. Pour ce faire, dans la fenêtre **Paramètres avancés** de l'Assistant d'installation, sélectionnez l'option **Optimiser les paramètres pour VDI**.

      Cela désactive la recherche de la présence de vulnérabilités dans les fichiers exécutables lors du lancement de l'appareil. De même, le transfert des informations suivantes vers le Serveur d'administration sera aussi désactivé :

      - Registre du matériel
      - Sur les applications installées sur l'appareil
      - Sur les mises à jour de Microsoft Windows qu'il faut installer sur l'appareil client local
      - Sur les vulnérabilités logicielles détectées sur l'appareil client local

      Par la suite, vous pourrez activer le transfert de ces informations dans les propriétés de l'Agent d'administration ou dans les paramètres de la stratégie de l'Agent d'administration.

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. 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 pour Windows 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 Linux, dans le dossier Packages\NetAgent\exec.

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.

Installation des applications en mode silencieux

Afin d'effectuer l'installation de l'application en mode silencieux, procédez comme suit :

1. Dans le menu principal, accédez à **Découverte et déploiement** → **Déploiement et attribution** → **Paquets d'installation**.

2. Cochez la case en regard du paquet d'installation de l'application nécessaire 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 Linux. 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.

Pour installer l'application à l'aide du paquet d'installation autonome, procédez comme suit :

1. Dans le menu principal, accédez à **Découverte et déploiement** → **Déploiement et attribution** → **Paquets d'installation**.

2. Cochez la case en regard du paquet d'installation de l'application nécessaire, puis cliquez sur le bouton **Déployer** .

3. Dans la fenêtre qui s'ouvre, sélectionnez **Utilisation d'un paquet autonome** , puis cliquez sur le bouton **Suivant** .

   L'assistant de création du paquet d'installation autonome démarre. Naviguez dans les fenêtres de l'Assistant à l'aide du bouton **Suivant**.

4. Sélectionnez l'option **Créer un paquet d'installation autonome** .

5. Indiquez si les appareils doivent être déplacés vers un groupe d'administration après l'installation de l'agent d'administration.

6. A la dernière étape de l'Assistant, sélectionnez une méthode pour transférer le paquet d'installation autonome sur l'appareil client, puis cliquez sur le bouton **Terminer** pour quitter l'Assistant.

7. Envoyez le paquet d'installation autonome de l'application à l'appareil client.

8. 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. 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 le nom du paquet d'installation de l'Agent d'administration.

La fenêtre des propriétés du paquet d'installation de l'Agent d'administration s'ouvre.

Les paramètres d'un paquet d'installation réseau sont regroupés dans les onglets suivants :

- Onglet **Général**

  Cet onglet affiche les informations suivantes 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

- Onglet **Paramètres**

  Cet onglet permet de configurer les paramètres nécessaires afin de garantir le fonctionnement de l'Agent d'administration tout de suite après son installation.

  - Section **Paramètres**

    - 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.

- **Utiliser un mot de passe de désinstallation**

  Si cette option est activée, vous pouvez 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.

- **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, Kaspersky Security Center Web Console, le Serveur des appareils mobiles Exchange et le Serveur MDM iOS téléchargés sont installés automatiques.

  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.

- Section **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 :

  - **Adresse du Serveur d'administration**

    Adresse de l'appareil sur lequel est installé le Serveur d'administration.

- **Numéro de 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 **Sélectionner le fichier du certificat**.

  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 d'administration**.

  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.

  Cette option est Inactif 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 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.

- **Ne pas utiliser de serveur proxy**

  Si l'option est activée, la connexion directe est utilisée pour connecter l'appareil au Serveur d'administration.

- **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.

- 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.

  Cette option est disponible uniquement pour les paquets d'installation d'Agent d'administration destinés aux appareils exécutant Windows.

- Section **Avancé**

  Dans cette section, vous pouvez configurer comment utiliser la passerelle de connexion.

  Dans le groupe de paramètres **Utiliser l'Agent d'administration en tant que passerelle de connexion dans la zone démilitarisée**, vous pouvez configurer la méthode de connexion entre un appareil et le Serveur d'administration :

  - Utiliser l'Agent d'administration en tant que passerelle de connexion en DMZ

    Si cette option est activée, l'Agent d'administration est utilisé 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

    Si cette option est activée, la connexion au Serveur d'administration est établie 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**.

  Dans le groupe de paramètres **Utilisation de Virtual Desktop Infrastructure (VDI)**, vous pouvez configurer la connexion pour Virtual Desktop Infrastructure (VDI) si votre réseau inclut des machines virtuelles :

  - 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.

- Section **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.

  Les règles de marquage automatique ne s'appliquent pas aux paquets d'installation d'Agents d'administration destinés aux appareils exécutant Linux et macOS.

- Onglet **Paquets autonomes**

  Sous cet onglet, vous pouvez effectuer les opérations suivantes :

  - Affichez la liste des paquets d'installation autonomes disponibles.
  - 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**.

- Onglet **Historique des révisions**

  Cet onglet 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.

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. Si la planification de la tâche d'analyse de groupe définie automatiquement ne convient pas à votre entreprise, vous devez configurer manuellement la planification qui vous convient le mieux pour cette tâche sur la base des règles de travail adoptées dans l'entreprise.

Par exemple, 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 l'entreprise sont désactivés les vendredis à 18:30, la tâche d'analyse de l'appareil ne sera jamais lancée. Dans ce cas, vous devez configurer la tâche d'analyse de groupe manuellement.

Administration des appareils clients

Kaspersky Security Center Linux 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.

  - **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**.

  - **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 Linux.

- 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 de serveurs push, qui fournissent une telle connexion.

  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

    Groupe de travail qui contient l'appareil.

  - Nom DNS

    Nom du domaine DNS de l'appareil client.

  - Nom NetBIOS

    Nom de l'appareil client.

  - **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.

    Les fichiers peuvent être chiffrés uniquement sur les appareils administrés sur lesquels Kaspersky Endpoint Security for Windows est installé.

- 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 Linux.

- 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, 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

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.

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 : 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 plus, les règles de déplacement de l'appareil peuvent être créées explicitement par l'administrateur de Kaspersky Security Center Linux, dans la section **Ressources (Appareils)** → **Règles de déplacement**.

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 un appareil a déjà été déplacé par cette règle, la règle ne le déplacera plus jamais, même si vous remettez manuellement l'appareil dans le groupe des appareils non attribués. 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 Linux (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.

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.

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 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 Linux, 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.

- 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** ou **Serveur d'administration de Kaspersky Security Center 15**.

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 du contrôleur 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 du contrôleur 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.

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 DNS de l'appareil.

    Le champ du nom de l'appareil ne doit pas contenir d'espaces, de retours arrière, ni aucun des 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, de retours arrière, ni aucun des 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 **Ressources (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 **Ressources (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.

À propos des clusters et des groupes des serveurs

Kaspersky Security Center Linux 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 Linux 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 Linux 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.

Réglage des points de distribution et des passerelles de connexion

La structure des groupes d'administration dans Kaspersky Security Center Linux 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*.

- 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 :

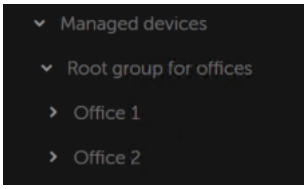
- Construction de la structure des groupes d'administration en tenant compte de la topologie du réseau. La structure des groupes d'administration ne doit pas obligatoirement refléter exactement la topologie du réseau. Il suffit que quelques groupes d'administration correspondent à des parties du réseau 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.

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.

Assignation automatique des points de distribution

Nous vous recommandons d'assigner les points de distribution automatiquement. Dans ce cas, Kaspersky Security Center Linux 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 Linux 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 Linux 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 Linux 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 Linux, 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 les groupes d'administration auxquels le point de distribution distribuera les mises à jour.
- 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 une 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.

    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.

  - **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.

- Dans la section **Passerelle de connexion**, vous pouvez configurer le point de distribution comme passerelle de 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 le sonage du contrôleur de domaine par le point de distribution.

  - Sondage du contrôleur de domaine

    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**

- Configurez l'interrogation des plages IP par le point de distribution.

  - **Sondage des 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**.

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.

Activation d'un serveur push

Dans Kaspersky Security Center Linux, 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.

À propos des états des appareils

Kaspersky Security Center Linux 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 statut à un appareil, Kaspersky Security Center Linux tient compte de l'indicateur de visibilité de l'appareil sur le réseau (voir le tableau ci-dessous). Si Kaspersky Security Center Linux 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*
- *Avertissement* ou *Avertissement/Visible*
- *OK* ou *OK/Visible*

Le tableau ci-dessous reprend les conditions d'attribution de l'état *Critique* ou *Avertissement* 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 d'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.
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.	Plus de 0 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.
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 Linux 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 *Avertissement*. 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 jour Kaspersky Security Center Linux à partir de la version précédente, les valeurs de la condition **Les bases sont dépassées** pour attribuer l'état à *Critique* ou *Avertissement* ne changent pas.

Lorsque Kaspersky Security Center Linux attribue un état 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*.

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 Linux 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 Linux 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

Si l'option est activée, la condition de sélection définie sera inversée. Tous les appareils qui ne correspondent pas à la condition feront partie de la sélection.

Cette option est Inactif par défaut.

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

  Affiche tous les appareils inclus dans le groupe de travail spécifié.

- 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 des expressions telles que **SUSE Linux Enterprise Server 12** ou **SUSE Linux Enterprise Server 15**, vous pouvez saisir **SUSE Linux Enterprise Server 1?**.

    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.

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 (*Aucune donnée de l'appareil, 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 (*Aucune donnée de l'appareil*, *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 (*Aucune donnée de l'appareil, 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 (*Aucune donnée de l'appareil, Arrêté(e), En cours de démarrage, Suspendu(e), En cours d'exécution, Échec*).

La sous-section **Problèmes ayant un impact 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**

  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**

  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.

- **Statut 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.

- **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 Linux dans la sélection d'appareils :

- **Oui**. L'application ajoute les appareils administrés via Kaspersky Security Center Linux à la sélection d'appareils.
- **Non**. L'application ajoute les appareils non administrés via Kaspersky Security Center Linux à la sélection d'appareils.
- **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.

- 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.

- Doit être exclu

  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 Linux 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 Linux permet de désigner les *tags* pour les appareils. Un tag est une valeur de chaîne 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. 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 Linux 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. Par exemple, vous pouvez configurer une règle qui attribuera le tag `[CentOS]` à tous les appareils exécutant le système d'exploitation CentOS. Vous pouvez utiliser ensuite cette balise lors de la création d'une sélection d'appareils ; cela vous aidera à trier tous les appareils fonctionnant sous CentOS et à leur attribuer une tâche.

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

Vous ne pouvez supprimer que les tags attribués manuellement.

Pour supprimer un tag attribué manuellement à l'appareil, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Tags** → **Tags de l'appareil**.
   La liste des tags s'affiche.
2. 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.

Lorsque vous supprimez un tag attribué à un appareil par une règle d'attribution automatique de tags, la règle n'est pas supprimée et le tag est attribué à un nouvel appareil lorsqu'il répond pour la première fois aux conditions de la règle. Si vous supprimez une règle d'attribution automatique de tags, le tag spécifié dans les conditions de la règle sera supprimé de tous les appareils auxquels il a été attribué, mais n'est pas supprimé de la liste des tags. Le cas échéant, vous pouvez supprimer le tag manuellement de la liste.

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.

   La liste des appareils reprend uniquement les appareils auxquels un tag a été attribué.

Pour revenir à la liste des tags de l'appareil, cliquez sur le bouton **Retour** de votre navigateur.

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.

Vous pouvez attribuer un autre tag à l'appareil ou retirer un tag déjà attribué. Vous pouvez aussi afficher tous les tags de l'appareil qui existent sur le Serveur d'administration.

Vous pouvez également afficher les balises attribuées à un appareil dans la ligne de commande à l'aide de l'utilitaire klscflag.

Pour afficher les balises attribuées à un appareil dans la ligne de commande, exécutez la commande suivante :

```
/opt/kaspersky/klnagent64/sbin/klscflag -ssvget -pv 1103/1.0.0.0 -s
KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -svt ARRAY_T -ss "|ss_type =
\"SS_PRODINFO\";"
```

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 de l'appareil (par exemple, nom DNS de l'appareil, appartenance de l'appareil 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 Linux, 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.
- **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 plusieurs tags à votre appareil à l'aide de l'utilitaire klscflag, procédez comme suit :

1. Exécutez l'invite de commande sous un compte disposant des privilèges d'administrateur, puis remplacez votre répertoire actuel par celui contenant l'utilitaire klscflag. L'utilitaire klsclag se trouve dans le répertoire dans lequel l'Agent d'administration est installé. Le répertoire d'installation par défaut est /opt/kaspersky/klnagent64/sbin/.

2. Saisissez l'une des commandes suivantes :

   - Pour attribuer un ensemble de balises :

     ```
     /opt/kaspersky/klnagent64/sbin/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 :

     ```
     /opt/kaspersky/klnagent64/sbin/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 :

     ```
     /opt/kaspersky/klnagent64/sbin/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 :

     ```
     /opt/kaspersky/klnagent64/sbin/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. Pour 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.

Chiffrement et protection des données

Le chiffrement des données réduit le risque de fuite involontaire de données sensibles et d'entreprise en cas de vol ou de perte de votre ordinateur portable ou de votre disque dur. De plus, le chiffrement des données vous permet d'interdire l'accès aux utilisateurs et aux applications non autorisés.

Vous pouvez utiliser la fonction de chiffrement des données si votre réseau comprend des appareils administrés Windows sur Kaspersky Endpoint Security for Windows est installé. Dans ce cas, sur les appareils exécutant le système d'exploitation Windows, vous pouvez gérer les types de chiffrement suivants :

- Chiffrement de disque BitLocker
- Kaspersky Disk Encryption

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.

Pour configurer le chiffrement, définissez la stratégie Kaspersky Endpoint Security for Windows dans Kaspersky Security Center Linux. 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.

L'administration du chiffrement pour une hiérarchie de Serveurs d'administration n'est actuellement pas disponible dans Web Console. Utilisez le Serveur d'administration principal pour administrer les appareils chiffrés.

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.

Consultation de la liste des disques chiffrés

Dans Kaspersky Security Center Linux, vous pouvez afficher les détails des disques chiffrés et des appareils chiffrés au niveau du disque. 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 Linux 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 Kaspersky Endpoint Security for Windows.
6. Suivez les instructions fournies dans l'aide de Kaspersky Endpoint Security for Windows (voir les instructions pour Kaspersky Security Center Web Console 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.

Modification du Serveur d'administration pour les appareils clients

Vous pouvez remplacer le Serveur d'administration par un autre pour des appareils clients spécifiques. Pour ce faire, utilisez 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. Connectez-vous au Serveur d'administration, qui administre les appareils.
2. Créez une tâche de modification du Serveur d'administration.

   Ceci permet de lancer l'Assistant de création d'une tâche. Suivez les instructions de l'assistant. Dans la fenêtre **Nouvelle tâche** de l'Assistant d'ajout de tâche, sélectionnez l'application **Kaspersky Security Center 15** et le type de tâche **Modification du Serveur d'administration**. Ensuite, indiquez les appareils pour lesquels vous souhaitez modifier le Serveur d'administration :

   - **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 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.

3. 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.

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.

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.

Envoi d'un message aux utilisateurs des appareils

Pour envoyer un message aux utilisateurs des appareils, 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 la liste déroulante **Type de tâche**, sélectionnez l'option **Envoyer le message à l'utilisateur**.
4. Sélectionnez une option pour spécifier le groupe d'administration, la sélection d'appareils ou les appareils auxquels la tâche s'applique.
5. Lancez la tâche créée.

A la fin du fonctionnement de la tâche, le message créé sera envoyé aux utilisateurs des appareils sélectionnés. La tâche **Envoyer le message à l'utilisateur** est disponible uniquement sur les appareils qui tournent sous Windows.

Démarrage, arrêt et redémarrage à distance des appareils clients

Kaspersky Security Center Linux 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. 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. À partir de la liste déroulante **Type de tâche**, sélectionnez **Administrer les appareils**.

4. Sélectionnez une option pour spécifier le groupe d'administration, la sélection d'appareils ou les appareils auxquels la tâche s'applique.

5. Sélectionnez la commande (activer, désactiver ou redémarrer).

6. Si nécessaire, configurez les paramètres suivants pour les commandes d'arrêt et de redémarrage :

   - Activez le commutateur **Confirmer l'action auprès de l'utilisateur** pour spécifier le message d'invite de l'utilisateur et les intervalles de temps après lesquels vous souhaitez répéter l'invite et redémarrer les appareils.

   - Cochez la case **Délai d'attente avant la fermeture forcée des applications dans les sessions bloquées (min)** et définissez le délai.

   Ces paramètres sont applicables aux appareils clients Windows uniquement. Les appareils Linux seront redémarrés ou éteints immédiatement après la fin de la tâche.

7. Lancez la tâche créée.

Après la fin du fonctionnement de la tâche, la commande (démarrage, arrêt, redémarrage) sera exécutée sur les appareils sélectionnés.

Administration des groupes d'administration

Cette section contient les informations sur le travail avec les groupes d'administration.

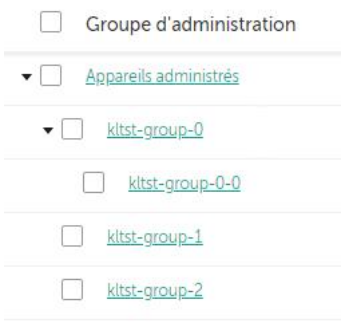
Avec les groupes d'administration, vous pouvez effectuer les actions suivantes :

- 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 disposez de l'autorisation **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

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.

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.

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. Dans le menu principal, accédez à **Ressources (Appareils)** → **Hiérarchie des groupes**, puis cliquez sur le nom du groupe d'administration requis.

2. Dans la fenêtre des propriétés qui s'ouvre, sélectionnez l'onglet **Installation automatique**.

3. Sélectionnez les paquets d'installation des applications à installer sur les appareils, puis cliquez sur le bouton **Enregistrer**.

   Si vous sélectionnez plusieurs paquets d'installation de la même application qui diffèrent uniquement par leurs versions, le paquet d'installation avec la dernière version est enregistré.

Après avoir sélectionné les paquets d'installation, un groupe de tâches pour l'installation des applications sur les appareils du groupe d'administration est créé pour chacune des applications. Ces tâches sont lancées sur les appareils clients juste après avoir été ajoutées au groupe d'administration.

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 ni déplacer le groupe d'**appareils administrés**.

Pour déplacer un groupe d'administration vers un autre niveau de la hiérarchie des groupes d'administration :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Hiérarchie des groupes**, puis cochez la case en regard du groupe d'administration que vous souhaitez déplacer.

2. Cliquez sur le bouton **Déplacer** dans la barre d'outils.

3. Dans la fenêtre qui s'ouvre, sélectionnez l'endroit où vous souhaitez déplacer le groupe d'administration et cliquez sur le bouton **Déplacer**.

   La fenêtre est fermée et le groupe d'administration est déplacé vers un autre niveau de la hiérarchie des groupes.

Suppression des groupes d'administration

Si vous supprimez un groupe d'administration contenant des Serveurs d'administration secondaires, des groupes imbriqués, des appareils clients, des tâches de groupe ou des stratégies créées pour ce groupe, tous ces éléments seront également supprimés.

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 d'administration, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Hiérarchie des groupes**, puis cochez la case en regard du groupe d'administration que vous souhaitez supprimer.

2. Cliquez sur le bouton **Supprimer** dans la barre d'outils.

   Le groupe d'administration est supprimé.

Déploiement des applications Kaspersky

Cette section explique comment déployer les applications Kaspersky sur les appareils clients dans votre organisation administrés par Kaspersky Security Center Web Console.

Scénario : déploiement des applications Kaspersky

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 Linux
- Kaspersky Endpoint Security for Windows

Étapes

Le déploiement des applications Kaspersky se déroule par étapes :

1. **Téléchargement du plug-in d'administration Web 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 les plug-ins manuellement.

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 Web 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 Linux sur certains appareils, par exemple sur les appareils des employés distants, vous pouvez créer des packages 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.

   Vous pouvez également télécharger les paquets de distribution de l'Agent d'administration et des applications de sécurité sur le site Internet de Kaspersky. Si l'installation à distance des applications n'est pas possible pour une raison quelconque, vous pouvez utiliser les paquets de distribution téléchargés pour installer les applications localement.

3. **Création, configuration et exécution d'une tâche d'installation à distance**

   Cette étape fait partie de l'Assistant de déploiement de la protection. 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.

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.

4. **Création et configuration des tâches**

   La tâche de *mise à jour* de Kaspersky Endpoint Security 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.)

5. **Création des stratégies**

   Créez la stratégie pour Kaspersky Endpoint Security manuellement ou via 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.

6. **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 d'administration pour les applications de Kaspersky

Pour déployer une application Kaspersky, telle que Kaspersky Endpoint Security for Linux ou Kaspersky Endpoint Security for Windows, vous devez ajouter et installer le plug-in Web d'administration de l'application.

Pour télécharger un plug-in Web d'administration pour une applications de Kaspersky, procédez comme suit :

1. Dans le menu principal, accédez à **Paramètres** → **Plug-ins Web**.
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 for Linux) 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 Web d'administration est téléchargé avec la configuration par défaut et s'affiche dans la liste des plug-ins Web d'administration.

Vous pouvez ajouter des plug-ins et mettre à jour les plug-ins téléchargés à partir d'un fichier. Vous pouvez télécharger les plug-ins Web d'administration à partir du site de Kaspersky.

