kaspersky

Kaspersky Security Center 16.2 Linux

© 2026 AO Kaspersky Lab

Contenu

Aide de Kaspersky Security Center Linux

Nouveautés

Bogues corrigés

À propos de Kaspersky Security Center Linux

- Kit de distribution
- Configurations logicielle et matérielle
  - Configuration requise pour le Serveur d'administration
  - Configuration requise pour Web Console
  - Configuration requise pour l'Agent d'administration
- Compatible avec les applications et les solutions de Kaspersky
- À propos de la compatibilité des modules de Kaspersky Security Center Linux
- Comparaison de Kaspersky Security Center : basé sur Windows et basé sur Linux
- À propos de Kaspersky Next Expert View

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
  - Serveur Web de Kaspersky Security Center Linux
  - 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
  - Serveurs d'administration virtuels

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

- Serveur d'administration et appareils administrés sur un réseau local (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
Guide de renforcement
Liste de contrôle de renforcement
Déploiement du Serveur d'administration
Sécurité des connexions
Comptes et authentification
Gestion de la protection du Serveur d'administration
Gestion de la protection des appareils clients
Configuration de la protection des applications administrées
Maintenance du Serveur d'administration
Transfert d'événements vers des systèmes tiers
Recommandations de sécurité pour les systèmes d'information des tiers
Recommandations relatives à l'utilisation des applications de sécurité de Kaspersky
Scénario : Authentification du serveur MySQL
Scénario : Authentification du serveur PostgreSQL
Préparatifs du déploiement
Sélection de la configuration 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
Sélection de la structure de protection de la société
Schémas typiques de déploiement du système de protection
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
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
Configuration du serveur MySQL x64 pour fonctionner avec Kaspersky Security Center Linux
Préparation du cluster de SGBD haute disponibilité pour le fonctionnement de 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
Déploiement du cluster de basculement Kaspersky Security Center Linux
Cluster de basculement Kaspersky Security Center Linux. Schémas de déploiement
Cluster de basculement Kaspersky Security Center Linux
Scénario : Déploiement du cluster de basculement Kaspersky Security Center Linux
Cluster de basculement Kaspersky Security Center Linux. Configurations logicielle et matérielle
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
Réinstallation d'un nœud de cluster de basculement
Installation de Kaspersky Security Center Web Console connecté au Serveur d'administration installé sur les nœuds du cluster de basculement Kaspersky Security Center Linux
Cluster de basculement Kaspersky Security Center Linux géo-distribué
Cluster géo-distribué fonctionnant sous Ubuntu avec le SGBD PostgreSQL
Préparation d'un système de fichiers pour les nœuds d'un cluster
Configuration d'un système de fichiers en cluster répliqué
Installation et configuration de Corosync et Pacemaker sur les nœuds du cluster
Installation et configuration du SGBD PostgreSQL
Installation de Kaspersky Security Center Linux sur les nœuds d'un cluster de basculement géo-distribué
Cluster géo-distribué fonctionnant sous SberLinux avec le SGBD Platform V Pangolin
Préparation d'un système de fichiers pour les nœuds d'un cluster
Configuration d'un système de fichiers en cluster répliqué
Installation et configuration de Corosync et Pacemaker sur les nœuds du cluster
Installation et configuration du SGBD Platform V Pangolin
Installation de Kaspersky Security Center Linux sur les nœuds d'un cluster de basculement géo-distribué
Installation de Kaspersky Security Center Web Console sur des nœuds de cluster de basculement géo-distribués
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
Déplacement de données d'un tablespace partagé vers un tablespace fichier par table dans les SGBD MySQL ou MariaDB
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 d'administration au Serveur d'administration à l'aide de l'utilitaire klmover
Réémettre le certificat du Serveur Web
Remplacer le certificat IAM par défaut par un certificat personnalisé
Ajout de l'adresse du Serveur d'administration à la configuration du serveur IAM