Pour télécharger ou mettre à jour le plug-in Web à partir d'un fichier :

1. Dans le menu principal, accédez à **Paramètres** → **Plug-ins Web**.
2. Indiquez le fichier du plug-in et la signature du fichier :
   - 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 Web d'administration est téléchargé à partir du fichier et s'affiche dans la liste des plug-ins Web 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 Linux.

4. Cliquez sur le nom d'un paquet d'installation, par exemple, Kaspersky Endpoint Security for Linux.

   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.

Création de paquets d'installation à partir d'un fichier

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.

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**.

5. Dans la fenêtre qui s'ouvre, choisissez un fichier 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).

   Le téléchargement du fichier vers le Serveur d'administration démarre.

6. Si vous avez indiqué un fichier d'une application Kaspersky, vous serez peut-être invité à lire et à accepter le Contrat de licence utilisateur final (CLUF) de l'application. Pour continuer, vous devez accepter le CLUF. Sélectionnez l'option **Accepter les termes et les conditions de ce Contrat de licence utilisateur final** uniquement si vous avez lu, compris et accepté intégralement les conditions du CLUF.

   De plus, vous pouvez être invité à lire et à accepter la Politique de confidentialité. Pour continuer, vous devez accepter la Politique de confidentialité. Sélectionnez l'option **J'accepte la Politique de confidentialité** 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.

7. 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.

8. 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 les paramètres de ligne de commande.

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 qui peut être stocké sur un Serveur Internet, 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 Linux. Vous pouvez créer des paquets d'installation autonomes pour toutes les applications Kaspersky que pour les applications tierces. 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 tiers.

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.

   Cette option est activée par défaut. Il est recommandé 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 sélectionnée par défaut. Si vous ne souhaitez pas déplacer l'appareil client vers un groupe d'administration après l'installation de l'Agent d'administration, ne modifiez pas l'option.

   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.

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 Linux (généralement, /opt/kaspersky/ksc64/sbin).
3. Selon le type d'installation du Serveur d'administration, saisissez une des commandes suivantes sous le compte root :

   - Installation locale normale :

     ```
     klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v <nombre d'octets>
     ```

   - Installation sur le cluster de basculement Kaspersky Security Center Linux :

     ```
     klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v <nombre d'octets> --stp klfoc
     ```

   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.

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. 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.

2. 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.

3. Définissez la valeur de la variable d'environnement KLAUTOANSWERS dans l'environnement root ou utilisateur en entrant le nom complet du fichier de réponse (y compris le chemin d'accès), par exemple, comme suit :

   ```
   export KLAUTOANSWERS=/tmp/nagent_install/answers.txt
   ```

4. Créez le fichier de réponse (au format TXT) dans le répertoire que vous avez indiqué dans la variable d'environnement. 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.

5. Installer l'Agent d'administration :

- Pour installer l'Agent d'administration à partir d'un paquet RPM dans un système d'exploitation 32 bits, exécutez la commande suivante :
  `# rpm -i klnagent-<numéro de version>.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 :
  `# rpm -i klnagent64-<numéro de version>.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 :
  `# rpm -i klnagent64-<build number>.aarch64.rpm`
- Pour installer l'Agent d'administration à partir d'un paquet DEB dans un système d'exploitation 32 bits, exécutez la commande suivante :
  `# apt-get install ./klnagent_<build number>_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 :
  `# apt-get install ./klnagent64_<build number>_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 :
  `# apt-get install ./klnagent64_<build number>_arm64.deb`

Pour installer l'Agent d'administration dans l'environnement utilisateur, ajoutez `sudo -E` avant la commande. Par exemple, pour installer l'Agent d'administration à partir d'un paquet RPM sur un système d'exploitation 32 bits, exécutez la commande suivante :

`$ sudo -E rpm -i klnagent-<numéro de version>.i386.rpm`

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.

Conditions préalables :

- Assurez-vous que l'appareil sur lequel vous voulez installer l'Agent d'administration pour Linux fonctionne sur une des distributions Linux supportées.
- Téléchargez le fichier d'installation nécessaire de l'Agent d'administration sur le site Internet de Kaspersky.

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/ksc64/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 Kaspersky Security Center Linux 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.

6. Effectuez les étapes de préparation communes à tout appareil Linux.

L'appareil est préparé. Vous pouvez maintenant procéder à l'installation de l'Agent d'administration.

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**.

Propagation des paquets d'installation sur les Serveurs d'administration secondaires

Kaspersky Security Center Linux permet de créer des paquets d'installation pour des applications de Kaspersky et des applications tierces, ainsi que de diffuser des paquets d'installation sur les appareils clients et d'installer les applications à partir de 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 **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.

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 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
2. 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 sudo `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`.

3. Ouvrez le fichier `/etc/systemd/logind.conf`, puis effectuez l'une des opérations suivantes :

- Spécifiez " non " 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/< username >/.bashrc`, où `< username >` est le compte à utiliser pour la connexion de l'appareil via SSH.

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 appliquer le paramètre modifié, redémarrez l'appareil Linux ou exécutez la commande suivante :

```
$ sudo systemctl restart systemd-logind.service
```

4. 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.

5. 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.

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. Téléchargez le paquet d'installation de l'Agent d'administration via l'interface de l'application ou depuis le site Internet de Kaspersky.

c. 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`.

Installation des applications à l'aide de la tâche d'installation à distance

Kaspersky Security Center Linux 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 :

- **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.

- **Définir les adresses des appareils manuellement ou les importer à partir d'une liste**. Vous pouvez définir 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 désigner une sélection créée par défaut ou votre sélection personnelle. Vous pouvez uniquement sélectionner jusqu'à 1 000 appareils.

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 Linux.

Installation d'une application à distance

Cette section contient des informations sur l'installation à distance d'une application sur les appareils d'un groupe d'administration, les appareils avec des adresses spécifiques ou une sélection d'appareils.

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 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.

Le seul moyen d'installer une application pour Windows (y compris l'Agent d'administration pour Windows) sur un appareil sur lequel l'Agent d'administration n'est pas installé est d'utiliser un point de distribution Windows. Par conséquent, lorsque vous installez une application Windows :

- Sélectionnez cette option.
- Assurez-vous qu'un point de distribution est attribué aux appareils clients cibles.
- Assurez-vous que le point de distribution est basé sur Windows.

- **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 Linux 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*.

- 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 Linux 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 Linux 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.

- **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**

     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.

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 Linux 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 Linux. 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 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 des applications** → **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 Linux 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 Linux 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 Linux 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**.

Remplacement d'application de sécurité d'éditeurs tiers

Pour installer des applications de protection de Kaspersky à l'aide des outils de Kaspersky Security Center Linux, il faut peut-être supprimer tout logiciel tiers incompatible avec l'application à installer. Kaspersky Security Center Linux offre plusieurs méthodes pour retirer des applications tiers.

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 l'Assistant de déploiement de la protection. Si cette option est activée, Kaspersky Security Center Linux supprime les applications incompatibles avant d'installer une application de sécurité sur un appareil administré.

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 d'applications ou de mises à jour logicielles à distance

Vous pouvez supprimer des applications ou des mises à jour logicielles sur les appareils administrés qui exécutent Linux à distance uniquement à l'aide de l'Agent d'administration.

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. Dans la liste déroulante **Application**, sélectionnez Kaspersky Security Center.

4. Dans la liste **Type de tâche**, sélectionnez le type de tâche **Désinstallation à distance d'une 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.

   Accédez à l'étape suivante de l'Assistant.

7. 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 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 Linux 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 Linux 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 Linux 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.

8. 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 du système d'exploitation Linux.

  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**

  L'option est obsolète. Utilisez plutôt l'option **En utilisant l'Agent d'administration** ou **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 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 Linux ne parvient pas à désinstaller une application sur un appareil administré conformément au nombre d'exécutions du programme d'installation paramétré, Kaspersky Security Center Linux 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 Linux 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 Linux 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.

Accédez à l'étape suivante de l'Assistant.

9. 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.)**
  - **Redémarrer le système au bout de (min.)**

- 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.

Accédez à l'étape suivante de l'Assistant.

10. 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 Linux 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 Linux. 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>"
  ```

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 sous **Ressources (Appareils)** → **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, l'application sélectionnée est 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.

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, 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.

Après avoir préparé l'appareil SUSE Linux Enterprise Server 15, déployez et installez l'Agent d'administration.

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 :

  - L'option **Désactiver le partage de fichiers simple** est activée 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 Linux.

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 de l'appareil fonctionnant sous le système d'exploitation macOS à l'installation à distance de l'Agent d'administration

Il existe les méthodes suivantes pour installer initialement l'Agent d'administration sur l'Appareil administré macOS :

- 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 Linux. Les paquets autonomes sont des modules exécutables qui contiennent la distribution des applications sélectionnés avec les paramètres configurés.

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 <device_name>` 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 :
      - À l'aide de l'interface de l'application
      - 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.

Licences

Cette section contient des informations sur :

- Concepts généraux liés aux licences Linux de Kaspersky Security Center
- Instructions sur la gestion des licences des applications Kaspersky administrées

License de Kaspersky Security Center Linux

Cette section décrit les concepts généraux liés aux licences de Kaspersky Security Center Linux.

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.

Lisez attentivement le Contrat de licence avant de commencer à utiliser l'application.

Kaspersky Security Center Linux et ses composants, 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 Linux 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 pour 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.
- Lors de l'installation 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 Linux.
- En lisant le document license.txt dans le dossier d'installation 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 de la licence

La *licence* est un droit d'utilisation limité dans le temps de Kaspersky Security Center Linux, 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.

  À l'expiration de la licence d'essai, toutes les fonctionnalités de Kaspersky Security Center Linux sont désactivées. 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 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 :

- Clé 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.

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.

La Politique de confidentialité est également disponible hors ligne :

- Vous pouvez lire la Politique de confidentialité avant d'installer Kaspersky Security Center Linux.
- Le texte de la Politique de confidentialité se trouve dans le fichier license.txt, dans le dossier d'installation de Kaspersky Security Center Linux.
- Le fichier privacy_policy.txt est disponible sur un appareil administré, dans le dossier d'installation de l'Agent d'administration.
- Vous pouvez décompresser le fichier privacy_policy.txt du paquet de distribution de l'Agent d'administration.

Options de licence de Kaspersky Security Center

Kaspersky Security Center est livré avec les applications de Kaspersky pour la protection des réseaux d'entreprise. Il peut également être téléchargé depuis le site Internet de Kaspersky.

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.
- Effectuer l'installation à distance des applications par Kaspersky et d'autres éditeurs de logiciels.
- 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.
- Gérez le chiffrement des informations stockées sur les disques durs des appareils Windows et sur les disques amovibles.
- Gérez l'accès des utilisateurs aux données chiffrées sur les appareils Windows.
- 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.

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.

À propos de la collecte des données

Données traitées localement

Kaspersky Security Center Linux est conçu pour l'exécution centralisée des tâches d'administration et de maintenance de base sur le réseau d'une organisation. Kaspersky Security Center Linux 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 Linux 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
- 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 Linux peut recevoir, stocker et traiter les informations suivantes :

- Informations sur les appareils du réseau de l'organisation reçues via l'analyse des contrôleurs de domaine Active Directory ou Samba ou via l'analyse des intervalles IP. Le Serveur d'administration obtient des données indépendamment ou reçoit des données de l'Agent d'administration.
- 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 lui-même ou reçoit les données de l'Agent d'administration chargé de fonctionner comme 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 affiché et la description de l'appareil 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 (pour les appareils appartenant à un domaine Windows), nom de l'appareil dans l'environnement Windows (pour les appareils appartenant à un domaine Windows), domaine DNS et nom DNS, adresse IPv4, adresse IPv6, emplacement réseau, adresse MAC, 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 requis pour l'audit des appareils administrés : 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 gère l'appareil.
    - 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 Kaspersky Security Center Web Console.

- 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 composants de l'application, 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.

- Données comprises dans les événements des modules de Kaspersky Security Center Linux et des applications administrées par Kaspersky. L'Agent d'administration transfère les données de l'appareil vers le Serveur d'administration.

- Paramètres des ;modules de Kaspersky Security Center Linux et des applications administrées par Kaspersky présentés dans les stratégies et les profils stratégiques L'Utilisateur saisit les données dans l'interface de Kaspersky Security Center Web Console.

- Paramètres des tâches des modules Kaspersky Security Center Linux et des applications administrées par Kaspersky L'Utilisateur saisit les données dans l'interface de Kaspersky Security Center Web Console.

- Données traitées par la fonction de gestion du système. L'Agent d'Administration transfère de l'appareil au Serveur d'administration les informations suivantes :

  - 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, 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

- Informations sur les logiciels installés sur les appareils administrés (Registre des logiciels). Le logiciel peut être comparé aux informations sur les fichiers exécutables détectées sur les appareils par la fonction Contrôle des applications.

- Catégories définies par l'utilisateur pour les applications. L'Utilisateur saisit les données 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'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 Windows chiffrés et l'état du 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 Windows 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.
- 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 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.

- Informations sur les erreurs de chiffrement des données sur les appareils. Le chiffrement est exécuté par la fonction Chiffrement des données des applications de Kaspersky. L'application administrée transfère les données de l'appareil vers le Serveur d'administration via l'Agent d'administration. La liste complète des données est fournie dans l'aide en ligne 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.

- Détails des codes d'activation saisis et des fichiers clés. 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 et mot de passe. L'Utilisateur saisit les données dans l'interface de Kaspersky Security Center Web Console.

- Historique des révisions des objets d'administration. L'Utilisateur saisit les données dans l'interface de Kaspersky Security Center Web Console.

- Registre des objets de gestion supprimés. L'Utilisateur saisit les données 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 saisit les données 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.

- Certificat de connexion sécurisée des appareils administrés aux composants Kaspersky Security Center Linux L'Utilisateur saisit les données dans l'interface de Kaspersky Security Center Web Console.

- Informations sur les conditions de l'accord légal de Kaspersky acceptées par l'utilisateur.

- Les données du Serveur d'administration que l'utilisateur saisit dans Kaspersky Security Center Web Console ou dans l'interface du programme Kaspersky Security Center Open API.

- Toutes les données saisies par l'utilisateur dans l'interface de Kaspersky Security Center Web Console.

Les données répertoriées ci-dessus peuvent être présentes dans Kaspersky Security Center Linux si l'une des méthodes suivantes est appliquée :

- L'Utilisateur saisit les données dans l'interface de Kaspersky Security Center Web Console.

- 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 lui-même les informations sur les appareils en réseau ou reçoit les données de l'Agent d'administration chargé de fonctionner comme point de distribution.

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 traitées localement ne peuvent être transférées à Kaspersky que par le biais de fichiers de vidage, de fichiers de trace ou de fichiers journaux des modules de Kaspersky Security Center Linux, y compris les fichiers journaux créés par les programmes d'installation et les utilitaires.

Les fichiers de vidage, les fichiers de traçage ou les fichiers journaux des Kaspersky Security Center Linux contiennent des données arbitraires du Serveur d'administration, de l'Agent d'administration et de Kaspersky Security Center Web Console. Les fichiers peuvent contenir des données personnelles ou confidentielles. Les fichiers dump, les fichiers de trace ou les fichiers journaux sont stockés sur les appareils sous une forme non chiffrée. Les fichiers de vidage, les fichiers de traçage ou les fichiers journaux ne sont pas transférés automatiquement vers Kaspersky, mais un administrateur peut transférer ces fichiers vers Kaspersky manuellement à la demande du Support Technique pour résoudre les problèmes liés aux performances de Kaspersky Security Center Linux.

Kaspersky protège les informations obtenues conformément à la législation et aux règles de Kaspersky. Les données sont transmises par un canal sécurisé.

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 Linux
- Version de Kaspersky Security Center Linux
- Localisation de Kaspersky Security Center Linux
- 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.

À propos de l'abonnement

Abonnement à Kaspersky Security Center Linux 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 Linux 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.

Pour utiliser Kaspersky Security Center Linux sous abonnement, vous devez appliquer le code d'activation reçu du fournisseur de services.

Vous pouvez appliquer un autre code d'activation pour l'utilisation de Kaspersky Security Center Linux 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.

Lorsque l'application est utilisée sous abonnement, Kaspersky Security Center Linux tente automatiquement d'accéder au serveur d'activation à des intervalles de temps spécifiés jusqu'à l'expiration de l'abonnement. Si l'accès aux 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 prestataire de services.

Activation de Kaspersky Security Center Linux

Vous pouvez activer Kaspersky Security Center Linux pour utiliser ses fonctionnalités complémentaires. Il existe deux façons d'accomplir cette tâche : via l'Assistant de configuration initiale du Serveur d'administration ou via les propriétés du Serveur d'administration.

Pour activer Kaspersky Security Center Linux :

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 **Clés de licence**.

3. Sous **Licence actuelle**, cliquez sur le bouton **Sélectionner**.

4. Dans la fenêtre qui s'ouvre, sélectionnez la clé de licence que vous souhaitez utiliser pour activer Kaspersky Security Center Linux. Si la clé de licence ne figure pas dans la liste, cliquez sur le bouton **Ajouter une nouvelle clé de licence**, puis indiquez une nouvelle clé de licence.

5. Si nécessaire, vous pouvez également ajouter une clé de licence de réserve. Pour cela, sous **Clé de licence de réserve**, cliquez sur le bouton **Sélectionner**, puis sélectionnez une clé de licence existante ou ajoutez-en une nouvelle. Notez que vous ne pouvez pas ajouter de clé de licence de réserve en l'absence de clé de licence active.

6. Cliquez sur le bouton **Enregistrer**.

Licence des applications Kaspersky administrées

Cette section décrit les possibilités de Kaspersky Security Center sur l'utilisation des clés de licence des applications administrées de Kaspersky.

Kaspersky Security Center Linux vous permet d'effectuer une distribution centralisée des clés de licence pour les applications Kaspersky sur les appareils clients, de surveiller leur utilisation et de renouveler les 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 activé l'option **Clé de licence diffusée automatiquement** pour les trois clés de licence. Sur les appareils de l'entreprise, l'application de sécurité de Kaspersky, par exemple, Kaspersky Endpoint Security for Linux 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 :

- 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 pratiques : 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 :

- 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** → **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.

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 Linux 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.

Événements de dépassement de la restriction de licence

Kaspersky Security Center Linux vous permet d'obtenir des informations sur les événements lorsque certaines limites de licence sont dépassées par les 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.

Suppression d'une clé de licence du stockage

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 des paramètres ( ) à côté du Serveur d'administration.

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.

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 Linux : 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 Linux 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 des applications Kaspersky

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 Linux
- Installation de Kaspersky Security Center Web Console
- Achevé le scénario d'installation principal de Kaspersky Security Center Linux
- 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

Étapes

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 être associées.

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 : Paramétrage de la tâche de groupe de mise à jour de Kaspersky Endpoint Security

   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 pratiques : 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.

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.

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.

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 Linux et Kaspersky Security Center Web Console. Vous pouvez envisager une administration de la sécurité aussi vouloir centrée sur l'utilisateur comme alternative ou option supplémentaire à l'approche centrée sur l'appareil. En savoir plus sur deux approches de gestion.

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 Linux crée la stratégie par défaut pour les applications suivantes :

   - Kaspersky Endpoint Security for Linux : pour les appareils clients Linux
   - Kaspersky Endpoint Security for Windows : pour les appareils clients Windows

   Si vous terminez cette procédure de configuration avec l'assistant, vous ne devez pas créer une nouvelle stratégie pour cette application.

   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. **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 dotés d'une configuration matérielle particulière ou de tags définis. Utilisez les tags pour filtrer les appareils qui répondent aux critères définis. Par exemple, vous pouvez créer un tag *CentOS*, l'attribuez à tous les appareils qui tournent sous CentOS, 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 CentOS seront administrées par leur propre profil de stratégie.

Instructions pour :

- 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. 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 Linux 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'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.

Prérequis

Avant de débuter, confirmez que vous avez bien installé le Serveur d'administration de Kaspersky Security Center Linux et/ou Kaspersky Security Center Web Console et que vous avez terminé le scénario de déploiement 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 Linux 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.

   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, Kaspersky Security Center Linux synchronise automatiquement le Serveur d'administration avec les appareils administrés toutes les 15 secondes. 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 Linux 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.

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. L'état d'une stratégie est l'un des suivants :

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.
- 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 :

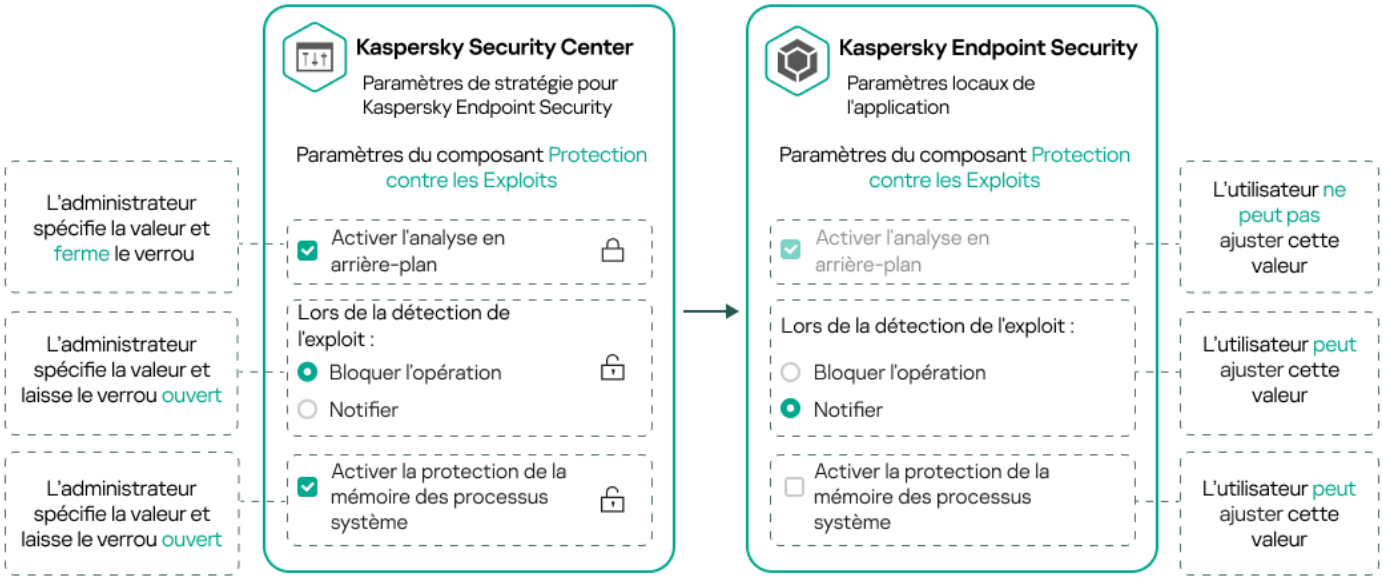
- Paramètres de verrouillage pour une stratégie de sous-groupe d'administration
- Paramètres de verrouillage d'une application Kaspersky sur un appareil administré

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

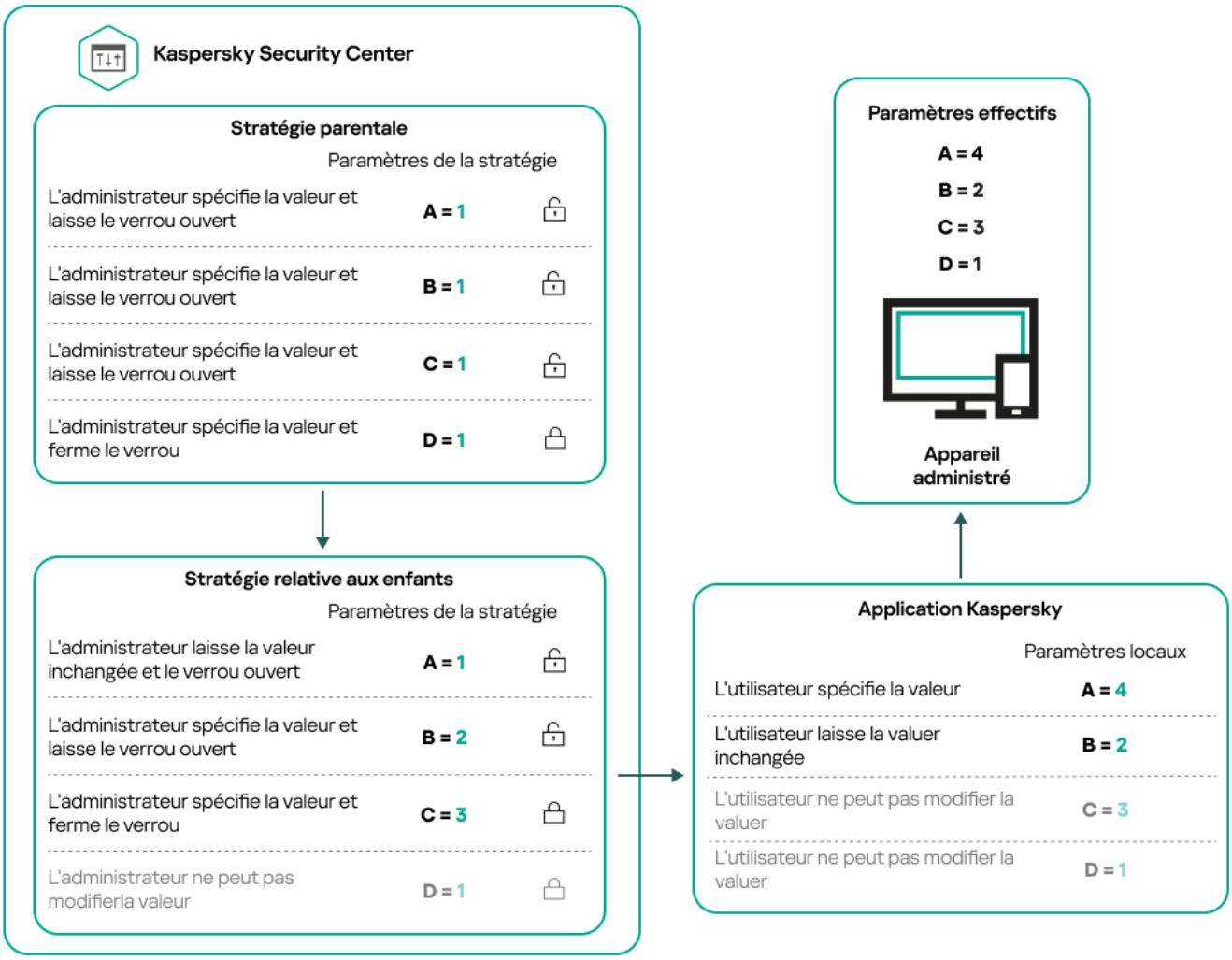
Si des appareils différents requièrent des paramètres différents, vous pouvez organiser les appareils en groupes d'administration.

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).

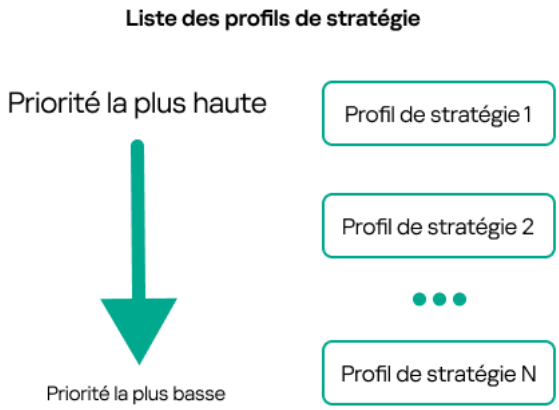


Hiérarchie des stratégies

Profils de stratégie dans une hiérarchie de stratégies

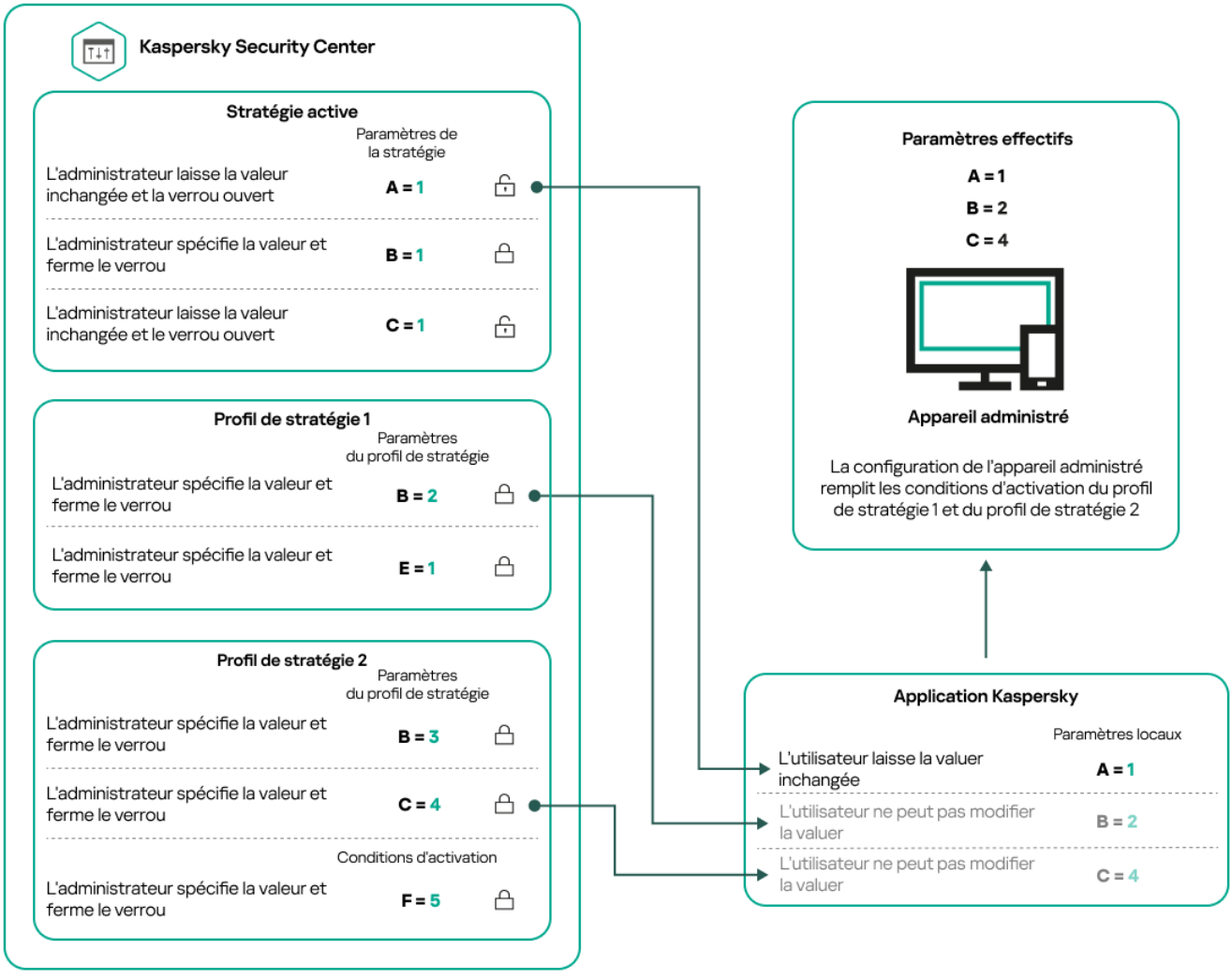
Les conditions d'attribution de priorité des profils de stratégie sont les suivantes :

- 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).



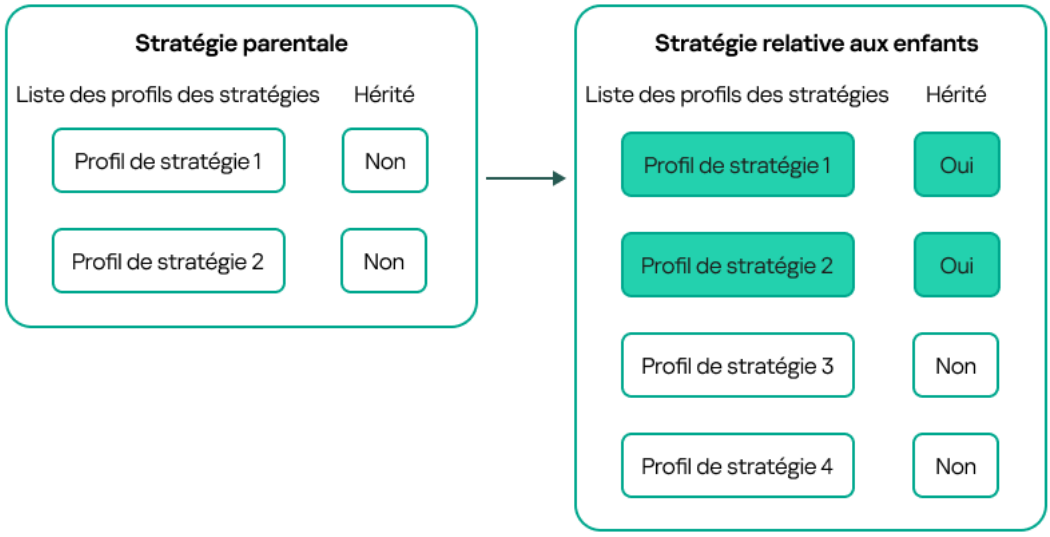
La configuration de l'appareil administré satisfait aux conditions d'activation de plusieurs profils de stratégie

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).

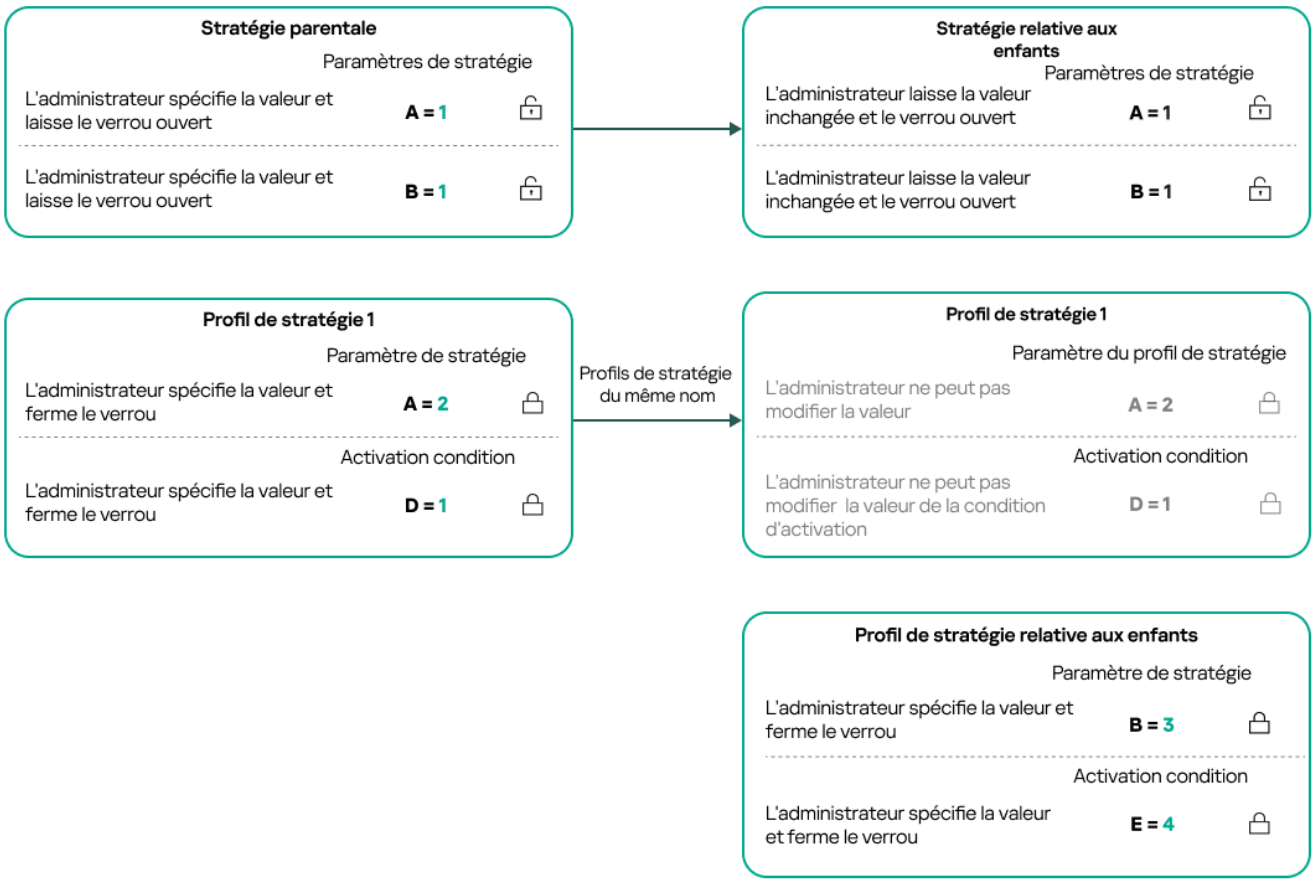


Héritage des profils de stratégie

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 des applications**.

   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 des applications**, 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
- Aide de Kaspersky Endpoint Security for Linux
- Aide de Kaspersky Endpoint Security for Windows

Pour plus de détails sur les paramètres des autres applications de sécurité, 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.

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.

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
   - Aide de Kaspersky Endpoint Security for Linux
   - Aide 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**.

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 Linux 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 Linux 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 **Détails** 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)**.

Synchronisation forcée

Malgré le fait que Kaspersky Security Center Linux 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 a déjà eu lieu à un moment précis et pour un appareil en particulier.

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 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.

Affichage du graphique de l'état de la distribution des stratégies

Dans Kaspersky Security Center Linux, 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 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 des applications**.

   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 des applications**, 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.

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 cette option pour configurer et activer la règle d'activation du profil sur l'appareil par l'appartenance du propriétaire à un groupe de sécurité interne de Kaspersky Security Center Linux. 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 Linux. 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 :

  - 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.

- 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.

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. La fenêtre des propriétés contient les onglets et les paramètres décrits ci-dessous.

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 pouvez modifier le nom de la stratégie, son état et spécifier l'héritage des paramètres de la stratégie :

- Le groupe **État de la stratégie** permet de sélectionner l'un des modes de stratégie suivants :
  - **Stratégie active**

    Si cette option a été sélectionnée, la stratégie devient active.

    Cette option est sélectionnée par défaut.
  - **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

Cet onglet permet de configurer l'enregistrement des événements dans le journal et les notifications relatives à ces derniers. Les événements sont répartis selon leur niveau d'importance dans les sections suivantes :

- **Erreur de fonctionnement**
- **Avertissement**
- **Information**

Dans chaque section, la liste indique les types d'événements et la durée de conservation par défaut des événements 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 des applications

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 Linux). 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 sur les appareils fonctionnant sous Windows.

  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.

- 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.

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, 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.

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**

  Les profils des connexions ne sont pris en charge que pour les appareils fonctionnant sous Windows.

  Vous pouvez consulter et 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

- **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 les utilisateurs itinérants. 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 :

- **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 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

La section **Paramètres du réseau pour les points de distribution** permet de configurer les paramètres d'accès au réseau Internet :

- **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.

  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.

- **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.

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.

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, Linux ou macOS.

Comparaison entre fonctionnalités de l'Agent d'administration

Fonctionnalité de l'Agent d'administration	Windows	Linux	macOS

Installation			
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	✓	✓	✓
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).
Modèle hors ligne de téléchargement des mises à jour	✓	✓	✓
Sondage réseau	✓ • Sondage des plages IP • Sondage du contrôleur de domaine	✓ • 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	✓	✓	✓
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	✓	—	—
Mises à jour du logiciel	✓	—	—
Inventaire du logiciel installé sur les appareils	✓	✓	—
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	✓	✓	✓
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.	

Comparaison des paramètres de l'Agent d'administration par système d'exploitation

Le tableau ci-dessous indique les paramètres de la stratégie de l'Agent d'administration disponibles en fonction du système d'exploitation de l'appareil administré sur lequel l'Agent d'administration a été installé.

Paramètres de l'Agent d'administration : comparaison par système d'exploitation

Section Paramètres	Windows	Linux	macOS
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	✓	✓ Les options suivantes sont proposées : • **Détails sur les applications installées** • **Informations sur le registre du matériel**	—
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	✓ Les options suivantes sont proposées : • **Réseau Windows** • **Plages IP** • **Contrôleurs de domaine**	✓ 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	✓	✓	✓

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 des applications** → **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 des applications** → **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 des applications** → **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 des applications** → **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 Linux (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 Linux, 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 des applications** → **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. Dans la section **Erreur de fonctionnement**, cliquez sur **Ajouter un événement** 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.

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 d'utiliser les bases de données de réputation de Kaspersky pour récupérer des informations sur les applications installées sur les appareils administrés.

En participant au 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 Linux. Le transfert des informations s'exécute conformément aux paramètres d'accès à KSN configurés.

Kaspersky Security Center Linux est compatible avec les solutions d'infrastructure KSN suivantes :

- Le *KSN global* est une solution qui permet d'échanger des informations avec Kaspersky Security Network. Quand vous participez au 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 Linux. 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 Linux 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 propose de 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 Linux vérifie si les serveurs KSN sont accessibles pour s'assurer que le niveau de sécurité est maintenu pour les appareils administrés. Si l'accès aux serveurs via le DNS système n'est pas possible, l'application utilise les serveurs DNS publics.

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 Activée**.

   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 Linux 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 Linux). 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 Linux).

4. Basculez le commutateur sur la position **Utiliser Kaspersky Security Network Activée**.

   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 Activée** 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 basculez le commutateur sur la position **Utiliser Kaspersky Private Security Network Activée**, un message s'affiche avec des détails sur le KPSN.

   Les applications Kaspersky suivantes prennent en charge KPSN :

   - Kaspersky Security Center Linux
   - Kaspersky Endpoint Security for Linux
   - Kaspersky Endpoint Security for Windows

   Si vous activez le KPSN dans Kaspersky Security Center Linux, 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.

   > Kaspersky Security Center Linux 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 Activée**.

   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 Activée**.

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.

Veuillez noter que le point de distribution ne prend pas en charge l'authentification des appareils administrés à l'aide du protocole NTLM.

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 Activée**.

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 Activée**.

     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 Activée**, 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 Activée**, 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 Désactivée** 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 désigné pour fonctionner comme point de distribution, vous pouvez activer le proxy Kaspersky Security Network (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 Linux fonctionne comme serveur proxy KSN, procédez comme suit :

1. Sur l'appareil du point de distribution, exécutez la commande `ps aux` pour afficher la liste des processus en cours d'exécution.

2. Dans la liste des processus en cours d'exécution, vérifiez si le processus `/opt/kaspersky/klnagent64/sbin/ksnproxy` est en cours d'exécution.

Si le processus `/opt/kaspersky/klnagent64/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.

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.

Gérer les tâches

Cette section décrit les tâches utilisées par Kaspersky Security Center Linux.

À propos des tâches

Kaspersky Security Center Linux 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 Kaspersky Security Center Web Console, mais aussi par l'utilisateur de l'appareil à distance (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) 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 Linux.

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 *Installation à distance d'une application* est reliée au Serveur d'administration et la tâche de *mise à jour* se rapporte à Kaspersky Endpoint Security.

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).

  - 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 vendredi 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 Linux.

  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 la tâche de *mise à jour*.

- Après l'exécution d'une autre tâche

  La tâche actuelle démarre à la fin d'une autre tâche. Vous pouvez sélectionner comment la tâche antérieure doit se terminer (réussite ou erreur) pour lancer l'exécution de la tâche actuelle. Ce paramètre ne fonctionne que si les deux tâches sont affectées aux mêmes appareils.

- 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 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 (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 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 Syslog 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 Syslog 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 Linux 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 Linux 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 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 **Détails** 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 actuellement valides dans votre système. Lorsque vous passez à l'étape suivante de l'assistant, Kaspersky Security Center Linux 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 Linux 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.

Affichage de l'historique des tâches entreposé sur le Serveur d'administration

Kaspersky Security Center Linux 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. La consultation des résultats d'exécution des tâches locales n'est pas disponible.

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**.

Tags de l'application

Kaspersky Security Center Linux vous permet de tagger les applications à partir du 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.

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, 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 déconnecté 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, dans la section **Paramètres des applications → Contrôles de sécurité → Contrôle des appareils**.

L'autorisation de l'accès hors ligne à l'appareil externe bloqué par le Contrôle des appareils comprend les étapes suivantes :

1. Dans la boîte de dialogue de Kaspersky Endpoint Security, 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 Linux.

2. Après avoir reçu cette requête, l'administrateur de Kaspersky Security Center Linux 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, 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 des applications** 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**.

9. Dans la fenêtre qui s'ouvre, 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, l'utilisateur dispose d'un accès temporaire à l'appareil bloqué pendant une période en particulier.

Utilisation de l'utilitaire klsclag pour ouvrir le port 13291

Vous pouvez automatiser le fonctionnement de Kaspersky Security Center Linux via l'utilitaire klakaut. L'utilitaire klakaut et son système d'aide se trouvent dans le dossier d'installation de Kaspersky Security Center Linux. Si vous souhaitez utiliser l'utilitaire klakaut, ouvrez le port 13291 à l'aide de l'utilitaire klscflag.

L'utilitaire klscflag modifie la valeur du paramètre KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN.

Pour ouvrir le port 13291 :

1. Exécutez la commande suivante dans la ligne de commande :
   ```
   $ /opt/kaspersky/ksc64/sbin/klscflag -ssvset -pv klserver -s 87 -n
   KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN -sv true -svt BOOL_T -ss "|ss_type =
   \"SS_SETTINGS\";"
   ```

2. Redémarrez le service Serveur d'administration de Kaspersky Security Center en exécutant la commande suivante :
   ```
   $ sudo systemctl restart kladminserver_srv
   ```

   Le port 13291 est ouvert.

Pour vérifier si le port 13291 a été ouvert avec succès :

Exécutez la commande suivante dans la ligne de commande :