Désignation du dossier partagé
Connexion et déconnexion de Kaspersky Security Center Web Console
Interface de Kaspersky Security Center Web Console
Modification de la langue de l'interface de Kaspersky Security Center Web Console
Modification de la page d'accueil de Kaspersky Security Center Web Console
Ajout et suppression de signets
Suppression de Kaspersky Security Center Web Console
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. Spécification des paramètres de gestion des mises à jour tierces
Étape 10. Création de la configuration de base de la protection d'un réseau
Étape 11. Configuration des notifications par email
Étape 12. Fin de l'assistant de démarrage rapide 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. Administration du redémarrage
Étape 8. Suppression des applications incompatibles avant l'installation
Étape 9. Déplacement des appareils vers Appareils administrés
Étape 10. Sélection des comptes pour accéder aux appareils
Étape 11. Démarrage de l'installation
Mise à jour de Kaspersky Security Center Linux
Mise à niveau de Kaspersky Security Center Linux à partir de la version 16 ou d'une version ultérieure
Mise à niveau de Kaspersky Security Center Linux à partir de la version 16 ou ultérieure à l'aide du fichier d'installation
Mise à niveau de Kaspersky Security Center Linux à partir de la version 16 ou d'une version ultérieure par le biais d'une sauvegarde
Mise à jour de Kaspersky Security Center à partir de la version 16 ou d'une version ultérieure sur les nœuds du cluster de basculement Kaspersky Security Center Linux
Mise à niveau de Kaspersky Security Center Linux à partir de la version 15.4 ou d'une version antérieure
Mise à niveau de Kaspersky Security Center Linux à partir de la version 15.4 ou toute version antérieure à l'aide du fichier d'installation
Mise à niveau de Kaspersky Security Center Linux à partir de la version 15.4 ou d'une version antérieure par le biais d'une sauvegarde
Mise à jour de Kaspersky Security Center à partir de la version 15.4 ou d'une version antérieure 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
Migration vers Kaspersky Security Center Linux à l'aide de la sauvegarde des données du Serveur d'administration
Tutoriel vidéo : Migration vers Kaspersky Security Center Linux à l'aide de la sauvegarde des données du Serveur d'administration
Migration vers Kaspersky Security Center Linux à l'aide de l'Assistant de migration
Exportation des objets du groupe depuis Kaspersky Security Center Windows
Importation du fichier d'exportation Kaspersky Security Center Cloud Linux
Basculer les appareils administrés vers l'administration de Kaspersky Security Center Linux
Configuration du Serveur d'administration
Configuration de l'adresse de connexion au 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 du nom du Serveur d'administration
Préservation des connexions par l'ajout d'un nouvel enregistrement DNS
Préservation des connexions par le passage à une connectivité basée sur les adresses IP
Restauration des connexions interrompues après la modification du nom du serveur
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
Utilisation de l'utilitaire klbackup pour basculer des appareils gérés sous l'administration d'un autre Serveur d'administration
Sauvegarde et restauration des données du Serveur d'administration avec MySQL ou MariaDB
Maintenance du Serveur d'administration
Suppression d'une hiérarchie des Serveurs d'administration
Accéder aux serveurs DNS publics
Configuration de l'interface
Connexion sécurisée au Serveur d'administration
Chiffrer la communication selon TLS
Paramètres réseau pour l'interaction avec des services externes
Liste globale des sous-réseaux
Vérification de l'intégrité des modules à l'aide des utilitaires klscmodchk et integrity_checker
Recherche d'appareils en réseau
Scénario de recherche d'appareils en réseau
Sondage du réseau Windows