```
$ /opt/kaspersky/ksc64/sbin/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)true
```

La valeur `true` signifie que le port est ouvert. Sinon, la valeur `false` s'affiche.

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.

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. Une fois le plug-in téléchargé et installé, la section **KICS for Networks** s'affiche dans le menu principal de Kaspersky Security Center Web Console.

- Dans l'interface Web de Kaspersky Industrial CyberSecurity for Networks, l'interaction avec Kaspersky Security Center est configurée et activée. Pour plus de détails, veuillez consulter l'Aide en ligne de Kaspersky Industrial CyberSecurity for Networks.

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. Ouvrez la fenêtre des propriétés de l'appareil sur lequel est installé le serveur Kaspersky Industrial CyberSecurity for Networks.

4. Sur la page des propriétés de l'appareil, dans la section **General**, 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 l'Agent d'administration de Kaspersky Security Center.

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 de Kaspersky Industrial CyberSecurity for Networks, vous pouvez le faire maintenant.

8. Si vous souhaitez consulter les statistiques de Kaspersky Industrial CyberSecurity for Networks, vous pouvez ajouter des widgets sur le tableau de bord. Pour ajouter les widgets, procédez comme suit :

   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 les widgets que vous souhaitez ajouter :

      - Carte de déploiement de KICS pour les réseaux
      - Informations sur KICS pour les serveurs de réseaux
      - Événements actualisés de KICS pour les réseaux
      - Appareils rencontrant des problèmes dans KICS pour les réseaux
      - Événements critiques dans KICS pour les réseaux

- Statuts dans KICS pour les réseaux

9. Pour accéder à l'interface Web de Kaspersky Industrial CyberSecurity for Networks, procédez comme suit :

   a. Dans le menu principal, accédez à **KICS pour les réseaux** → **Rechercher**.

   b. Cliquez sur le bouton **Rechercher des événements ou des appareils**.

   c. Dans la fenêtre **Paramètres de requête** qui s'ouvre, cliquez sur le champ **Serveur**.

   d. Sélectionnez le serveur Kaspersky Industrial CyberSecurity for Networks dans la liste déroulante des serveurs intégrés à Kaspersky Security Center, puis cliquez sur le bouton **Rechercher**.

   e. Cliquez sur le lien **Aller au serveur** à côté du nom du serveur Kaspersky Industrial CyberSecurity for Networks.

      La page de connexion de Kaspersky Industrial CyberSecurity for Networks s'affiche.

      Pour vous connecter à l'interface Web de Kaspersky Industrial CyberSecurity for Networks, vous devez fournir les informations d'identification du compte utilisateur de l'application.

Administration des utilisateurs et des rôles d'utilisateur

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 comptes utilisateurs

Kaspersky Security Center Linux permet d'administrer les comptes utilisateurs et les groupes de sécurité. 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 des appareils administrés, ainsi que les comptes locaux de l'appareil sur lequel le Serveur d'administration est installé.
- Comptes des utilisateurs internes de Kaspersky Security Center Linux. Vous pouvez créer des comptes d'utilisateurs internes. Ces comptes sont utilisés uniquement dans Kaspersky Security Center Linux.

Le groupe kladmins ne peut pas être utilisé pour accéder à Kaspersky Security Center Web Console dans Kaspersky Security Center Linux. Le groupe kladmins ne peut contenir que les comptes utilisés pour lancer les services Kaspersky Security Center Linux.

Pour consulter les tableaux des comptes utilisateurs et des groupes de sécurité, procédez comme suit :

1. Dans le menu principal, accédez à **Utilisateurs et rôles** → **Utilisateurs et groupes**.
2. Sélectionnez l'onglet **Utilisateurs** ou **Groupes**.

Le tableau des utilisateurs ou groupes de sécurité s'ouvre. Si vous souhaitez afficher le tableau avec uniquement des utilisateurs ou des groupes internes ou uniquement avec des utilisateurs ou des groupes locaux, définissez les critères de filtre **Sous-type** sur **Interne** ou **Local** respectivement.

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.

Configuration des droits d'accès aux fonctionnalités de l'application. Restriction d'accès selon un rôle

Kaspersky Security Center Linux fournit des possibilités d'accès selon un rôle aux fonctionnalités de Kaspersky Security Center Linux et des applications Kaspersky administrées.

Vous pouvez configurer les droits d'accès aux fonctionnalités de l'application pour les utilisateurs de Kaspersky Security Center Linux 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 Linux avec les droits d'accès pour administrer 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**, d'**écriture** et d'**exécution** s'appliquent à toute tâche, rapport ou paramètre. En plus de ces droits, un utilisateur doit disposer du droit **Effectuer des opérations sur les sélections d'appareils** pour gérer les tâches, les rapports ou les paramètres sur les sélections d'appareils.

La zone fonctionnelle **Fonctionnalités générales** : **Accéder aux objets quel que soit leur ACL** est conçue à des fins d'audit. Lorsque les utilisateurs disposent des droits de **lecture** dans cette zone fonctionnelle, ils bénéficient d'un accès complet en **lecture** 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.

Toutes les tâches, rapports, paramètres et paquets d'installation qui manquent dans le tableau appartiennent à la zone fonctionnelle **Fonctionnalités 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
Caractéristiques générales : **Gestion 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
Caractéristiques générales : **Accéder aux objets, quel que soit leur ACL**	**Lecture**	Obtenir un accès en lecture à tous les objets : **Lire**	Aucun	Aucun	L'accès est accordé indépendamment des autres droits, même s'ils interdisent l'accès en lecture à des objets particuliers.
Caractéristiques générales : **Fonctionnalité de base**	• **Lecture** • **Écrire** • **Exécuter** • **Effectuer des opérations sur les sélections d'appareils**	• Règles de déplacement des appareils (création, modification ou suppression) pour le Serveur virtuel : **Écrire**, **Effectuer des opérations sur les sélections d'appareils** • Certificat personnalisé du protocole Get Mobile (LWNGT) : **Lire**	• " Télécharger les mises à jour dans le stockage du Serveur d'administration " • "Livrer des rapports" • "Diffusion du paquet d'installation"	• "Rapport sur l'état de la protection" • "Rapport sur les menaces" • "Rapport sur les appareils les plus infectés"	Aucun

		• 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** • Consulter le journal du système d'exploitation : **Lire** • Afficher la clé de récupération pour restaurer l'accès à un disque dur chiffré par le chiffrement de disque BitLocker : **Exécuter**	• "Installation des applications sur les Serveurs d'administration secondaires à distance"	• "Rapport sur l'état des bases antivirus" • "Rapport sur les erreurs" • " Rapport sur les attaques réseau " • " Rapport récapitulatif sur les applications de défense de périmètre installées " • "Rapport de synthèse sur les types d'application installés" • "Rapport sur les utilisateurs des appareils infectés" • " Rapport d'incidents " • "Rapport sur les événements" • "Rapport d'activité des points de distribution" • "Rapport sur les Serveurs d'administration secondaires" • " Rapport sur les événements du Contrôle des appareils " • " Rapport sur les applications interdites " • "Rapport sur le fonctionnement du Contrôle Internet" • " Rapport de l'état de chiffrement des appareils administrés " • " Rapport de l'état de chiffrement des appareils de stockage de masse " • « Rapport sur les privilèges d'accès aux	

				disques chiffrés » • " Rapport sur les erreurs de chiffrement des fichiers " • " Rapport sur le blocage de l'accès aux fichiers chiffrés " • "Rapport sur les droits effectifs de l'utilisateur" • "Rapport sur les privilèges"	
Caractéristiques générales : **Objets supprimés**	• **Lecture** • **Écrire**	• Afficher les objets supprimés dans la corbeille : **Lire** • Supprimer des objets de la corbeille : **Écrire**	Aucun	Aucun	Aucun
Caractéristiques générales : **Traitement des événements**	• **Supprimer des événements** • **Modifier les paramètres de notification d'événement** • **Modifier les paramètres de journalisation des événements** • **Écrire**	• Modifier les paramètres d'enregistrement des événements : **Modifier les paramètres de journalisation des événements** • Modifier les paramètres de notification d'événements **Modifier les paramètres de notification d'événements** • Supprimer des événements : **Supprimer des événements**	Aucun	Aucun	Paramètres : • Le nombre maximal d'événements stockés dans la base de données • Période de stockage des événements des appareils supprimés
Caractéristiques générales : **Opérations sur le Serveur d'administration**	• **Lecture** • **Écrire** • **Exécuter** • **Modifier les ACL d'objets** • **Effectuer 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	• "Sauvegarde des données du Serveur d'administration" • "Maintenance de la base de données"	Aucun	Aucun

		distribution des profils MDM : **Écrire** • Spécifier les ports SSL du Serveur d'administration pour la connexion via 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**			
Caractéristiques générales : **Déploiement logiciel Kaspersky**	• **Administration des correctifs de Kaspersky** • **Lecture** • **Écrire** • **Exécuter** • **Effectuer des opérations sur les sélections d'appareils**	Approuver ou refuser l'installation du correctif : **Gérer les correctifs 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"
Caractéristiques générales : **Gestion des clés**	• **Ajouter 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
Caractéristiques générales : **Administration des rapports mis en œuvre**	• **Lecture** • **Écrire**	• Créer des rapports quel que soit leur ACL : **Écrire**	Aucun	Aucun	Aucun

		• Exécuter des rapports quel que soit leur ACL : **Lire**			
Caractéristiques 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
Caractéristiques générales : **Autorisations des utilisateurs**	**Modifier les ACL d'objets**	• Modifier les propriétés Sécurité de n'importe quel objet : **Modifier les ACL des objets** • Gérer les rôles utilisateur : **Modifier les ACL des objets** • Gérer les utilisateurs internes : **Modifier les ACL des objets** • Gérer les groupes de sécurité : **Modifier les ACL des objets** • Gérer les alias : **Modifier les ACL des objets**	Aucun	Aucun	Aucun
Caractéristiques générales : **Serveurs d'administration virtuels**	• **Gérer les Serveurs d'administration virtuels** • **Lecture** • **Écrire** • **Exécuter** • **Effectuer 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 : **Gérer les Serveurs d'administration virtuels** • Déplacer un Serveur d'administration virtuel vers un autre groupe : **Gérer les Serveurs d'administration virtuels** • Définir les autorisations du Serveur virtuel d'administration : **Gérer les Serveurs d'administration virtuels**	Aucun	Aucun	Aucun
Caractéristiques générales : **Gestion des clés de chiffrement**	**Écrire**	Importer les clés de chiffrement : **Écrire**	Aucun	Aucun	Aucun
Gestion du	• **Lecture**	• Afficher les propriétés	• "Corriger les	"Rapport sur les	Aucun

système : **Gestion des vulnérabilités et des correctifs**	• **Écrire** • **Exécuter** • **Effectuer des opérations sur les sélections d'appareils**	des correctifs tiers : **Lire** • Modifier les propriétés des correctifs tiers : **Écrire**	vulnérabilités" • "Installation des mises à jour requises et correction des vulnérabilités"	mises à jour des logiciels"	

À propos des rôles d'utilisateurs prédéfinis

Les rôles d'utilisateurs attribués aux utilisateurs de Kaspersky Security Center Linux 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 Linux. Certains des rôles utilisateur prédéfinis disponibles dans Kaspersky Security Center Linux peuvent être associés à des fonctions spécifiques, par exemple **Auditeur**, **Responsable de la sécurité**, **Superviseur**. 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	Ceci autorise toutes les opérations avec tous les types de rapports, toutes les opérations de visualisation, y compris la visualisation des objets supprimés (accorde les droits de **Lire** et **Écrire** dans la zone **Objets supprimés**). Ceci n'autorise pas les autres opérations. Vous pouvez attribuer ce rôle à une personne qui réalise un audit de votre organisation.
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.

Caractéristiques des domaines fonctionnels **Administration des appareils mobiles : Générale** et **Administration du système** ne sont pas disponibles dans Kaspersky Security Center Linux. Un utilisateur doté des rôles **Administrateur de Gestion des vulnérabilités et des correctifs / opérateur** ou **Administrateur dédié à l'administration des appareils mobiles / Opérateur** n'a accès qu'aux droits de la zone fonctionnelle **Fonctionnalités générales** : **Fonctionnalités de base**.

Droits d'accès des rôles utilisateur prédéfinis

Rôle	Description
Administrateur du Serveur d'administration	Autorise toutes les opérations dans les domaines fonctionnels suivants, dans **Fonctions générales** : • **Fonctionnalité de base** • **Traitement des événements** • **Hiérarchie des Serveurs d'administration** • **Serveurs d'administration virtuels** Accorde les droits de **lecture** et d'**écriture** dans la zone fonctionnelle **Fonctions 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, dans **Fonctions générales** : • **Fonctionnalité de base** • **Serveurs d'administration virtuels**
Auditeur	Autorise toutes les opérations dans les domaines fonctionnels suivants, 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	Autorise toutes les opérations dans les domaines fonctionnels suivants, dans **Fonctions générales** : • **Fonctionnalité de base** • **Déploiement de logiciels Kaspersky** • **Gestion des clés de licence** 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, dans **Fonctions générales** : • **Fonctionnalité de base** • **Déploiement de logiciels Kaspersky** (accorde également les **correctifs Manage Kaspersky** directement dans cette zone) • **Serveurs d'administration virtuels**
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 **Fonctions 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 **Fonctions générales : Gestion des clés de chiffrement**.
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 logiciels Kaspersky** • **Serveurs d'administration virtuels** • Zone Kaspersky Endpoint Security, y compris toutes les fonctionnalités

Administrateur Administration des appareils mobiles	Autorise toutes les opérations dans la zone fonctionnelle **Fonctions générales : Fonctionnalité de base**.
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.

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

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 logiciels 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
  - 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

Pour ajouter un nouveau compte d'utilisateur interne à Kaspersky Security Center Linux, 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** pour connecter l'utilisateur à Kaspersky Security Center Linux.
     Le mot de passe doit remplir les conditions suivantes :
     - Le mot de passe doit compter entre 8 et 16 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 afficher les caractères que vous avez entrés, cliquez sur le bouton **Afficher** et maintenez-le 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. Il est possible de débloquer le compte utilisateur uniquement en modifiant le mot de passe.

4. Cliquez sur le bouton **Enregistrer** afin d'enregistrer les modifications.

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

Pour modifier le compte d'un utilisateur interne dans Kaspersky Security Center Linux, 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 :

   - **Description**
   - **Nom complet**
   - **Adresse email**
   - **Numéro de téléphone principal**
   - **Définir un nouveau mot de passe** pour connecter l'utilisateur à Kaspersky Security Center Linux.

     Le mot de passe doit remplir les conditions suivantes :

     - Le mot de passe doit compter entre 8 et 16 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 autorisé ; cependant, pour des raisons de sécurité, nous vous déconseillons de diminuer ce nombre. Si l'utilisateur saisit incorrectement le mot de passe le nombre de fois indiqué, le compte utilisateur associé est bloqué pour une heure. Il est possible de débloquer le compte utilisateur uniquement en modifiant le mot de passe.

   - 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.

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. Cliquez sur le bouton **Enregistrer** afin d'enregistrer les modifications.

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**.

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**.

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 et groupes**, puis sélectionnez l'onglet **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 **Sécurité d'authentification**.

4. Sous l'onglet **Sécurité d'authentification**, sélectionnez l'option **Demander une authentification pour vérifier l'autorisation de modifier ce compte utilisateur** 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**.

Vérification en deux étapes

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

Scénario : 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 Linux 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 Linux 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**

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.

5. **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.

6. **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.

7. **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.

8. **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 Web Console. Dans le cas contraire, il ne pourra pas accéder au Serveur d'administration conformément à ses privilèges.

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 pour un compte

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

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. Vous pouvez modifier le nom de l'émetteur du code de sécurité. Le nom par défaut de l'émetteur du code de sécurité est identique au nom du Serveur d'administration. Le nom de l'émetteur est utilisé comme identifiant du Serveur d'administration dans l'application d'authentification. 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. Un code de sécurité est à usage unique et valide jusqu'à 90 secondes (la durée exacte peut varier).

Tout utilisateur pour lequel la vérification en deux étapes est activée peut réémettre sa clé secrète. Lorsqu'un utilisateur s'authentifie avec la clé secrète réémise et l'utilise pour se connecter, le Serveur d'administration enregistre la nouvelle clé secrète pour le compte de l'utilisateur. Si l'utilisateur saisit la nouvelle clé secrète de façon incorrecte, le Serveur d'administration n'enregistre pas la nouvelle clé secrète et laisse la clé secrète actuelle valide pour l'authentification ultérieure.

Tout logiciel d'authentification prenant en charge l'algorithme TOTP (Time-based One-time Password) peut être utilisé comme application d'authentification, par exemple, Google Authenticator. Afin de générer le code de sécurité, vous devez synchroniser l'heure définie dans l'application d'authentification avec l'heure définie pour le Serveur d'administration.

Pour vérifier si Kaspersky Security Center Linux 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 Linux prend en charge l'authentificateur sélectionné.

Une application d'authentification génère le code de sécurité comme suit :

1. Le Serveur d'administration génère une clé secrète spéciale et un code QR.
2. Vous transmettez la clé secrète ou le code QR généré à l'application d'authentification.
3. L'application d'authentification génère un code de sécurité à usage unique que vous transmettez à la fenêtre d'authentification du Serveur d'administration.

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 Linux, 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.

La vérification en deux étapes fonctionne selon les règles suivantes :

- Seul un compte utilisateur disposant du droit Modifier les ACL des objets dans la zone fonctionnelle **Fonctionnalités générales : Autorisations utilisateur** peut activer la vérification en deux étapes pour tous les utilisateurs.
- Seul un utilisateur qui a activé la vérification en deux étapes pour son propre compte peut activer l'option de vérification en deux étapes pour tous les utilisateurs.
- Seul un utilisateur qui a activé la vérification en deux étapes pour son propre compte peut exclure d'autres comptes utilisateurs de la liste de la vérification en deux étapes activée pour tous les utilisateurs.
- Un utilisateur peut activer la vérification en deux étapes uniquement pour son propre compte.
- Un compte utilisateur disposant du droit Modifier les ACL des objets de la zone fonctionnelle **Caractéristiques générales : Autorisations utilisateur** et connecté à Kaspersky Security Center Web Console à l'aide de la vérification en deux étapes peut désactiver la vérification en deux étapes : pour tout autre utilisateur,

uniquement si la vérification en deux étapes pour tous les utilisateurs est désactivée et pour un utilisateur exclu de la liste de la vérification en deux étapes qui est activée pour tous les utilisateurs.

- Tout utilisateur qui s'est connecté Kaspersky Security Center Web Console à l'aide de la vérification en deux étapes peut réémettre sa propre clé secrète.

- Vous pouvez activer l'option de vérification en deux étapes pour tous les utilisateurs pour le Serveur d'administration que vous utilisez actuellement. Si vous activez cette option sur le Serveur d'administration, vous activez également cette option pour les comptes utilisateurs de ses Serveurs d'administration virtuels et vous n'activez pas la vérification en deux étapes pour les comptes utilisateurs des Serveurs d'administration secondaires.

Activation de la vérification en deux étapes pour votre compte

Vous ne pouvez activer la vérification en deux étapes que pour votre propre compte.

Avant de commencer à 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 et groupes**, puis sélectionnez l'onglet **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** :

   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**.

   Cliquez sur **Afficher le code QR.**

   c. 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.

   d. 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**.

4. Cliquez sur le bouton **Enregistrer**.

La vérification en deux étapes est activée pour votre compte.

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.

Activation de la vérification en deux étapes obligatoire pour tous les utilisateurs

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. Cliquez sur **Afficher le code QR.**

   c. 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.

      Vous pouvez également saisir manuellement la clé secrète dans l'application d'authentification.

   d. 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.

Désactivation de la vérification en deux étapes d'un compte utilisateur

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 et groupes**, puis sélectionnez l'onglet **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 **Sécurité d'authentification**.

4. 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 obligatoire pour tous les utilisateurs

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 d'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**.

3. Saisissez les identifiants de votre compte dans la fenêtre d'authentification.

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