Sondage des plages IP
Ajout et modification d'une plage IP
Sondage Zeroconf
Sondage du contrôleur de domaine
Authentification et connexion au contrôleur de domaine
Configuration d'un contrôleur de domaine Samba
Inventaire du matériel
Ajout d'informations sur les nouveaux appareils
Configuration des critères de définition des appareils d'entreprise
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
Administration des appareils clients
Paramètres de l'appareil administré
Vérification de la connexion de l'appareil client avec le Serveur d'administration. L'utilitaire klnagchk
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
À propos des points de distribution
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
Ajout d'une passerelle de connexion dans la DMZ en tant que point de distribution
Modifier la liste des points de distribution pour un groupe d'administration
Activation d'un serveur push
Augmentation du nombre de descripteurs de fichiers pour le service klnagent
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
Transmission des clés de chiffrement entre les Serveurs d'administration
Modification du Serveur d'administration pour les appareils clients
Évitement des conflits entre plusieurs Serveurs d'administration
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
Accès à distance aux appareils administrés
Accès à distance depuis un appareil Linux avec Kaspersky Security Center Web Console vers un appareil administré basé sur Linux
Accès à distance depuis un appareil Linux avec Kaspersky Security Center Web Console vers un appareil administré basé sur Windows
Accès à distance depuis un appareil Windows avec Kaspersky Security Center Web Console vers un appareil administré basé sur Linux
Accès à distance depuis un appareil Windows avec Kaspersky Security Center Web Console vers un appareil administré basé sur Windows
Administration des appareils mobiles
Utilisation de Firebase Cloud Messaging
Intégration avec l'infrastructure à clé publique
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
Paquets
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
Paramètres du paquet d'installation de l'Agent d'administration
Lancement de paquets autonomes créés par Kaspersky Security Center Linux

Installation de l'application à l'aide des paquets autonomes
Utilité de la mise à jour des bases de données dans le paquet d'installation de l'application de sécurité
Modification de la limite de la taille des données du paquet d'installation personnalisé
Propagation des paquets d'installation sur les Serveurs d'administration secondaires
Affichage de la liste des paquets d'installation autonomes
Installation de l'Agent d'administration pour Linux
Préparation de l'appareil fonctionnant sous le système d'exploitation Linux à l'installation de l'Agent d'administration
Préparation d'un appareil exécutant SUSE Linux Enterprise Server 15 pour l'installation de l'Agent d'administration
Préparation d'un appareil exécutant Astra Linux dans l'environnement logiciel fermé mode pour l'installation de l'Agent d'administration
Préparation de l'installation de l'Agent d'administration sur un système d'exploitation Linux équipé de glibc 2.5 (ancien système d'exploitation)
Préparation de l'installation de l'Agent d'administration sur un système d'exploitation Linux équipé d'OpenSSH version 6.4 (ancien système d'exploitation)
Installation à distance de l'Agent d'administration sur un appareil Linux
Installation de l'Agent d'administration pour Linux en mode silencieux (avec un fichier de réponse)
Installation de l'Agent d'administration pour Linux en mode interactif
Prise en charge de la restauration du système de fichiers pour les appareils dotés de l'Agent d'administration
Installation de l'Agent d'administration pour Windows
Installation de l'Agent d'administration pour Windows en mode interactif
Installation de l'Agent d'administration pour Windows en mode silencieux
Déploiement par prise d'image et copie d'image d'un appareil
Mode de clonage du disque de l'Agent d'administration
Paramètres d'installation de l'Agent d'administration
Installation des applications à l'aide de la tâche d'installation à distance
À propos des tâches d'installation à distance des applications de Kaspersky Security Center Linux
Installation d'une application à distance
Installation à distance des applications sur les appareils macOS
Installation des applications sur les Serveurs d'administration secondaires
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
Déploiement forcé à l'aide d'une tâche d'installation à distance des applications de Kaspersky Security Center Linux
Installation des applications en mode silencieux
Préparation de l'appareil fonctionnant sous le système d'exploitation macOS à l'installation à distance 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
Spécification des paramètres pour l'installation à distance sur les appareils Unix
Surveillance du déploiement
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 de l'appareil Windows pour l'installation à distance
Création de la tâche Exécuter des scripts à distance
Création d'un paquet d'installation sur la base d'un fichier manifeste
Préparation d'une archive pour la tâche Exécuter des scripts à distance

Installation à distance d'applications sur les appareils à l'aide de la tâche Exécuter des scripts à distance
Configuration des notifications et de la surveillance de la tâche Exécuter des scripts à distance
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
Activation automatique d'une stratégie lors d'un événement " Propagation de virus "
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
Exportation et importation 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
Activation et désactivation du mode de faible consommation de ressources pour l'Agent d'administration
Configuration des paramètres de protection des applications administrées
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
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
Consultation des statistiques du 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
Lancement d'une tâche pour les appareils sélectionnés
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
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
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 de sécurité
Ajout d'un compte d'un utilisateur interne
Création d'un groupe de sécurité
Modification d'un compte d'un utilisateur interne
Modification d'un groupe de sécurité
Attribution d'un rôle à un utilisateur ou à un groupe de sécurité
Ajout de comptes utilisateurs à un groupe de sécurité interne
Désignation d'un utilisateur en tant que propriétaire de l'appareil
Désignation d'un utilisateur en tant que propriétaire de l'appareil pendant l'installation de l'Agent d'administration
Désignation d'un utilisateur en tant que propriétaire de l'appareil Linux après l'installation de l'Agent d'administration
Suppression d'un utilisateur en tant que propriétaire de l'appareil
Activation de la protection du compte contre les modifications non autorisées
Configuration de l'authentification à deux facteurs
À propos de l'authentification à deux facteurs pour un compte
Configuration d'une clé secrète d'authentification à deux facteurs pour Kaspersky Security Center Web Console
Autorisation des utilisateurs à configurer l'authentification à deux facteurs
Réinitialisation et suppression d'une clé secrète d'authentification à deux facteurs
Exclusion de comptes de l'authentification à deux facteurs
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
Modification du mot de passe d'un compte utilisateur
Création d'un rôle d'utilisateur
Modification d'un rôle d'utilisateur
Modification de la zone d'action d'un rôle d'utilisateur
Suppression d'un rôle d'utilisateur
Association des profils des stratégies aux rôles
Propagation des rôles d'utilisateurs sur les Serveurs d'administration secondaires
Modification du mot de passe d'un compte
Révocation des droits d'administrateur local
Configuration de l'authentification de domaine Kerberos
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
Approbation et refus des mises à jour du logiciel
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
Déclenchement des règles en mode Apprentissage intelligent
Consultation et confirmation des détections réalisées à l'aide des règles du Contrôle évolutif des anomalies
Ajout d'exclusions au départ des règles du contrôle évolutif des anomalies
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 d'administration et de protection
Utilisation des rapports
Création d'un modèle de 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 liés aux erreurs de fonctionnement de l'Agent d'administration
Événements d'avertissement de l'Agent d'administration
Événements informatifs de l'Agent d'administration
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 zones de détails des événements
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 de la permutation des états des appareils
Configuration des paramètres d'envoi des notifications
Vérification de déploiement des notifications
Paramètres et variables d'environnement pour décrire un événement
Annonces de Kaspersky
À propos des annonces de Kaspersky
Désactivation des annonces de Kaspersky
Affichage d'informations sur les détections de menaces
Intégrations pour la réponse aux alertes
Configuration de l'intégration à Active Directory pour l'exécution des actions de réponse
Configuration de l'intégration à Kaspersky Automated Security Awareness Platform
Configuration de l'intégration à Kaspersky Threat Intelligence Portal Sandbox
Regroupement des alertes par attributs
Cloud Discovery
Activation de Cloud Discovery à l'aide du widget
Ajout du widget Cloud Discovery au tableau de bord
Affichage des informations sur l'utilisation des services cloud
Niveau de risque d'un service cloud
Blocage de l'accès aux services cloud indésirables
Exportation des événements dans les systèmes SIEM
Configuration de l'export d'événements vers des systèmes SIEM
Prérequis
À propos de l'exportation des événements
À propos de la configuration de l'exportation d'événements dans le système SIEM
À propos de l'exportation des événements via les formats CEF et LEEF
Conversion d'événements au format CEF ou LEEF