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. 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, dans le tableau des exclusions de la vérification en deux étapes, cliquez sur le bouton **Ajouter**.

3. 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.

Configuration de la vérification en deux étapes pour votre compte

Lors de la première connexion à Kaspersky Security Center Linux 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.

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 Linux 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.

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 et groupes**, puis sélectionnez l'onglet **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 **Sécurité d'authentification**.

4. Sous l'onglet **Sécurité d'authentification**, 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.

Modification du nom d'un émetteur de code de sécurité

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 **Sécurité d'authentification**.

3. Sous l'onglet **Sécurité d'authentification**, 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 nombre de tentatives de saisie du mot de passe autorisées

L'utilisateur de Kaspersky Security Center Linux 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. Sur l'appareil du Serveur d'administration, lancez une ligne de commande Linux.

2. Pour l'utilitaire klscflag, exécutez la commande suivante :

   ```
   sudo /opt/kaspersky/ksc64/sbin/klscflag -fset -pv klserver -n SrvSplPpcLogonAttempts -t d -v N
   ```

   où N est le nombre de tentatives de saisie d'un mot de passe.

3. Pour appliquer les modifications, redémarrez le service du Serveur d'administration.

Le nombre maximal de tentatives autorisées de saisie du mot de passe est modifié.

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.

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.

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 Linux

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 Linux

Lorsque vous terminez ce scénario, vous pouvez être sûr que :

- Votre réseau est protégé par le dernier logiciel de Kaspersky, y compris les composants et les applications de sécurité de Kaspersky Security Center Linux.
- 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. En cas d'absence de connexion, envisagez de mettre à jour manuellement les bases de données et les modules logiciels 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**

   Il existe plusieurs schémas pour installer les mises à jour des applications de sécurité. 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 Linux. 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 : créer la tâche de téléchargement des mises à jour sur 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 Linux 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 : 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.

5. **Optimisation du processus de mise à jour à l'aide de fichiers diff (facultatif)**

   Vous pouvez optimiser le trafic entre le Serveur d'administration et les appareils administrés à l'aide 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

6. **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 modules logiciels et des bases de données Kaspersky, et notamment des bases antivirus. Pour garantir des mises à jour opportunes, nous vous recommandons de sélectionner l'option **Lors du téléchargement des mises à jour dans le stockage** pendant 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 13.2 et l'Agent d'administration version 13.2 sont installés sur les appareils administrés.

   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.

Résultats

Une fois le scénario terminé, Kaspersky Security Center Linux est configuré pour mettre à jour les bases de données Kaspersky une fois les mises à jour téléchargées dans le stockage du Serveur d'administration. 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 Linux 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 Linux

  Kaspersky Security Center Linux ne peut pas mettre à jour automatiquement les applications Kaspersky. Pour mettre à jour les applications, téléchargez les dernières versions des applications depuis le site Web de Kaspersky et installez-les manuellement :

  - Serveur d'administration de Kaspersky Security Center Linux et de Kaspersky Security Center Web Console
  - Agent d'administration, Kaspersky Endpoint Security, plug-in Web d'administration

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 :

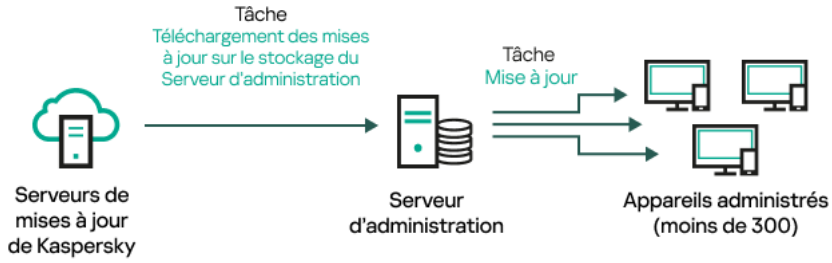
- En utilisant une seule tâche : *Téléchargement des mises à jour sur le stockage du Serveur d'administration*
- En utilisant deux tâches :

- *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 Linux 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).



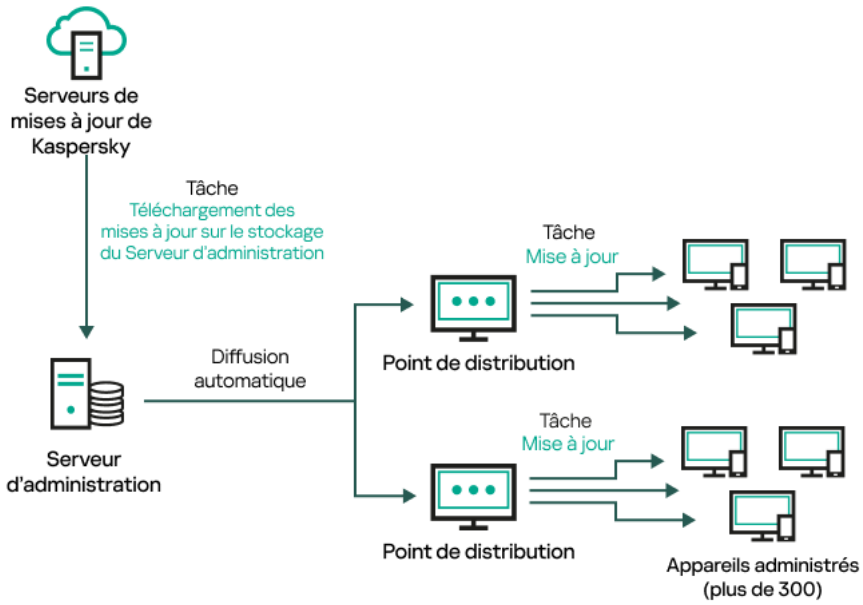
Mise à jour à l'aide de la tâche *Téléchargement des mises à jour sur le stockage du Serveur d'administration* sans points de distribution

En tant que source de mises à jour, vous pouvez utiliser non seulement les serveurs de mise à jour de Kaspersky, mais également un dossier local ou réseau.

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 300 appareils administrés ou plus dans un seul segment de réseau ou 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

Quand la tâche *Téléchargement des mises à jour sur le stockage du Serveur d'administration* est terminée, les mises à jour des bases de données et des modules logiciels de Kaspersky Endpoint Security sont téléchargées dans le stockage du Serveur d'administration. Ces *mises à jour* sont installées via la tâche de mise à jour pour Kaspersky Endpoint Security.

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.

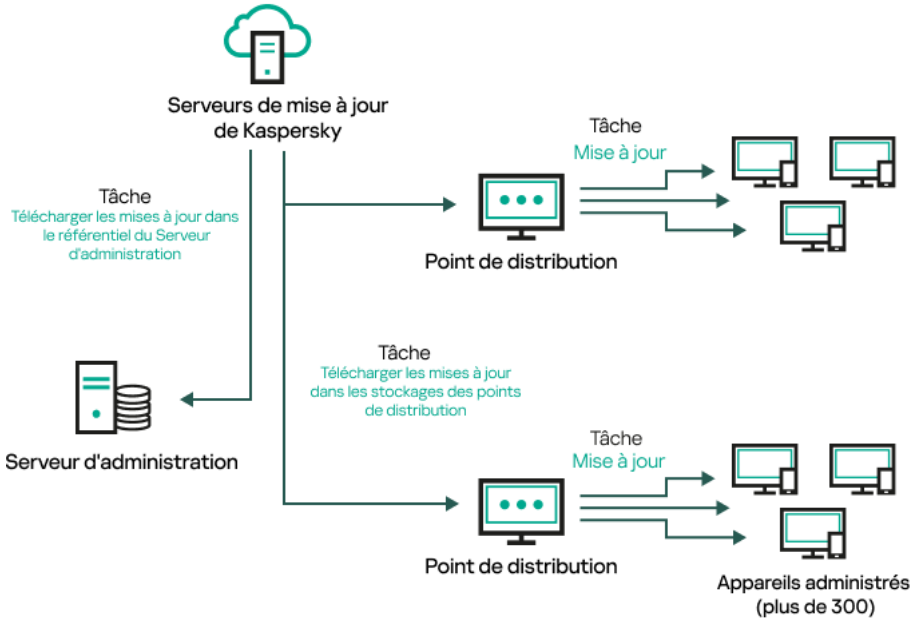
Chaque application de Kaspersky sollicite les mises à jour requises au serveur d'administration. Le Serveur d'administration accumule ces requêtes et télécharge uniquement les mises à jour requises par n'importe quelle application. Cela évite de télécharger les mêmes mises à jour plusieurs fois, voire 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
- ID de configuration 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* de la tâche *Téléchargement des mises à jour sur les stockages des points de distribution*

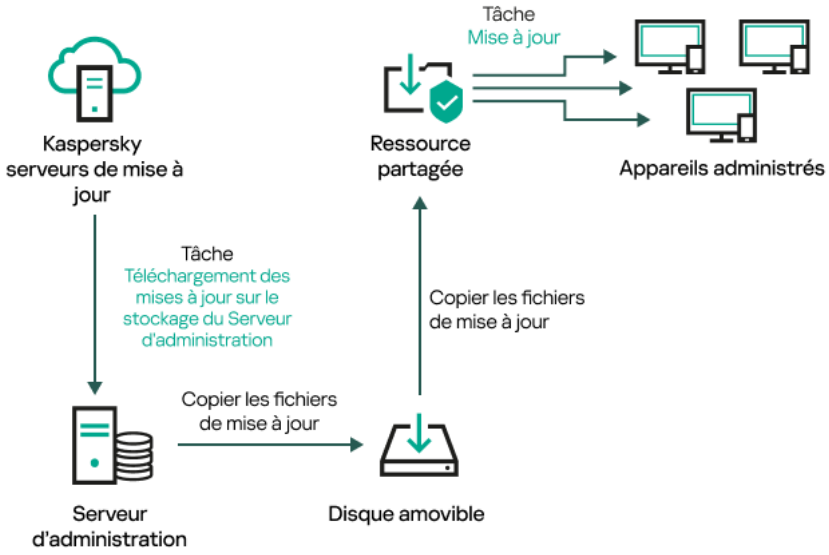
Par défaut, le Serveur d'administration et les points de distribution communiquent avec les serveurs de mise à jour de Kaspersky et télécharge les mises à jour au moyen du protocole HTTPS. Vous pouvez configurer le Serveur d'administration et/ou les points de distribution pour utiliser le protocole HTTP 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.

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 Linux.

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).



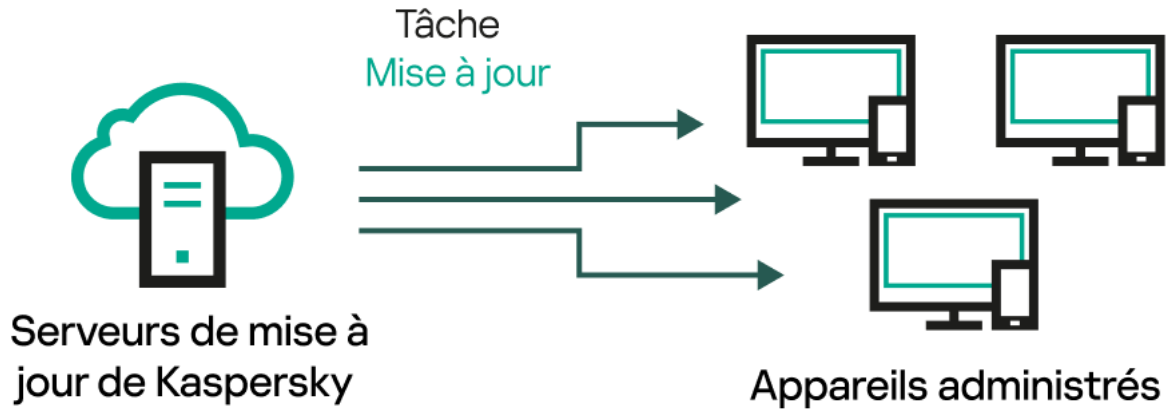
Mise à jour via un dossier local, un dossier partagé ou un serveur FTP

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 Linux
- Aide de Kaspersky Endpoint Security for Windows

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 Linux. 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'application de sécurité. Pour plus d'informations sur ces paramètres, consultez les aides suivantes :

- Aide de Kaspersky Endpoint Security for Linux
- Aide de Kaspersky Endpoint Security for Windows

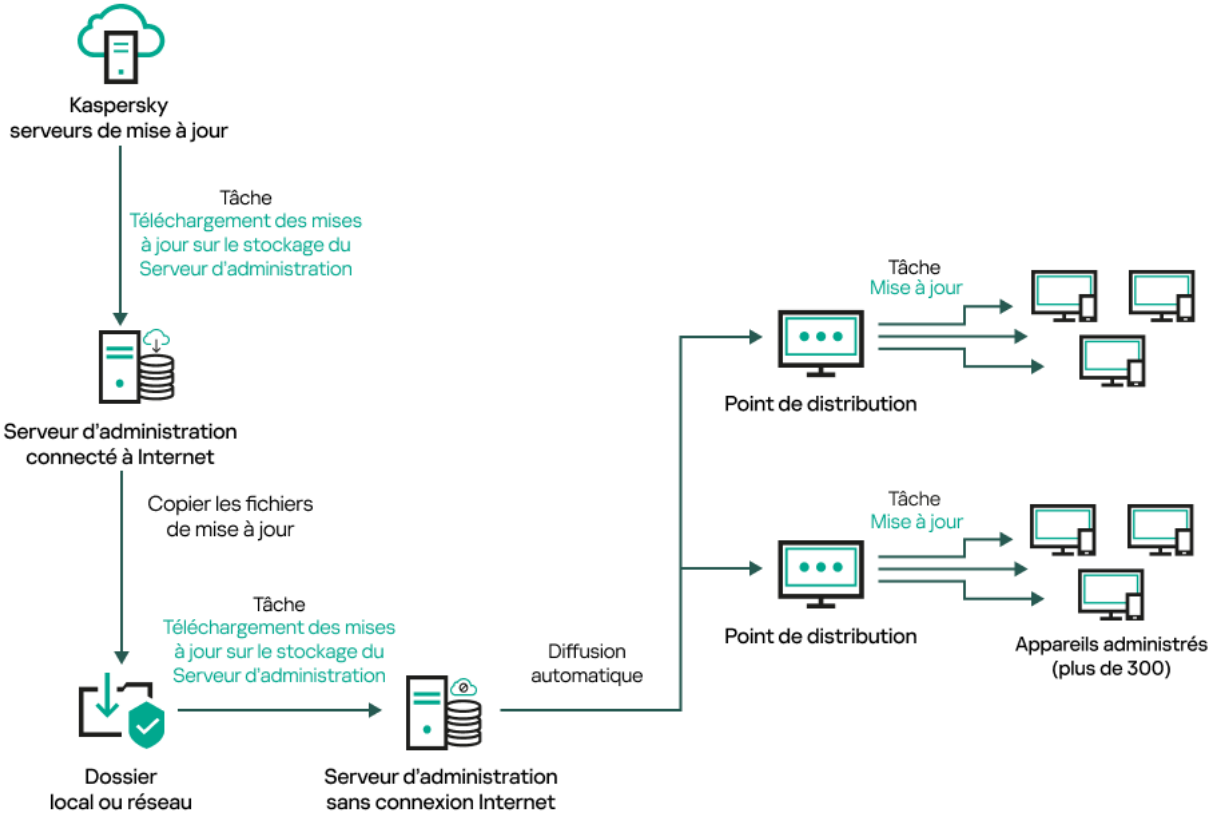
Via un dossier local ou réseau si le Serveur d'administration n'a pas de connexion Internet

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* permet de télécharger les mises à jour des bases de données et des modules logiciels pour les applications de sécurité de Kaspersky depuis les serveurs de mise à jour de Kaspersky vers le stockage du Serveur d'administration.

L'Assistant de Kaspersky Security Center crée automatiquement la tâche *Téléchargement des mises à jour sur le stockage du Serveur d'administration* du Serveur d'administration. La liste des tâches ne peut contenir qu'une seule tâche *Téléchargement des mises à jour sur le stockage du Serveur d'administration*. Vous pouvez recréer cette tâche si elle est supprimée de la liste des tâches du Serveur d'administration.

Une fois que la tâche *Téléchargement des mises à jour sur le stockage du Serveur d'administration* est terminée et que les mises à jour sont téléchargées, elles peuvent être propagées sur les appareils administrés.

Avant de distribuer les mises à jour sur les appareils administrés, vous pouvez exécuter la tâche *Vérification de la mise à jour*. Cela vous permet de vous assurer que le Serveur d'administration installe correctement les mises à jour téléchargées et qu'un niveau de sécurité ne diminue 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. 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 modifier les paramètres de la tâche par défaut. Sinon, vous pouvez configurer les paramètres de la tâche ultérieurement et à tout moment.
6. Cliquez sur le bouton **Terminer**.

   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 des applications**, spécifiez les paramètres suivants :

   - **Sources des mises à jour**

     Comme source de mises à jour, vous pouvez utiliser les serveurs de mise à jour de Kaspersky, un dossier local ou réseau ou un Serveur d'administration primaire.

     Dans la tâche *Téléchargement des mises à jour sur le stockage du Serveur d'administration* et dans la tâche *Téléchargement des mises à jour sur les stockages des points de distribution*, l'authentification de l'utilisateur ne fonctionne pas si vous sélectionnez un dossier local ou réseau protégé par mot de passe comme source de mise à jour. Pour résoudre ce problème, montez d'abord le dossier protégé par mot de passe, puis indiquez les informations d'identification requises, par exemple à l'aide du système d'exploitation. Après cela, vous pouvez sélectionner ce dossier comme source de mise à jour dans une tâche de téléchargement de mise à jour. Kaspersky Security Center Linux ne vous demandera pas de saisir vos identifiants.

- **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.

- **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.

- **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 Linux 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 Linux

  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 :

   - **Lancement planifié** :

     - **Manuel** (Sélectionné par défaut)

       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 vendredi à l'heure système actuelle.

- **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 Linux.

  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.

- **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.

- **Après l'exécution d'une autre tâche**

  La tâche actuelle démarre à la fin d'une autre tâche. Vous pouvez sélectionner comment la tâche antérieure doit se terminer (réussite ou erreur) pour lancer l'exécution de la tâche actuelle. Ce paramètre ne fonctionne que si les deux tâches sont affectées aux mêmes appareils.

- Paramètres supplémentaires 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.

- **Arrêter la tâche si elle prend plus de (min.)**

  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 de mise à jour et d'analyse antivirus d'une application prise en charge par Kaspersky Security Center Linux, par exemple, Kaspersky Endpoint Security for Linux. 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 Linux 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 des applications**, 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 Linux, 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 dans les stockages des points de distribution

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.

*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 des applications** 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.

     - 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. Seul un partage SMB monté peut être utilisé en tant que dossier réseau. Lors de la sélection du dossier local, il faut indiquer le dossier sur l'appareil avec le Serveur d'administration installé.

       Dans la tâche *Téléchargement des mises à jour sur le stockage du Serveur d'administration* et dans la tâche *Téléchargement des mises à jour sur les stockages des points de distribution*, l'authentification de l'utilisateur ne fonctionne pas si vous sélectionnez un dossier local ou réseau protégé par mot de passe comme source de mise à jour. Pour résoudre ce problème, montez d'abord le dossier protégé par mot de passe, puis indiquez les informations d'identification requises, par exemple à l'aide du système d'exploitation. Après cela, vous pouvez sélectionner ce dossier comme source de mise à jour dans une tâche de téléchargement de mise à jour. Kaspersky Security Center Linux ne vous demandera pas de saisir vos identifiants.

   - **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 Linux 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 Linux

    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 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 référentiels 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 :

- **Lancement planifié** :

  - **Manuel** (Sélectionné par défaut)

    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 vendredi à l'heure système actuelle.

- 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 Linux.

  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.

- 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. Vous pouvez sélectionner comment la tâche antérieure doit se terminer (réussite ou erreur) pour lancer l'exécution de la tâche actuelle. Ce paramètre ne fonctionne que si les deux tâches sont affectées aux mêmes appareils.

- 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. 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.

Ajout des sources de mises à jour pour la tâche Télécharger les mises à jour dans le référentiel du Serveur d'administration

Lorsque vous créez ou utilisez la tâche de téléchargement des mises à jour dans le stockage du Serveur d'administration, vous pouvez choisir les sources de mises à jour suivantes :

- Serveurs de mise à jour de Kaspersky
- Serveur d'administration principal

  Cette ressource s'applique aux tâches créées pour un Serveur d'administration virtuel ou secondaire.
- Dossier local ou réseau

Dans la tâche *Téléchargement des mises à jour sur le stockage du Serveur d'administration* et dans la tâche *Téléchargement des mises à jour sur les stockages des points de distribution*, l'authentification de l'utilisateur ne fonctionne pas si vous sélectionnez un dossier local ou réseau protégé par mot de passe comme source de mise à jour. Pour résoudre ce problème, montez d'abord le dossier protégé par mot de passe, puis indiquez les informations d'identification requises, par exemple à l'aide du système d'exploitation. Après cela, vous pouvez sélectionner ce dossier comme source de mise à jour dans une tâche de téléchargement de mise à jour. Kaspersky Security Center Linux ne vous demandera pas de saisir vos identifiants.

Les serveurs de mise à jour de Kaspersky sont utilisés par défaut, mais vous pouvez également télécharger les mises à jour à partir d'un dossier local ou réseau. Vous voudrez peut-être utiliser le dossier si votre réseau n'a pas accès à Internet. Dans ce cas, vous pouvez télécharger manuellement les mises à jour à partir des serveurs de mise à jour de Kaspersky et placer les fichiers téléchargés dans le dossier requis.

Vous ne pouvez indiquer qu'un seul chemin d'accès à un dossier local ou réseau. En tant que dossier local, vous devez spécifier un dossier sur l'appareil où le Serveur d'administration est installé. En tant que dossier réseau, vous pouvez utiliser un serveur FTP ou HTTP ou un partage SMB. Si le partage SMB nécessite une authentification, il doit être monté au préalable dans le système avec les informations d'identification requises. Il est déconseillé d'utiliser le protocole SMB1 car il n'est pas sécurisé.

Si vous ajoutez à la fois les serveurs de mise à jour de Kaspersky et le dossier local ou réseau, les mises à jour seront téléchargées d'abord à partir du dossier. En cas d'erreur lors du téléchargement, les serveurs de mise à jour de Kaspersky seront utilisés.

Pour ajouter les sources de mises à jour :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Tâches**.
2. Cliquez sur **Téléchargement des mises à jour sur le stockage du Serveur d'administration**.
3. Accédez à l'onglet **Paramètres des applications**.
4. Sur la ligne **Sources des mises à jour**, cliquez sur le bouton **Configurer**.
5. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Ajouter**.
6. Dans la liste des sources de mise à jour, ajoutez les sources nécessaires. Si vous cochez la case **Dossier local ou réseau**, indiquez un chemin d'accès au dossier.
7. Cliquez sur **OK**, puis fermez la fenêtre des propriétés de la source de mise à jour.
8. Dans la fenêtre de la source de mise à jour, cliquez sur **OK**.
9. Cliquez sur le bouton **Enregistrer** dans la fenêtre des tâches.

Les mises à jour sont maintenant téléchargées dans le stockage du Serveur d'administration à partir des sources indiquées.

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 des applications** 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 Linux (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*. Elles seront installées localement via l'interface de l'application ou via Kaspersky Security Center Linux.

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.

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 Linux 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.

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

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 la sauvegarde 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 dans les paramètres de stratégie de l'Agent d'administration pour un point de distribution qui reçoit les mises à jour du Serveur d'administration.

   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 la stratégie 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.

Téléchargement des mises à jour par les points de distribution

Kaspersky Security Center Linux permet aux points de distribution d'obtenir des mises à jour du Serveur d'administration, des serveurs Kaspersky, du dossier local ou réseau.

Pour configurer le téléchargement des mises à jour pour 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 via lequel les mises à jour seront livrées aux appareils clients du groupe.

4. Dans la fenêtre des propriétés du point de distribution, sélectionnez la section **Source de mises à jour**.

5. Sélectionnez la source des 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 une 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.

Le point de distribution obtient les mises à jour depuis la source indiquée.

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.

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 : /var/opt/kaspersky/klnagent_srv/1093/.working/share_srv/Updates/.

   Sinon, vous pouvez configurer Kaspersky Security Center Linux 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 Kaspersky Endpoint Security 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.

   Instructions pour :

   - Aide de Kaspersky Endpoint Security for Linux
   - Aide de Kaspersky Endpoint Security for Windows
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 hors ligne qui nécessite l'installation de la mise à jour, lancez la tâche *Mise à jour* de Kaspersky Endpoint Security for Linux ou Kaspersky Endpoint Security for Windows, selon le système d'exploitation de l'appareil hors ligne.

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.

Surveillance, reporting et audit

Cette section décrit les capacités de surveillance et d'élaboration de rapports de Kaspersky Security Center Linux. Ces capacités offrent un aperçu de votre infrastructure, des états de la protection et des statistiques.

Une fois Kaspersky Security Center Linux 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 Linux.

Prérequis

Une fois que vous avez déployé Kaspersky Security Center Linux 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. **Exécution des actions recommandées pour les notifications critiques et d'avertissement**

   Instructions pour :

   Effectuer les actions recommandées pour le réseau de votre organisation

4. **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

5. **Localisation des appareils clients non protégés**

   Instructions pour :

- Contrôlez le widget Nouveaux appareils
- Générez et contrôlez le Rapport sur le déploiement de la protection

6. **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

7. **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 :

   - Limiter le nombre maximum d'événements

8. **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 Linux (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 Linux, 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 Linux 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 Linux 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. Notez que cette option n'affecte pas le nombre maximal d'événements que vous pouvez inclure dans le rapport lorsque vous exportez le rapport dans un fichier.

       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 enregistrer un ou plusieurs rapports au format XML, HTML ou PDF. Kaspersky Security Center Linux vous permet d'exporter simultanément jusqu'à 10 rapports vers des fichiers du format spécifié.

Pour exporter un rapport dans un fichier, procédez comme suit :

1. Dans le menu principal, accédez à **Surveillance et rapports → Rapports**.
2. Sélectionnez les rapports que vous souhaitez exporter.

   Si vous sélectionnez plus de 10 rapports, le bouton **Rapport d'exportation** sera désactivé.
3. Cliquez sur le bouton **Rapport d'exportation**.
4. Dans la fenêtre qui s'ouvre, précisez les paramètres d'export suivants :

   - **Nom du fichier**.

     Si vous sélectionnez un rapport à exporter, indiquez le nom du fichier du rapport.

Si vous sélectionnez plusieurs rapports, les noms des fichiers de rapport coïncideront avec le nom des modèles de rapport sélectionnés.

- **Nombre maximal d'entrées**.

  Indiquez le nombre maximal d'entrées incluses dans le fichier de rapport. La valeur par défaut est de 10 000.

  Vous pouvez exporter un rapport avec un nombre illimité d'entrées. Notez que si votre rapport contient un grand nombre d'entrées, le temps nécessaire à la génération et à l'exportation du rapport augmente.

- **Format de fichier**.

  Sélectionnez le format de fichier du rapport : XML, HTML ou PDF. Si vous exportez plusieurs rapports, tous les rapports sélectionnés sont enregistrés dans le format spécifié dans des fichiers séparés.

  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.

5. Cliquez sur le bouton **Rapport d'exportation**.

Le rapport est enregistré dans un fichier au format indiqué.

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.

Dans les rapports générés, certaines polices peuvent s'afficher de manière incorrecte sur les diagrammes. Pour résoudre ce problème, installez la bibliothèque fontconfig. Vérifiez également que les polices correspondant aux paramètres régionaux de votre système d'exploitation sont installées dans le système d'exploitation.

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 **Détails**, 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. [Optionnel] 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 **Création d'une tâche de remise de rapports**.

4. Ceci permet de lancer l'assistant de création d'une tâche. Parcourez les étapes de l'assistant à l'aide du bouton **Suivant**.

5. À la première page de l'assistant, saisissez le nom de la tâche. Le nom par défaut est **Envoi de rapports (<N>)**, où <N> est le numéro de séquence de la tâche.

6. Sur la page des paramètres de la tâche de l'assistant, définissez les paramètres suivants :

   a. Modèles de rapports que la tâche doit diffuser. Si vous les avez sélectionnés à l'étape 2, ignorez cette étape.

   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.

   d. Si les rapports doivent être enregistrés dans un dossier, avec les paramètres correspondants.

      Après avoir activé l'option **Enregistrer les rapports dans un dossier**, vous devez spécifier un chemin POSIX vers le dossier. Si vous souhaitez enregistrer les rapports dans un dossier partagé, vous devez également cocher la case **Créer un compte utilisateur pour accéder au dossier partagé**, puis spécifier le compte d'utilisateur et le mot de passe pour accéder à ce dossier.

      > Si vous choisissez d'enregistrer les rapports dans un dossier partagé, vous devez garantir l'accès à ce dossier à partir de l'appareil sur lequel le Serveur d'administration est installé. Les moyens de garantir l'accès et les outils utilisés dépendent de votre infrastructure.

      Lors de l'enregistrement des rapports dans un dossier local, les identifiants ne sont généralement pas nécessaires puisque le compte sous lequel le Serveur d'administration s'exécute a accès à ce dossier. Si nécessaire, vous pouvez spécifier les identifiants de l'utilisateur à l'étape **Sélection du compte utilisateur pour exécuter la tâche** de l'assistant.

      Quel que soit le choix du dossier, vous pouvez également cocher la case **Remplacer les rapports précédents du même type** si vous souhaitez que le nouveau fichier de rapport remplace le fichier enregistré dans le dossier de rapports au démarrage de la tâche précédente.

7. Si vous souhaitez modifier un autre paramètre de la tâche une fois que la tâche est créée, sur la page **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**.

8. Cliquez sur le bouton **Créer** pour créer la tâche et fermer l'assistant.

   La tâche de remise de rapports est créée. 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.

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 Linux et sur l'administration du blocage d'événements fréquents.

À propos des événements de Kaspersky Security Center Linux

Kaspersky Security Center Linux 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.

Événements par type

Dans Kaspersky Security Center Linux, 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.

Événements par source

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.

Les événements peuvent être générés par les applications suivantes :

- Modules de Kaspersky Security Center Linux :
  - Serveur d'administration
  - Agent d'administration
- 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.

Événements par niveau d'importance

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 Linux. 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.

Événements des modules de Kaspersky Security Center Linux

Chaque module de Kaspersky Security Center Linux 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 et l'Agent d'administration. 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 Linux 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 Linux 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 stockage des événements : Définition de la durée de stockage d'un événement

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 suivant reprend les événements du Serveur d'administration de Kaspersky Security Center, regroupés par niveau d'importance **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.

Événements critiques du Serveur d'administration

Nom affiché	ID de type	Type d'événement	Description	Durée de

du type d'événement	d'événement			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 Linux 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 Linux définit les règles de génération d'événements lorsqu'une limite de la licence est dépassée.	180 jours
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
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 Linux vérifie si la date d'expiration 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. Ce nombre de jours ne peut pas être modifié. 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 Linux 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 du Serveur d'administration pour l'Administration des appareils mobiles expire. Vous devez mettre à jour le certificat expiré.	180 jours

Événements liés à des erreurs de fonctionnement du Serveur d'administration

Le tableau ci-dessous montre les événements du Serveur d'administration de Kaspersky Security Center au niveau d'importance **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
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
Le dossier en accès public	4108	KLSRV_SHARED_FOLDER_UNAVAILABLE	Ce type d'événements se produit si le dossier partagé du Serveur d'administration n'est pas disponible.	180 jours

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.	
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 le SGBD est installé est disponible. • Affichez les journaux du SGBD pour trouver la raison de l'indisponibilité de la base de données du Serveur d'administration.	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 : • 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 concernant le stockage des événements du Contrôle des applications dans la base de données du Serveur d'administration. Consulter les informations sur la sélection du SGBD.	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

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 Linux 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 Linux 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 Kaspersky Security Center Web Console. • Spécifiez l'intervalle de temps après lequel l'appareil est automatiquement supprimé du groupe à l'aide de Kaspersky Security Center Web Console.	90 jours
Noms d'appareil en conflit	4102	KLSRV_EVENT_HOSTS_CONFLICT	Des événements de ce type se produisent lorsque le Serveur d'administration	90 jours

			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.	
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
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
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
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	4136	KLSRV_APN_CERTIFICATE_EXPIRES_SOON	Les événements de ce type se produisent lorsqu'il reste moins de 14 jours avant	Non stocké

certificat APNs expire bientôt			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.	
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 Google 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 Google Firebase (voir le chapitre " Codes de réponse d'erreur aux messages en aval ").	90 jours
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 Google 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 Google 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 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 Google 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	90 jours

			le Serveur d'administration est installé ne dispose presque plus d'espace libre. Libérez de l'espace disque sur l'appareil.	
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 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 du système d'exploitation sur l'appareil sur lequel 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 du système d'exploitation sur l'appareil sur lequel le serveur d'administration primaire est installé et répondez en conséquence.	90 jours
Les nouvelles mises à jour des modules des applications	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	90 jours

Kaspersky ont été enregistrées			administrés dont l'installation nécessite une autorisation. Approuvez ou refusez les mises à jour à l'aide de Kaspersky Security Center Web Console.	
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

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.

Événements informatifs 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	Ce type d'événements se produit si le serveur d'administration détecte que certaines limites de licence sont sur le point d'être dépassées par les applications Kaspersky installées sur les appareils clients et si le nombre d'unités de licence actuellement utilisé sous licence unique constitue plus de 90 % du nombre total d'unités sous licence.

				Même lorsqu'une limite de licence est dépassée, 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 Linux définit les règles de génération d'événements lorsqu'une limite de la licence est dépassée.
Un nouvel appareil a été détecté	4100	KLSRV_EVENT_HOSTS_NEW_DETECTED	30 jours	Des événements de ce type se produisent lorsque de nouveaux appareils en réseau ont été découverts.
L'appareil a été ajouté automatiquement au groupe	4101	KLSRV_EVENT_HOSTS_NEW_REDIRECTED	30 jours	Ce type d'événements se produit lorsque les appareils ont été attribués à un groupe conformément aux règles de déplacement des appareils.
L'appareil a été supprimé du groupe : longue absence d'activité sur le réseau	4104	KLSRV_INVISIBLE_HOSTS_REMOVED	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 Kaspersky Security Center Web Console. Ces événements incluent l'adresse IP de l'appareil sur lequel le serveur Kaspersky Security Center Web Console est installé.
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	

Événements de l'Agent d'administration

Cette section contient des informations sur les événements liés à l'agent d'administration.

Événements d'avertissement de l'Agent d'administration

Le tableau suivant reprend les événements de l'Agent d'administration, 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	Description	Durée de stockage par défaut
Un problème de sécurité est survenu	549	GNRL_EV_APP_INCIDENT_OCCURED	Ce type d'événements se produit lorsqu'un incident a été détecté sur un appareil. Par exemple, cet événement se produit lorsque l'espace disque est insuffisant.	30 jours
Le proxy KSN a démarré. Échec de la vérification de la disponibilité de KSN	7718	KSNPROXY_STARTED_CON_CHK_FAILED	Des événements de ce type se produisent lorsque la connexion test pour la connexion par proxy à KSN configurée échoue.	30 jours
L'installation de la mise à jour du logiciel tiers a été reportée	7698	KLNAG_EV_3P_PATCH_INSTALL_SLIPPED	Par exemple, des événements de ce type se produisent lorsque le CLUF pour l'installation de la mise à jour tierce est refusée.	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	Téléchargez les fichiers de traçage et vérifiez la valeur du champ KLRI_PATCH_RES_DESC pour en savoir plus.	30 jours
Avertissement renvoyé lors de l'installation des mises à jour des modules de l'application	7701	KLNAG_EV_PATCH_INSTALL_WARNING	Téléchargez les fichiers de traçage et vérifiez la valeur du champ KLRI_PATCH_RES_DESC pour en savoir plus.	30 jours

Événements d'information de l'Agent d'administration

Le tableau suivant reprend les événements de l'Agent d'administration, 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
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
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
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
L'application tierce a été installée	7707	KLNAG_EV_INV_CMPTR_APP_INSTALLED	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
L'installation de la mise à jour du module logiciel est lancée	7700	KLNAG_EV_PATCH_INSTALL_STARTING	30 jours
Partage du bureau Windows : l'application a démarré	7714	KLUSRLOG_EV_PROCESS_LAUNCHED	30 jours
Partage du bureau Windows : le fichier a été modifié	7713	KLUSRLOG_EV_FILE_MODIFIED	30 jours
Partage du bureau Windows : le fichier est lu	7712	KLUSRLOG_EV_FILE_READ	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

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 Linux 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 Linux 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 Linux 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 Linux (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 Linux 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 Linux 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 Linux 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.

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 Linux, 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**, procédez comme suit :

   - 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 **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 **Bloquer**.

     b. Cliquez sur **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 des événements fréquents**, sélectionnez les types d'événements fréquents pour lesquels vous souhaitez supprimer le blocage.

4. Cliquez sur le bouton **Supprimer du blocage**.

L'événement fréquent est supprimé de la liste des événements fréquents. Le Serveur d'administration recevra des événements de ce type.

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 conservation des événements dans la base de données : limiter le nombre d'enregistrements sur les événements et le temps de conservation 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 sur les événements rejetés sont écrites dans le journal du système d'exploitation. Les nouveaux événements sont placés dans une file d'attente et enregistrés dans la base de données dès que la suppression est terminée. Par défaut, la file d'attente des événements est limitée à 20 000 événements. Vous pouvez personnaliser la limite de la file d'attente en modifiant la valeur de l'indicateur KLEVP_MAX_POSTPONED_CNT.

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 Linux 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)
   - **Actualités de la société Kaspersky** (ceci inclut les informations sur les versions des applications 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 Linux 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 statut à un appareil, Kaspersky Security Center Linux tient compte de l'indicateur de visibilité de l'appareil sur le réseau (voir le tableau ci-dessous). Si Kaspersky Security Center Linux 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*
- *Avertissement* ou *Avertissement/Visible*
- *OK* ou *OK/Visible*

Le tableau ci-dessous reprend les conditions d'attribution de l'état *Critique* ou *Avertissement* 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	Certains virus ont été retrouvés sur l'appareil par une tâche de détection de virus, par exemple,	Plus de 0.

été détectés	la tâches d'Analyse des logiciels malveillants, et le nombre de virus détectés dépasse la valeur spécifiée.	
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.
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.	Plus de 0 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.

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 Linux 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 *Avertissement*. 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 jour Kaspersky Security Center Linux à partir de la version précédente, les valeurs de la condition **Les bases sont dépassées** pour attribuer l'état à *Critique* ou *Avertissement* ne changent pas.

Lorsque Kaspersky Security Center Linux attribue un état 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 des paramètres d'envoi des notifications

Vous pouvez configurer une notification à propos des événements qui se produisent dans Kaspersky Security Center Linux. En fonction de la méthode de notification choisie, les types de notifications suivants sont disponibles :

- Email : quand un événement se produit, Kaspersky Security Center Linux envoie une notification aux adresses email indiquées.
- SMS : quand un événement se produit, Kaspersky Security Center Linux 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 Linux :

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 **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 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 Linux vérifie si le certificat d'un serveur SMTP est également signé par une autorité de certification de confiance ou non. Kaspersky Security Center Linux 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.

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.

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 **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 : si ce paramètre n'est pas défini, l'adresse du destinataire sera utilisée. 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.

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.

- 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 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 Linux vérifie si le certificat d'un serveur SMTP est également signé par une autorité de certification de confiance ou non. Kaspersky Security Center Linux 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 **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.

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.

- **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 Linux.

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.

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. Ensuite, activez à nouveau la tâche de protection en temps réel du système de fichiers.

2. Exécutez une tâche d'analyse pour les appareils clients dans un groupe d'administration ou pour des appareils spécifiques, y compris un avec le virus de test 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.

Pour ouvrir un enregistrement de la détection du virus de test :

1. Dans le menu principal, accédez à **Surveillance et rapports** → **Sélections d'événements**.
2. Cliquez sur le nom de la sélection **Derniers événements**.

   Dans la fenêtre qui s'ouvre, la notification concernant le virus de test s'affiche.

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 officiel de l'organisation EICAR.

Notification relative aux événements via un fichier exécutable

Kaspersky Security Center Linux 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 du produit.
%KL_VERSION%	Numéro de version du produit.
%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 Linux et aux applications administrées installées sur les appareils administrés. Kaspersky Security Center Linux met régulièrement à jour les informations de la section en supprimant les annonces obsolètes et en ajoutant de nouvelles informations.

Kaspersky Security Center Linux 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. Par défaut, les annonces liées à la sécurité sont activées. 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 Linux 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 Linux 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. Si vous ne souhaitez pas recevoir les annonces de Kaspersky, vous pouvez désactiver cette fonctionnalité.

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 **Les annonces relatives à la sécurité sont 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 Activée**.

4. Cliquez sur le bouton **Enregistrer**.

   Les annonces marketing sont désactivées.

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 Linux permet de configurer l'exportation des événements vers les systèmes SIEM de l'une des manières suivantes : exportation vers tout système SIEM utilisant le format Syslog ou exportation des événements vers les systèmes SIEM directement depuis la base de données de 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 Linux :

- 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 Linux**

  Procédure : Configuration de l'exportation d'événements dans un système SIEM

- **Sélection des événements que vous souhaitez exporter vers le système SIEM**

  Marquez les événements que vous souhaitez exporter vers le système SIEM. Tout d'abord, marquez les événements généraux qui se produisent dans toutes les applications Kaspersky administrées. Ensuite, vous pouvez marquer les événements pour des applications Kaspersky administrées spécifiques.

- **Configuration de l'exportation des événements vers le système SIEM**

  Vous pouvez exporter des événements en utilisant une des méthodes suivantes :

  - Avec les protocoles TCP/IP, UDP ou TLS par TCP
  - 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

Après avoir configuré l'exportation des événements vers un système SIEM, vous pouvez afficher les résultats de l'exportation si vous avez sélectionné les événements que vous souhaitez exporter.

Conditions préalables

Dans le cadre de la configuration de l'exportation des événements automatique dans Kaspersky Security Center Linux, 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 Linux.

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 Linux et le serveur du système SIEM. Il faut définir cette valeur dans les paramètres de Kaspersky Security Center Linux et les paramètres du récepteur du système SIEM.

- **Protocole**

  Le protocole utilisé pour la transmission des messages depuis Kaspersky Security Center Linux vers le système SIEM. Il faut définir cette valeur dans les paramètres de Kaspersky Security Center Linux et les paramètres du récepteur du système SIEM.

À propos de l'exportation des événements

Kaspersky Security Center Linux 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.

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 Linux vers les systèmes SIEM fait intervenir deux parties : l'expéditeur des événements (Kaspersky Security Center Linux), 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 Linux. L'ordre des configurations n'a pas d'importance : Vous pouvez soit choisir de commencer par configurer l'envoi des événements à Kaspersky Security Center Linux, puis configurer leur réception par le système SIEM, soit l'inverse.

Format Syslog d'exportation d'événements

Vous pouvez envoyer des événements au format Syslog vers n'importe quel système SIEM. Le protocole Syslog permet de transmettre n'importe quel événement survenu sur le Serveur d'administration et dans les applications de Kaspersky installées sur les appareils administrés. Lors de l'exportation des événements au format Syslog vous pouvez choisir exactement les événements qu'il faut transmettre au système SIEM.

Réception des événements par le système SIEM

Le système SIEM doit accepter et analyser correctement les événements en provenance de Kaspersky Security Center Linux. 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 Linux vers les systèmes SIEM fait intervenir deux parties : l'expéditeur des événements (Kaspersky Security Center Linux), et le destinataire de ceux-ci (le système SIEM). Vous devez configurer l'exportation dans votre système SIEM et dans Kaspersky Security Center Linux.

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 Linux. En général, il faut définir les paramètres suivants dans le système SIEM :

- **Protocole d'exportation**

  Un protocole de transfert de messages, UDP, TCP ou TLS, sur TCP. Il est nécessaire d'indiquer le même protocole que celui qui a été choisi dans Kaspersky Security Center Linux pour envoyer les événements.

- **Port**

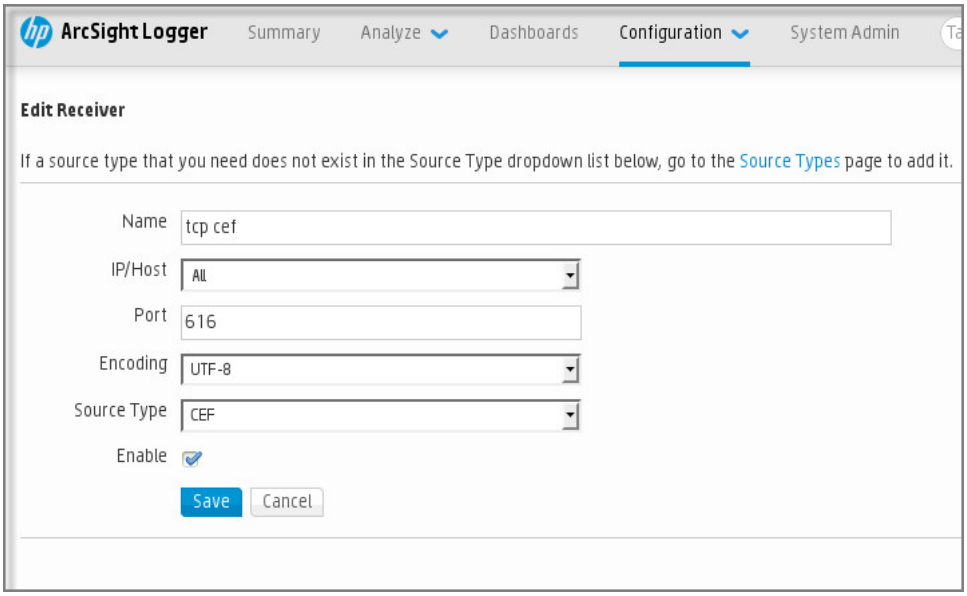
  Indiquez le numéro de port pour vous connecter à Kaspersky Security Center Linux. Il est nécessaire d'indiquer le même numéro de port que celui qui a été choisi dans Kaspersky Security Center Linux lors de la configuration avec un système SIEM.

- **Format de données**

  Spécifiez le format Syslog.

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 Linux 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 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 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 (normes Internet). Le standard RFC 5424 est le standard utilisé pour exporter les événements de Kaspersky Security Center Linux 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 Linux.

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 Linux de telle sorte que les événements soient envoyés au système SIEM. L'envoi des événements de Kaspersky Security Center Linux 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 Linux 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 Linux.