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
Affichage et enregistrement d'une révision de la stratégie
Comparaison des révisions de stratégies
Restauration d'un objet à une révision précédente
Menaces actives
Désinfection d'un fichier non traité
Téléchargement d'un fichier non traité
Suppression des fichiers de la section Menaces actives
Suppression d'objets
Téléchargement et suppression de fichiers à partir de la Quarantaine et de la Sauvegardes de fichiers
Téléchargement de fichiers à partir de la Quarantaine et des Sauvegardes de fichiers
À propos de la suppression d'objets des stockages Quarantaine, Sauvegardes de fichiers ou Menaces actives
Gestion des applications via le protocole SNMP
Configuration du service snmpd dans le système d'exploitation
Activation et désactivation des notifications via le protocole SNMP
Activation et désactivation du protocole SNMP dans Kaspersky Security Center Linux
Valeurs des identificateurs d'objet pour SNMP
Utilisation de Kaspersky Security Center Linux sous licence pour Kaspersky Next XDR Optimum
Intégrations pour la réponse aux alertes
Configuration de l'intégration à Active Directory pour l'exécution des actions de réponse
Configuration de l'intégration à Kaspersky Automated Security Awareness Platform
Configuration de l'intégration à Kaspersky Threat Intelligence Portal Sandbox
Regroupement des alertes par attributs
Intégration entre Kaspersky Security Center Web Console et d'autres solutions Kaspersky
Établissement d'une connexion en arrière-plan
Configuration de la connexion au serveur proxy
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
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
Obtention et consultation d'une liste des fichiers exécutables stockés sur les appareils client
Création d'une catégorie d'applications enrichie manuellement
Création d'une catégorie d'applications incluant des fichiers exécutables provenant des appareils sélectionnés
Création d'une catégorie d'applications incluant des fichiers exécutables provenant du dossier sélectionné
Affichage de la liste des catégories d'applications
Ajout de fichiers exécutables liés par un événement à la catégorie d'applications
Configuration du Contrôle des applications dans la stratégie Kaspersky Endpoint Security for Windows
Obtention et consultation d'une liste des applications installées sur les appareils client
À propos des applications tierces
Installation des mises à jour du logiciel tiers
Scénario : mise à jour des logiciels tiers
Options d'installation des mises à jour logicielles tierces
La tâche Recherche de vulnérabilités et de mises à jour requises est créée
Création de la tâche Recherche de vulnérabilités et des mises à jour requises
Consultation des informations sur les mises à jour du logiciel tiers disponibles
Exportation de la liste des mises à jour du logiciel disponibles vers un fichier
Approuver et refuser les mises à jour du logiciel tiers
Création de la tâche Installer les mises à jour requises et corriger les vulnérabilités
Ajout de règles pour l'installation de la mise à jour
Paramètres de la tâche Installation des mises à jour requises et correction des vulnérabilités spécifiés après la création de la tâche
Mise à jour automatique des applications tierces
Correction des vulnérabilités dans les applications tierces
À propos de la recherche et de la correction des vulnérabilités dans les applications
Scénario : Recherche et correction des vulnérabilités dans les logiciels tiers
Correction des vulnérabilités dans les applications tierces
Création de la tâche Correction des vulnérabilités
Sélection des correctifs utilisateur pour les vulnérabilités dans le logiciel tiers
Consultation des informations relatives aux vulnérabilités dans les applications sur tous les appareils administrés
Consultation des informations relatives aux vulnérabilités dans les applications sur l'appareil administré sélectionné
Consultation des statistiques relatives aux vulnérabilités sur les appareils administrés
Exportation de la liste des vulnérabilités dans les applications vers un fichier
Ignorer les vulnérabilités dans les applications
Création d'un paquet d'installation d'une application tierce à partir de la base de données Kaspersky
Affichage et modification des paramètres d'un paquet d'installation d'une application tierce à partir de la base de données de Kaspersky
Paramètres d'un paquet d'installation d'une application tierce à partir de la base de données de Kaspersky
Correction des vulnérabilités dans un réseau isolé
Scénario : Correction des vulnérabilités des logiciels tiers dans un réseau isolé
À propos de la correction des vulnérabilités des logiciels tiers dans un réseau isolé
Configuration du Serveur d'administration avec accès à Internet pour corriger les vulnérabilités dans un réseau isolé
Configuration des Serveurs d'administration isolés pour corriger les vulnérabilités d'un réseau isolé