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 **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 Linux et le serveur du système SIEM. Il faut définir cette valeur dans les paramètres de Kaspersky Security Center Linux 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 Linux. Kaspersky Security Center Linux 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 Linux. 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 Linux. Ainsi, vous utiliserez un certificat auto-signé délivré par Kaspersky Security Center Linux. 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 Linux 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 Linux 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 Linux.

  - **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 Linux. Par conséquent, Kaspersky Security Center Linux stocke le certificat auto-signé généré, et vous pouvez transmettre la partie publique du certificat ou l'empreinte SHA1 au système SIEM.

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**.

   c. Cliquez sur le bouton **OK**.

6. Basculez l'option en position **Exporter automatiquement les événements dans la base du système SIEM Activée**.

7. Cliquez sur le bouton **Enregistrer**.

L'exportation vers le système SIEM est configurée. Désormais, si vous avez configuré la réception des événements dans un système SIEM, le Serveur d'administration exporte les événements marqués vers un système SIEM. Si vous définissez la date de début de l'exportation, le Serveur d'administration exporte également les événements marqués stockés dans la base de données du Serveur d'administration à compter de la date indiquée.

Exportation des événements directement depuis la base de données

Vous pouvez extraire les événements directement de la base de données de Kaspersky Security Center Linux sans passer par l'interface de Kaspersky Security Center Linux. 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 Linux 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 Linux, 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 Linux, 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 décrit comment utiliser l'utilitaire klsql2 et exécuter une requête SQL à l'aide de cet utilitaire. Utilisez la version de l'utilitaire klsql2 incluse dans la version Linux de Kaspersky Security Center installée.

Pour utiliser l'utilitaire klsql2 :

1. Accédez au répertoire où le Serveur d'administration est installé. Le chemin d'installation par défaut est /opt/kaspersky/ksc64/sbin.
2. Dans ce répertoire, créez un fichier vierge avec l'extension .sql.
3. Ouvrez le fichier .sql créé à l'aide de n'importe quel éditeur de texte.
4. Dans le fichier .sql, entrez la requête SQL souhaitée, puis enregistrez le fichier.
5. Sur l'appareil sur lequel le Serveur d'administration 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 :
   ```
   sudo ./klsql2 -i src.sql -u <username> -p <password> -o result.xml
   ```
   où `<username>` et `<password>` sont les identifiants du compte qui a accès à la base de données.
6. Si nécessaire, saisissez le login et le mot de passe du compte qui a accès à la base de données.
7. 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 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 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 Linux

Pour accéder à la base de données Kaspersky Security Center Linux à l'aide des outils d'administration de base de données 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 Linux, 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 **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.

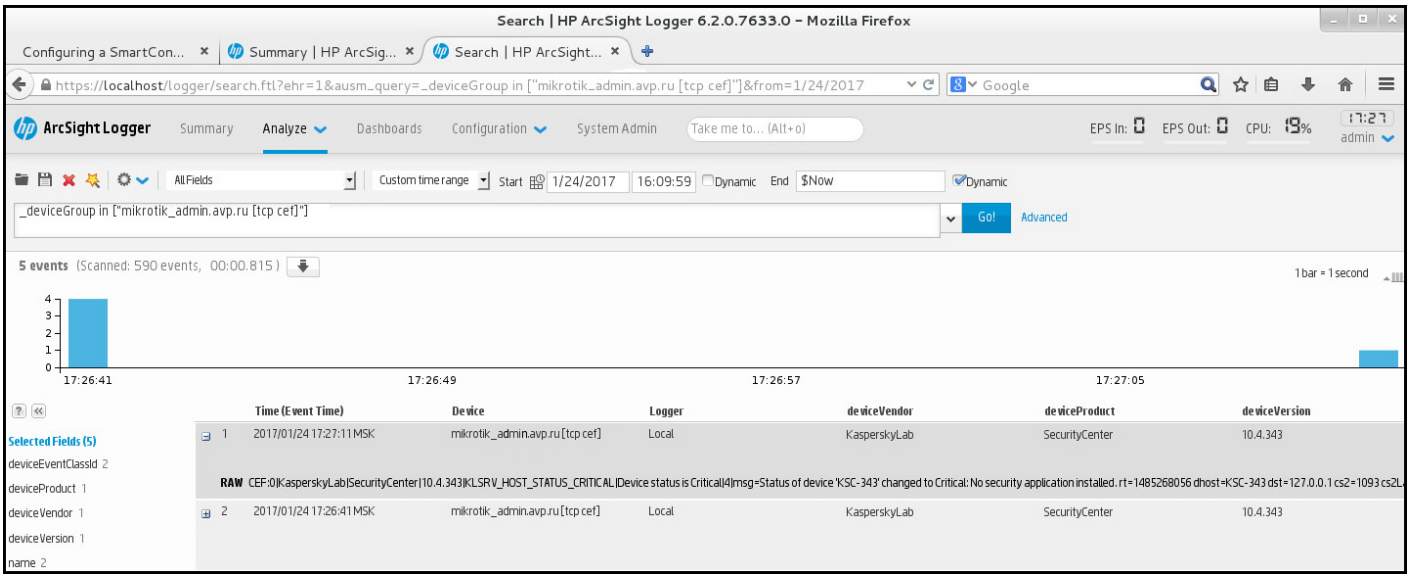
Consultation des résultats de l'exportation

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 Linux 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 Linux 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 des révisions des objets

Cette section contient les informations sur l'utilisation des révisions des objets. Kaspersky Security Center Linux 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 consulter la liste des révisions et annuler les modifications apportées à un objet dans une révision sélectionnée.

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.
- **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.

Suppression d'objets

Cette section explique comment supprimer des objets et consulter les informations relatives à ces objets une fois qu'ils ont été supprimés.

Vous pouvez supprimer les objets suivants :

- Stratégies
- Tâches
- Paquets d'installation
- Serveurs d'administration virtuels
- Utilisateurs
- Groupes de sécurité
- Groupes d'administration

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 Linux 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.

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 Linux 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.

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.

À propos de la suppression d'objets des référentiels Quarantaine, Sauvegarde ou Menaces actives

Lorsque les applications de sécurité Kaspersky installées sur les appareils clients placent des objets dans les référentiels Quarantaine, Sauvegarde ou Menaces actives, elles envoient les informations sur les objets ajoutés aux sections **Quarantaine**, **Sauvegarde**, ou alors **Menaces actives** dans Kaspersky Security Center Linux. Lorsque vous ouvrez l'une de ces sections, sélectionnez un objet dans la liste et cliquez sur le bouton **Supprimer**, Kaspersky Security Center Linux effectue l'une des actions suivantes ou les deux actions :

- Supprime l'objet sélectionné de la liste
- Supprime l'objet sélectionné du référentiel

L'action à effectuer est définie par l'application Kaspersky qui a placé l'objet sélectionné dans le référentiel. L'application Kaspersky est indiquée dans le champ **Entrée ajoutée par**. Reportez-vous à la documentation de l'application Kaspersky pour plus de détails sur l'action à effectuer.

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 des applications**, 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 informations système à partir d'un appareil client

Pour télécharger les informations système 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 **Informations système**.
3. Cliquez sur le bouton **Télécharger** pour télécharger les informations système sur l'appareil client.

   Si vous obtenez des informations système sur un appareil Linux, un fichier de vidage pour les applications terminées en urgence est ajouté au fichier résultant.

Le fichier avec les informations est téléchargé 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 Linux et télécharger les résultats

Pour lancer le diagnostic de l'Agent d'administration de Kaspersky Security Center Linux 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 Linux**.

   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 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 Linux.

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 Linux.

Exécution de diagnostics à distance sur un appareil client basé sur Linux

Kaspersky Security Center Linux 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 Linux, 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.

Administration des applications et des fichiers exécutables tiers sur les appareils clients

Cette section décrit les fonctions de Kaspersky Security Center Linux associées à l'administration des applications et des fichiers exécutables tiers exécutés 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 module Contrôle des applications est disponible à partir de Kaspersky Endpoint Security 11.2 for Linux.

Prérequis

- Kaspersky Security Center Linux est déployé dans votre entreprise.
- La stratégie de Kaspersky Endpoint Security for Linux ou de Kaspersky Endpoint Security for Windows est créée et activée. Le module Contrôle des applications est activé dans la stratégie.

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 : obtenir et consulter une liste des fichiers exécutables installés sur les appareils clients

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.

   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 de fichiers exécutables dans Kaspersky Security Center Linux :

- Catégorie complétée à la main. vous définissez des conditions, par exemple les métadonnées du fichier, le hashcode du fichier, le certificat du fichier, 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.

3. **Configuration du Contrôle des applications dans la stratégie Kaspersky Endpoint Security**

   Configurez le composant Contrôle des applications dans la stratégie Kaspersky Endpoint Security for Linux à l'aide des catégories que vous avez créées à l'étape précédente.

   Instructions pour : Configuration du Contrôle des applications dans la stratégie Kaspersky Endpoint Security for Windows

4. **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 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.

5. **Modification des paramètres 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 pratiques : Kaspersky Security Center Web Console : Ajout de fichiers exécutables liés par un événement à la catégorie de l'application

6. **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.

7. **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 l'aide de Kaspersky Endpoint Security for Linux et Aide de Kaspersky Endpoint Security for Windows.

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 composant Contrôle des applications est disponible pour Kaspersky Endpoint Security 11.2 for Linux et les versions ultérieures.

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 Linux :

- Catégorie complétée à la main. vous définissez des conditions, par exemple les métadonnées du fichier, le hashcode du fichier, le certificat du fichier, 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 l'aide de Kaspersky Endpoint Security for Linux et Aide de Kaspersky Endpoint Security for Windows.

Obtention et consultation d'une liste des applications installées sur les appareils client

Kaspersky Security Center Linux 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.

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.

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 l'aide de Kaspersky Endpoint Security for Linux et Aide de Kaspersky Endpoint Security for Windows.

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

Pour Kaspersky Endpoint Security for Linux, la fonction d'inventaire des fichiers exécutables est disponible depuis la version 11.2.

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.

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 **Nouvelle tâche**, dans la liste déroulante **Application**, sélectionnez Kaspersky Endpoint Security for Linux ou Kaspersky Endpoint Security for Windows, selon le 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 l'aide de Kaspersky Endpoint Security for Linux et l'aide de Kaspersky Endpoint Security for Windows.

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**, spécifiez le nom de la catégorie de l'application et 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 La chemin d'accès au fichier du le dossier sur l'appareil client dont les fichiers exécutables seront ajoutés dans une catégorie d'applications définie par l'utilisateur.

- 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 Linux 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 for Linux prend en charge le calcul SHA256.

Choisissez une des options du calcul de la fonction hash par l'application Kaspersky Security Center Linux pour les fichiers de la catégorie :

- Si toutes les instances des applications de sécurité installées sur votre réseau sont Kaspersky Endpoint Security for Linux, cochez la case **SHA-256**.
- Cochez la case **Hash MD5** uniquement si vous utilisez Kaspersky Endpoint Security for Windows. Kaspersky Endpoint Security for Linux ne prend pas en charge la fonction de hachage 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 le dossier archivé

Si cette option est sélectionnée, vous pouvez spécifier un fichier d'un dossier archivé, puis sélectionner la condition à utiliser pour ajouter des applications à la catégorie d'utilisateurs. Le dossier archivé est décompressé et les conditions que vous sélectionnez sont appliquées aux fichiers du dossier. Comme condition, vous pouvez sélectionner l'un des critères suivants :

- **Hash du fichier**

  Vous sélectionnez la fonction de hachage (MD5 ou SHA256) que vous souhaitez utiliser pour calculer les valeurs de hachage. Les applications, possédant les mêmes valeurs de hachage que les fichiers du dossier archivé, seront ajoutées dans une catégorie d'applications définie par l'utilisateur.

  Sélectionnez une fonction de hachage MD5 uniquement si vous utilisez Kaspersky Endpoint Security for Windows. Kaspersky Endpoint Security for Linux ne prend pas en charge la fonction de hachage MD5.

- **Données méta**

  Vous sélectionnez les métadonnées que vous souhaitez utiliser comme critères. Les fichiers exécutables, possédant les mêmes données méta, seront ajoutés dans une catégorie d'applications définie par l'utilisateur.

- **Certificat**

  Vous sélectionnez les propriétés de certificat (objet du certificat, empreinte digitale ou émetteur) que vous souhaitez utiliser comme critères. Les fichiers exécutables signés conformément aux certificats et qui en possèdent les mêmes propriétés seront ajoutés à la catégorie utilisateur.

Si cette option est sélectionnée, vous pouvez spécifier un fichier d'un dossier archivé, puis sélectionner la condition à utiliser pour ajouter des applications à la catégorie d'utilisateurs. Le dossier archivé est décompressé et les conditions que vous sélectionnez sont appliquées aux fichiers du dossier. Comme condition, vous pouvez sélectionner l'un des critères suivants :

- **Hash du fichier**

  Vous sélectionnez la fonction de hachage (MD5 ou SHA256) que vous souhaitez utiliser pour calculer les valeurs de hachage. Les applications, possédant les mêmes valeurs de hachage que les fichiers du dossier archivé, seront ajoutées dans une catégorie d'applications définie par l'utilisateur.

  Sélectionnez une fonction de hachage MD5 uniquement si vous utilisez Kaspersky Endpoint Security for Windows. Kaspersky Endpoint Security for Linux ne prend pas en charge la fonction de hachage MD5.

- **Données méta**

  Vous sélectionnez les métadonnées que vous souhaitez utiliser comme critères. Les fichiers exécutables, possédant les mêmes données méta, seront ajoutés dans une catégorie d'applications définie par l'utilisateur.

- **Certificat**

  Vous sélectionnez les propriétés de certificat (objet du certificat, empreinte digitale ou émetteur) que vous souhaitez utiliser comme critères. Les fichiers exécutables signés conformément aux certificats et qui en possèdent les mêmes propriétés seront ajoutés à la catégorie 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 l'aide de Kaspersky Endpoint Security for Linux et Aide de Kaspersky Endpoint Security for Windows.

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.

Assurez-vous que les conditions préalables suivantes sont remplies :

- Le module Contrôle des applications est activé dans la stratégie de Kaspersky Endpoint Security.
- Une liste des fichiers exécutables stockés sur les appareils administrés a été obtenue.

Pour créer une catégorie d'applications 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 de fichiers exécutables 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**, indiquez 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 **Ajouter**.

5. Dans la fenêtre qui s'ouvre, sélectionnez l'appareil (les appareils) dont les fichiers exécutables seront utilisés pour créer la catégorie d'applications.

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 Linux 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 for Linux prend en charge le calcul SHA256.

Choisissez une des options du calcul de la fonction hash par l'application Kaspersky Security Center Linux pour les fichiers de la catégorie :

- Si toutes les instances des applications de sécurité installées sur votre réseau sont Kaspersky Endpoint Security for Linux, cochez la case **SHA-256**.

Cochez la case **Hash MD5** uniquement si vous utilisez Kaspersky Endpoint Security for Windows. Kaspersky Endpoint Security for Linux ne prend pas en charge la fonction de hachage 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 SHA-256 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 Linux 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 for Linux prend en charge le calcul SHA256.

Choisissez une des options du calcul de la fonction hash par l'application Kaspersky Security Center Linux pour les fichiers de la catégorie :

- Si toutes les instances des applications de sécurité installées sur votre réseau sont Kaspersky Endpoint Security for Linux, cochez la case **SHA-256**.

Cochez la case **Hash MD5** uniquement si vous utilisez Kaspersky Endpoint Security for Windows. Kaspersky Endpoint Security for Linux ne prend pas en charge la fonction de hachage 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 l'aide de Kaspersky Endpoint Security for Linux et Aide de Kaspersky Endpoint Security for Windows.

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.

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 des applications** → **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. Utilisez le bouton à bascule **Contrôle des applications DÉSACTIVÉ** pour désactiver l'option.

5. Dans les paramètres de blocage des paramètres du **Contrôle des applications**, activez le mode de fonctionnement pour 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 du 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 enregistre 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 l'aide de Kaspersky Endpoint Security for Linux et Aide de Kaspersky Endpoint Security for Windows.

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, 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 de l'application :

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 SHA-256 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.

- **SHA-256 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)**

  Sélectionnez cette option uniquement si vous utilisez Kaspersky Endpoint Security for Windows. Kaspersky Endpoint Security for Linux ne prend pas en charge la fonction de hachage MD5.

  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.

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 l'aide de Kaspersky Endpoint Security for Linux et Aide de Kaspersky Endpoint Security for Windows.

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. Vous pouvez automatiser les tâches que vous ne souhaitez peut-être pas administrer manuellement. 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. En utilisant OpenAPI, vous pouvez développer une application cliente.

Vous pouvez utiliser le champ de recherche dans la partie droite de l'écran pour localiser les informations dont vous avez besoin dans le guide de référence d'OpenAPI.

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 Linux 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 Linux.

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 de Serveurs d'administration, ajout d'un Serveur d'administration secondaire et suppression d'une hiérarchie de Serveurs d'administration
Télécharger les fichiers avec la liste des réseaux via la passerelle de connexion vers l'hôte 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	Vous pouvez vous connecter au Serveur d'administration primaire, télécharger une clé de licence requise à partir de celui-ci et	Licence des applications administrées

d'administration sur les Serveurs d'administration secondaires	transmettre cette clé à tous les Serveurs d'administration secondaires inclus dans une hiérarchie.	
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
Démarrer la tâche de l'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
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.	Gérer les 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.	Ajout d'un compte d'un utilisateur interne
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 utilisateurs et des rôles d'utilisateur

Applications interagissant avec Kaspersky Security Center Linux via OpenAPI

Certaines applications interagissent avec Kaspersky Security Center Linux 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 Linux 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 Linux 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 Linux.

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 Linux

Lors de la planification du déploiement des modules de Kaspersky Security Center Linux 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 50 000 appareils. Si le total des appareils sur le réseau d'une entreprise est supérieur à 50 000, 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 Kaspersky Security Center Web Console
- 8060 TCP : port HTTP, utilisé pour la publication des paquets autonomes à l'aide des outils de Kaspersky Security Center Web Console
- 13292 TCP : ce port TLS est requis uniquement s'il faut administrer des appareils mobiles

- 8080 TCP : port HTTPS pour Kaspersky Security Center Web Console

Configuration typique de Kaspersky Security Center Linux

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 50 000 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 probablement pas sonder le réseau du client MSP, 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 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) (option **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.

Un client MSP peut souhaiter gérer les appareils Android et appareils iOS des employés. Le Serveur d'administration gère les appareils mobiles via TLS, port TCP 13292.

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

- 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

Certaines entreprises clientes, par exemple MSP, peuvent exécuter plusieurs Serveurs d'administration. L'administration de plusieurs serveurs hétérogènes n'est pas pratique et pour cette raison, il est utile de les regrouper dans une hiérarchie. Dans la hiérarchie, un Serveur d'administration basé sur Linux peut fonctionner à la fois comme Serveur primaire et comme Serveur secondaire. Le Serveur primaire basé sur Linux peut gérer à la fois les Serveurs secondaires Linux et Windows. Un Serveur Windows primaire peut administrer un Serveur Linux secondaire.

La configuration " primaire/secondaire " entre deux Serveurs d'administration offre les possibilités suivantes :

- Un Serveur d'administration secondaire hérite des stratégies, des tâches, des rôles d'utilisateur et des paquets d'installation du Serveur d'administration primaire, évitant ainsi la duplication des paramètres.
- 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.
- Un Serveur d'administration principal peut être utilisé comme source de mises à jour pour un Serveur d'administration secondaire.

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.

Déploiement et configuration initiale

Kaspersky Security Center Linux est une application distribuée. Kaspersky Security Center Linux 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.
- 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 Linux dans le réseau de l'entreprise se réalise comme suit :

- Installation du Serveur d'administration
- Installation de Kaspersky Security Center Web Console
- 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

Avant de commencer le déploiement de Kaspersky Security Center Linux sur un cluster de basculement, vous devez créer des comptes pour les services Kaspersky Security Center Linux.

Pour ce faire, exécutez les étapes suivantes sur le nœud actif, le nœud passif et le serveur de fichiers :

1. Créez un groupe portant le nom " kladmins " et attribuez le même GID aux trois groupes.
2. Créez un compte utilisateur portant le nom " ksc " et attribuez le même UID aux trois comptes utilisateur. Définissez le groupe principal sur 'kladmins' pour les comptes créés.
3. Créez un compte utilisateur avec le nom " rightless " et attribuez le même UID aux trois comptes utilisateur. Définissez le groupe principal sur 'kladmins' pour les comptes créés.

Choix d'un SGBD

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
MySQL (voir versions supportées)	Utilisez ce SGBD si vous prévoyez d'utiliser un seul Serveur d'administration pour moins de 20 000 appareils.
MariaDB (voir versions supportées)	Utilisez ce SGBD si vous prévoyez d'utiliser un seul Serveur d'administration pour moins de 20 000 appareils.
PostgreSQL, Postgres Pro (cf. les versions compatibles)	Utilisez ce SGBD si vous prévoyez d'utiliser un seul Serveur d'administration pour moins de 50 000 appareils.

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

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.

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.

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

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.

Indication de l'adresse du Serveur d'administration

Lors de l'installation du Serveur d'administration, il faut indiquer le nom DNS ou l'adresse IP statique 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 Kaspersky Security Center Web Console, toutefois dans ce cas elle n'est pas modifiée automatiquement dans les paquets d'installation de l'Agent d'administration déjà créés.

Déploiement de l'Agent d'administration et des applications de sécurité

Pour gérer les appareils d'une organisation et les protéger contre les menaces de sécurité, vous devez installer l'Agent d'administration et une application de sécurité Kaspersky sur chacun d'eux.

Pour plus d'informations sur le déploiement de la protection, reportez-vous à la section Déploiement de l'Agent d'administration et de l'application de sécurité.

Sous Microsoft Windows XP, l'Agent d'administration peut ne pas exécuter correctement les opérations suivantes : télécharger les mises à jour directement depuis les serveurs Kaspersky (en tant que point de distribution) et fonctionner en tant que serveur proxy KSN (en tant que point de distribution).

Configuration de la protection sur le réseau d'une entreprise cliente

Après la fin de l'installation du Serveur d'administration, Kaspersky Security Center Web Console, 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.

Lorsque vous modifiez un paramètre, gardez à l'esprit que vous pouvez verrouiller ou déverrouiller le paramètre afin d'interdire ou d'autoriser la modification de sa valeur sur un 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 Linux (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 Kaspersky Security Center Web Console, 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. Si la planification de la tâche d'analyse de groupe définie automatiquement ne convient pas à votre entreprise, vous devez configurer manuellement la planification qui vous convient le mieux pour cette tâche sur la base des règles de travail adoptées dans l'entreprise.

Par exemple, 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 l'entreprise sont désactivés les vendredis à 18:30, la tâche d'analyse de l'appareil ne sera jamais lancée. Dans ce cas, vous devez configurer la tâche d'analyse de groupe manuellement.

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 Linux 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 portée des stratégies est définie avec, par exemple, des balises d'appareil, des rôles d'utilisateur.

- 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.

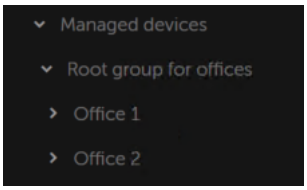
Les moyens suivants de construction de la structure de groupes d'administration existent :

- 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 ou traceroute 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 Linux, 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 Linux 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 Linux 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

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 Kaspersky Security Center Web Console, mais aussi par l'utilisateur de l'appareil à distance (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 le journal des événements Syslog et dans le journal des événements de Kaspersky Security Center Linux, de manière centralisée sur le Serveur d'administration et localement 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

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 : 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 plus, les règles de déplacement de l'appareil peuvent être créées explicitement par l'administrateur de Kaspersky Security Center Linux, dans la section **Ressources (Appareils) → Règles de déplacement**.

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 un appareil a déjà été déplacé par cette règle, la règle ne le déplacera plus jamais, même si vous remettez manuellement l'appareil dans le groupe des appareils non attribués. 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 Linux (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.

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 Linux 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.

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 Linux 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.

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.

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 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 DNS ou adresse 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.
- Exécutez l'utilitaire klbackup et effectuez 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. Exécutez l'utilitaire klbackup et effectuez 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 Linux et par conséquent, un mauvais fonctionnement de l'application.

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 Linux 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.

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 Linux 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 ou la réception des statistiques de l'application administrée. 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 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.

3. Dans la fenêtre des propriétés de l'appareil, dans la section **Général**, activez 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 Kaspersky Security Center Web Console, cet appareil est affiché comme étant arrêté. 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 Kaspersky Security Center Web Console, 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 Linux 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.

La fenêtre des propriétés d'un appareil administré contient le bouton **Forcer la synchronisation**. Quand Kaspersky Security Center Linux 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.

Guide de dimensionnement

Cette section fournit des informations sur la mise à l'échelle de Kaspersky Security Center Linux.

Présentation du manuel

Le guide de dimensionnement de Kaspersky Security Center Linux (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.

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

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.

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 réseau comporte 50 000 appareils

Configuration de l'appareil avec le Serveur d'administration

Matériel	Valeur
Processeur	8 cœurs (12 cœurs recommandés), 2 500 MHz
Mémoire vive	16 Go
Espace disque	300 Go, 150 IOPS ou plus

Configuration de l'appareil sur lequel le SGBD PostgreSQL est installé

Matériel	Valeur
Processeur	16 noyaux, 2500 MHz
Mémoire vive	32 Go
Espace disque	300 Go, 150 IOPS ou plus

Configuration de l'appareil sur lequel le Serveur d'administration et le SGBD PostgreSQL sont installés

Matériel	Valeur
Processeur	24 cœurs (28 cœurs recommandés), 2 500 MHz
Mémoire vive	48 Go
Espace disque	600 Go, 300 IOPS ou plus

Le réseau comporte 30 000 appareils

Configuration de l'appareil avec le Serveur d'administration

Matériel	Valeur
Processeur	6 cœurs (8 cœurs recommandés), 2 500 MHz

Mémoire vive	12 Go
Espace disque	200 Go, 150 IOPS ou plus

Configuration de l'appareil sur lequel le SGBD PostgreSQL est installé

Matériel	Valeur
Processeur	12 noyaux, 2500 MHz
Mémoire vive	24 Go
Espace disque	250 Go, 150 IOPS ou plus

Configuration de l'appareil sur lequel le Serveur d'administration et le SGBD PostgreSQL sont installés

Matériel	Valeur
Processeur	18 cœurs (20 cœurs recommandés), 2 500 MHz
Mémoire vive	36 Go
Espace disque	450 Go, 300 IOPS ou plus

Le réseau comporte 10 000 appareils

Configuration de l'appareil avec le Serveur d'administration

Matériel	Valeur
Processeur	4 cœurs (6 cœurs recommandés), 2 500 MHz
Mémoire vive	8 Go
Espace disque	100 Go, 150 IOPS ou plus

Configuration de l'appareil sur lequel le SGBD PostgreSQL est installé

Matériel	Valeur
Processeur	8 noyaux, 2500 MHz
Mémoire vive	18 Go
Espace disque	200 Go, 150 IOPS ou plus

Configuration de l'appareil sur lequel le Serveur d'administration et le SGBD PostgreSQL sont installés

Matériel	Valeur
Processeur	12 cœurs (14 cœurs recommandés), 2 500 MHz
Mémoire vive	26 Go
Espace disque	300 Go, 300 IOPS ou plus

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.
- Le SGBD PostgreSQL n'inclut pas d'extensions autres que plpgsql.

Sur l'appareil sur lequel est installé le SGBD, la base de données occupe environ 100 Go d'espace disque et le journal des transactions environ 200 Go d'espace disque.

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.

Pendant l'utilisation, il se forme toujours ce que l'on appelle de l'*espace non alloué* (unallocated space) dans la base de données. Par conséquent, la taille réelle du fichier de la base de données s'avère souvent être environ deux fois plus grande que l'espace occupé dans la base de données.

Il n'est pas recommandé de limiter explicitement la taille du journal des transactions. Il est recommandé de conserver la valeur par défaut du paramètre MAXSIZE.

Calcul de l'espace disque

L'espace sur le disque du Serveur d'administration requis pour le dossier /var/opt/kaspersky/klnagent_srv/ 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 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 Linux crée un enregistrement pour cette VM dynamique dans Kaspersky Security Center Web Console 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 Linux 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 Linux et du Serveur d'administration et peuvent réduire les performances de Kaspersky Security Center Linux et du SGBD. Nous vous recommandons de connecter jusqu'à 20 000 VM dynamiques à Kaspersky Security Center Linux.

Vous pouvez connecter plus de 20 000 VM dynamiques à Kaspersky Security Center Linux 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

La configuration matérielle et logicielle requise pour les points de distribution Windows et Linux est décrite dans cet article.

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.

Il n'est pas recommandé de désigner le Serveur d'administration comme point de distribution, car la charge sur le Serveur d'administration augmentera.

Configuration matérielle requise pour les points de distribution Windows

Configuration matérielle minimale requise pour les points de distribution Windows

Nombre d'appareils clients	Processeur	Mémoire vive	RAM, avec la gestion des correctifs activée	Espace disque
10 000	4 noyaux, 2500 MHz	8 Go	8 Go	120 Go
5 000	4 noyaux, 2500 MHz	6 Go	8 Go	120 Go
1000	2 noyaux, 2 500 MHz	4 Go	8 Go	120 Go

Configuration matérielle requise pour les points de distribution basés sur Linux

Configuration matérielle minimale requise pour les points de distribution Linux

Nombre d'appareils clients	Processeur	Mémoire vive	Espace disque
10 000	4 noyaux, 2500 MHz	10 Go	120 Go
5 000	4 noyaux, 2500 MHz	8 Go	120 Go
1000	2 noyaux, 2 500 MHz	6 Go	120 Go

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.

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 Linux.
- Le journal du système d'exploitation commence à afficher 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).

Bonnes pratiques pour un Serveur d'administration qui gère un grand nombre d'appareils

Meilleures pratiques d'utilisation des SGBD

Configurez l'exécution régulière de la tâche de **Maintenance du Serveur d'administration**, surtout si vous utilisez un SGBD PostgreSQL.

Excluez le dossier SGBD de l'analyse IOC.

Meilleures pratiques pour les stratégies et les profils

Réduisez le nombre de stratégies actives pour un module (par exemple, Kaspersky Endpoint Security for Windows). Vous pouvez remplacer des stratégies par des profils de stratégie.

Bonnes pratiques pour un Serveur d'administration qui gère un grand nombre d'appareils

Réduisez le nombre de tâches exécutées simultanément, en particulier l'installation à distance et la gestion des correctifs.

Réduisez le nombre et optimisez le calendrier des tâches liées aux sélections d'appareils.

Dans la section **Configuration des événements** des paramètres de la stratégie, réduisez le nombre de types d'événements enregistrés.

Bonnes pratiques en matière de stockage des événements

Réduisez la fréquence des événements de type unique à partir du module Contrôle des applications. Pour en savoir plus, consultez la section suivante : À propos du blocage des événements fréquents.

Réduisez la durée de stockage des événements des modules (par exemple, Kaspersky Endpoint Security for Windows) et des événements d'information sur les vulnérabilités corrigées.

Activez l'option **Sauvegarder les événements relatifs à la progression de la tâche** dans les paramètres des tâches courantes, comme les tâches de mise à jour. Pour en savoir plus, consultez la section suivante : Conservation des événements pour les tâches et les stratégies.

Optimisez les paramètres de la tâche d'inventaire. Pour en savoir plus, consultez la section suivante : Tâche d'inventaire.

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 de la base de données et les tâches de groupe de la mise à jour de Kaspersky Endpoint Security font partie des fonctionnalités de base de Kaspersky Security Center Linux.

La tâche d'inventaire entre dans la fonctionnalité de Gestion des vulnérabilités et des correctifs et n'est pas accessible, si cette fonctionnalité n'est pas activée.

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 de la base de données

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 Linux 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.

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	Trafic de chaque appareil

	d'administration vers chaque appareil administré	administré vers le Serveur d'administration
Installation de Kaspersky Endpoint Security for Linux 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 for Linux	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 for Linux 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.

Moyens de bénéficier de l'assistance technique

Si vous ne trouvez pas de solution à votre problème dans la documentation de Kaspersky Security Center Linux ou dans les sources d'information relatives à Kaspersky Security Center Linux, 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 Linux.

Kaspersky apporte un soutien en relation avec Kaspersky Security Center Linux 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 répertoire /var/lib/systemd/coredump. Les fichiers de vidage sont conservés tant que Kaspersky Security Center Linux 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 plante, vous pouvez contacter le Support Technique de Kaspersky. Un expert du 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 Linux sur le site Internet de Kaspersky

La page Kaspersky Security Center Linux sur le site Internet de Kaspersky fournit des informations générales sur l'application, ses possibilités, et ses particularités.

Page Kaspersky Security Center Linux dans la Base de connaissances

La *Base de connaissances* est une section du site Internet du Support Technique de Kaspersky.

Sur la page de Kaspersky Security Center Linux de la Base de connaissances, vous pouvez lire des articles qui fournissent 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 Linux 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.

Problèmes connus

Kaspersky Security Center Linux présente une série de restrictions qui n'ont pas une incidence critique sur le fonctionnement de l'application :

- 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 votre réseau inclut un domaine Microsoft Active Directory qui contient plusieurs dizaines de milliers d'objets (appareils administrés, groupes de sécurité et comptes utilisateurs) et que la taille de la page de réponse (le paramètre `MaxPageSize`) est inférieure à 5 000, le sondage du contrôleur de domaine n'est pas disponible et les informations sur les objets du domaine ne sont pas reçues. Lorsque vous essayez d'interroger le contrôleur de domaine, l'erreur *Taille limite dépassée* s'affiche. L'augmentation de la taille de la page de réponse peut aider à corriger l'erreur. Vous pouvez utiliser l'utilitaire Ntdsutil.exe pour augmenter la valeur du paramètre `MaxPageSize` sur `5000` ou `10000`, si nécessaire.

- Lorsque vous activez KPSN dans les propriétés du Serveur d'administration et utilisez le port HTTPS 17111, la connexion avec ds.kaspersky.com n'est pas interrompue.

- Kaspersky Endpoint Security for Windows ne prend pas en charge le service KSN Proxy si l'option **Utiliser HTTPS** est activée dans les paramètres du proxy KSN des propriétés du Serveur d'administration et si l'adresse du Serveur d'administration contient des caractères non latins.

- Lorsque vous passez au Serveur secondaire à partir de l'interface du Serveur d'administration primaire de Kaspersky Security Center Linux, la section **Mises à jour transparentes** du menu principal ne peut pas être ouverte.

- Quand vous créez la tâche *Ajout d'une clé* pour Kaspersky Endpoint Security 11.3 for Mac, l'Assistant affiche un tableau des clés de licence qui peut contenir des lignes vides.

- Le niveau de protection affiché dans la stratégie Kaspersky Endpoint Security for Windows ne correspond pas au niveau de protection affiché dans l'interface de Kaspersky Endpoint Security for Windows.

- Lorsque vous exécutez la tâche *Désinstallation à distance d'une application* pour supprimer une application Kaspersky d'un appareil administré, la tâche se termine avec succès, mais l'application n'est pas supprimée. Ce problème concerne Kaspersky Endpoint Security for Linux, Kaspersky Embedded Systems Security for Linux et Kaspersky Industrial CyberSecurity for Linux Nodes.

- La fenêtre des propriétés du Serveur d'administration contient les paramètres pour les appareils mobiles, mais Kaspersky Security Center Linux ne prend pas en charge l'administration des appareils mobiles.

- 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.

- Si vous installez l'Agent d'administration sur un appareil fonctionnant sous le système d'exploitation ALT Linux via une tâche d'installation à distance et que vous exécutez cette tâche sous un compte avec des privilèges non racine, la tâche échoue. Exécutez la tâche d'installation à distance sous le compte utilisateur racine ou créez et utilisez un paquet d'installation autonome de l'Agent d'administration pour installer l'application localement.

- Dans les rapports au format lettre, un saut de page peut couper une ligne de texte horizontalement.

- Dans l'Assistant **Ajouter un 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.

- 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.

- 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.

- Dans l'édition 64 bits d'Astra Linux, le paquet klnagent-astra ne peut pas être mis à jour avec le paquet klnagent64_14 : l'ancien paquet klnagent64-astra sera supprimé et le nouveau paquet klnagent64 sera installé à la place de la mise à jour, donc la nouvelle icône pour l'appareil avec le paquet klnagent64_14 sera ajouté. Vous pouvez supprimer l'ancienne icône de cet appareil.

Glossaire

Administrateur de Kaspersky Security Center Linux

Personne qui gère les opérations de l'application via le système d'administration centralisé à distance Kaspersky Security Center Linux.

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 Linux 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.

Appareils administrés

Les appareils du réseau inclus dans un groupe d'administration.

Application incompatible

Une application antivirus d'un développeur tiers ou une application Kaspersky qui ne prend pas en charge l'administration via Kaspersky Security Center Linux.

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 Linux. 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 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 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.

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. La Console d'administration est un analogue de Kaspersky Security Center Web 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 programmes de protection 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 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 de rôle

Groupe d'utilisateurs d'appareils mobiles Exchange ActiveSync qui possèdent des autorisations d'administration identiques.

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.

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 d'importance, 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 Linux.

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.

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 Linux conçu pour vérifier la puissance du système d'exploitation lors de l'utilisation simultanée de l'application Kaspersky Security Center Linux avec Microsoft NAP.

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.

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.

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 à partir duquel vous ouvrez Kaspersky Security Center Web Console. Ce composant offre une interface d'administration Kaspersky Security Center Linux.

Le poste de travail de l'administrateur sert à configurer et à administrer la partie serveur de Kaspersky Security Center Linux. 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

L'ensemble des paramètres de comportement des appareils mobiles Exchange lors de la connexion au serveur Microsoft Exchange.

Profil de configuration

La stratégie qui contient l'ensemble de paramètres et de restrictions pour l'appareil mobile MDM iOS.

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.

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.

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

Sans utiliser la reconnaissance de l'emplacement réseau (NLA).

Service Windows qui aide le système d'exploitation à identifier le réseau actuel. NLA effectue la détection des modifications apportées au réseau et ajuste la configuration de sécurité de l'appareil.

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 Linux 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 Linux 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 Web de Kaspersky Security Center Linux

Un module de Kaspersky Security Center Linux 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.

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 Linux.

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.

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 Linux, 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 Linux. Les informations sur les utilisateurs internes ne sont pas transmises au système d'exploitation. Kaspersky Security Center Linux effectue l'authentification des utilisateurs internes.

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 répertoire 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, Cisco Jabber, Cisco Systems 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, Google Public DNS, Hangouts, 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, PowerShell, PowerPoint, SharePoint, SQL Server, Office 365, OneNote, Outlook, Skype, Tahoma, Visio, Win32, Windows, Windows PowerShell, Windows Media, Windows Server, Windows Phone, Windows Vista et Windows Azure sont des marques déposées du groupe de sociétés Microsoft.

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.

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.

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.