Transmission des correctifs et installation des mises à jour dans un réseau isolé
Désactivation de la transmission des correctifs et de l'installation des mises à jour dans un réseau isolé
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
Maintien des connexions inactives
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
À propos du transfert de l'Agent d'administration à d'autres Serveurs d'administration
Création d'un profil 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
Restrictions de Kaspersky Security Center Linux
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
Enregistrement des événements sur 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 selon différents scénarios
Débit moyen du trafic par 24 heures
Problèmes connus et restrictions
Contacter le Support Technique
Façons de profiter du support technique
Support technique via le Kaspersky CompanyAccount
Obtention des fichiers de vidage du Serveur d'administration
Sources d'informations sur l'application
Glossaire
Administrateur de Kaspersky Security Center Linux
Administrateur du client
Administrateur du prestataire de services
Administration centralisée des applications
Agent d'administration
Agent d'authentification
Agent de mise à jour
Appareil MDM iOS
Appareils administrés
Application incompatible
Bases antivirus
Boutique des apps
Certificat du Serveur d'administration
Certificat général
Clé active
Clé de réserve

Client du Serveur d'administration (Appareil client)
Cloud Discovery
Console d'administration
Copie de sauvegarde des données du Serveur d'administration
Domaine multidiffusion
Dossier de sauvegarde
Durée de validité de la licence
État de la protection
État de la protection du réseau
Fichier clé
FileTransferBridge
Gestion directe des applications
Gestionnaire des identités et des accès (IAM)
Gravité de l'événement
Groupe d'administration
Groupe de rôle
HTTPS
Installation à distance
Installation locale
Installation manuelle
JavaScript
Kaspersky Security Center System Health Validator (SHV)
Mise à jour disponible
Mises à jour
Nagent léger (LWNGT)
Niveau d'importance du correctif
Paquet d'installation
Paramètres de l'application
Paramètres de la tâche
Passerelle des connexions
Poste de travail de l'administrateur
Prestataire de services de protection antivirus
Privilèges d'administrateur
Profil
Profil de configuration
Profil provisioning
Propagation de virus
Propriétaire de l'appareil
Protection antivirus du réseau
Reconnaissance de l'emplacement réseau (NLA)
Restauration
Restauration des données du Serveur d'administration
Serveur d'administration
Serveur d'administration domestique
Serveur d'administration virtuel
Serveur MDM iOS
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
Vulnérabilité
Zone démilitarisée (DMZ)
Informations sur le code tiers
Avis de marques déposées

Aide de Kaspersky Security Center Linux

Nouvelles fonctions

- 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
- Déploiement des applications Kaspersky Déploiement centralisé

- Configuration de la protection réseau
- Déploiement des applications Kaspersky Mise à jour des bases de données et des modules logiciels
- Configuration de l'adresse de connexion au Serveur d'administration
- Migration vers Kaspersky Security Center Linux
- À propos de la mise à niveau de Kaspersky Security Center Linux

Surveillance

- Suivi et rapports
- Cloud Discovery

Administration des appareils clients

- Accès à distance aux appareils administrés

Gestion des vulnérabilités et des correctifs

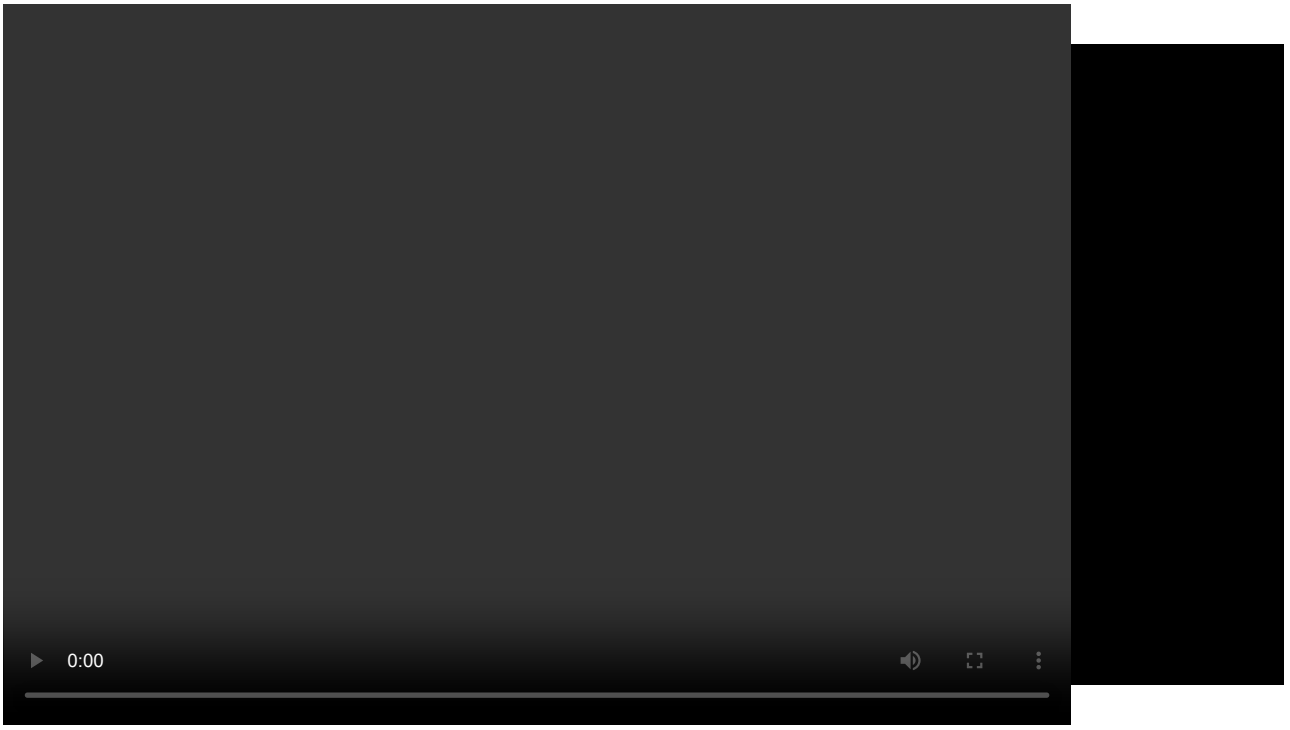
- Recherche et correction des vulnérabilités dans les logiciels tiers

Fonctionnalités supplémentaires

- Exportation des événements dans les systèmes SIEM
- Consultation des statistiques du serveur proxy KSN
- Guide de dimensionnement (Aide en ligne uniquement)

Nouveautés

Kaspersky Security Center 16.2 Linux



Présentation des nouveautés de la version 16.2. Enregistrements vidéo

Kaspersky Security Center 16.2 Linux comprend plusieurs nouvelles fonctionnalités et améliorations :

- Kaspersky Security Center Web Console permet désormais de configurer une passerelle de connexion dans la zone démilitarisée (DMZ).

  Utilisez l'option **Utiliser la passerelle de connexion DMZ par adresse** pour configurer une passerelle de connexion.

- Amélioration de l'algorithme de conservation de l'identifiant d'appareil de l'Agent d'administration (le paramètre `Device ID`) sur les appareils Linux. Si le numéro de série du BIOS, le numéro de série de la carte mère, les identifiants du disque de stockage ou l'adresse MAC d'un appareil correspondent à des valeurs déjà connues, le Serveur d'administration identifie correctement l'appareil comme ayant déjà été détecté après une mise à jour du système d'exploitation ou un changement d'adresse MAC.

- Ajout de la prise en charge des clusters de basculement Kaspersky Security Center Linux répartis géographiquement, dont les nœuds sont situés dans différents centres de données. Dans la configuration de cluster géo-distribué, tous les composants sont à basculement.

- Vous pouvez désormais exporter des événements vers un système SIEM aux formats CEF ou LEEF.

- Ajout de la prise en charge du cluster PostgreSQL à haute disponibilité avec Patroni pour le basculement automatique et HAProxy pour l'équilibrage de charge.

- Vous pouvez comparer les révisions des stratégies. Cette option est disponible pour les stratégies du Serveur d'administration, de l'Agent d'administration, de Kaspersky Endpoint Security for Windows (à partir de la version 14.0 du plug-in Internet) et de Kaspersky Endpoint Security for Mac (à partir de la version 12.2.1 Correctif A du plug-in Internet). La liste des applications Kaspersky prenant en charge cette fonctionnalité sera élargie dans les prochaines versions.

- Le protocole SNMP est désormais pris en charge. Vous pouvez transmettre les informations, les statistiques et les événements liés au Serveur d'administration à des applications clientes tierces à l'aide du protocole SNMP.

- Le sondage réseau Windows est désormais pris en charge pour les points de distribution Windows.

- Un seul paquet d'installation pour l'Agent d'administration sous Linux est désormais disponible. Ce paquet d'installation comprend des versions adaptées à différents gestionnaires de paquets et architectures de processeur. Lors de l'installation, l'environnement est automatiquement détecté, et le paquet de l'Agent d'administration approprié est installé.

- Les événements contiennent désormais des informations sur l'initiateur des commandes exécutées sur les appareils mobiles.

- Le module NSQ a été retiré du paquet de distribution de Kaspersky Security Center Web Console. Le service KSCWebConsoleMessageQueue.service n'est plus utilisé et sera supprimé après la mise à jour de Kaspersky Security Center Web Console.

- Si le Serveur d'administration n'a pas accès au référentiel des distributions d'applications pour l'installation à distance, vous devez, avant de créer des paquets d'installation à partir d'un fichier pour les applications sur les appareils Windows, télécharger des modules supplémentaires depuis le site Internet de Kaspersky : les fichiers pour l'installation à distance via Kaspersky Security Center (les archives ri_utils_win32.zip et ri_utils_arm64.zip).

- L'Agent d'administration prend désormais en charge l'architecture Windows ARM 64 bits. La compatibilité avec les applications administrées peut être vérifiée dans la documentation d'aide correspondante.

- Kaspersky Security Center Linux prend en charge l'utilisation de Kaspersky Sandbox.

- Améliorations de l'expérience utilisateur :

  - Vous pouvez désormais supprimer en une seule fois tous les événements d'une sélection d'événements et d'une liste d'événements d'un appareil.

    Les options **Tout sélectionner** et **Tout sélectionner sur la page actuelle** sont disponibles dans la sélection d'événements et dans la liste des événements de l'appareil.

  - Vous pouvez désormais définir manuellement la priorité d'une règle de déplacement.

    Le bouton **Modifier la priorité** devient disponible dès que vous sélectionnez une règle de déplacement et permet d'indiquer une nouvelle priorité.

- Kaspersky Security Center Linux est compatible avec Platform V SberLinux OS Server (SLO) 9.6.

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

  - MySQL Standard Edition 8.4

  - MySQL Enterprise Edition 8.4

  - PostgreSQL 18

- Postgres Pro 18 (toutes les éditions)
- Postgres Pro 18 Enterprise (haute disponibilité intégrée du cluster)

- L'Agent d'administration prend désormais en charge le travail avec les nouvelles versions de système d'exploitation suivantes :
  - Microsoft Windows 11 Famille/Pro/Pro pour Stations de travail/Entreprise/Éducation ARM
  - Platform V SberLinux OS Server (SLO) 9.6

Kaspersky Security Center 16.1 Linux

Kaspersky Security Center 16.1 Linux comprend plusieurs nouvelles fonctionnalités et améliorations :

- L'authentification à deux facteurs est désormais activée par défaut. L'option générale permettant de désactiver l'authentification à deux facteurs n'est plus disponible. Pour vous assurer que les utilisateurs peuvent se connecter à Kaspersky Security Center Web Console et continuer à utiliser les scripts d'automatisation OpenAPI, activez l'authentification à deux facteurs pour tous les utilisateurs avant la mise à niveau.
- Vous pouvez désormais enregistrer un profil de stratégie dans un fichier KLPROF sans exporter de stratégie, puis utiliser ce fichier KLPROF pour importer le profil enregistré dans la stratégie.
- L'Agent d'administration fonctionne désormais sur un appareil exécutant ALT OS en mode environnement logiciel fermé.
- Ajout de la prise en charge de l'authentification de domaine basée sur Kerberos pour les utilisateurs de domaine sans mot de passe à l'aide du protocole SCRIL, permettant l'authentification unique (SSO) basée sur des certificats.
- Améliorations de l'expérience utilisateur :
  - Le filtrage des appareils clients par version du système d'exploitation et gestionnaire des paquets inclut désormais les versions du système d'exploitation Linux.
  - Amélioration du mécanisme de pagination des tableaux dans Kaspersky Security Center Web Console : le nombre par défaut d'éléments affichés a été augmenté à 50, et le nombre personnalisé d'éléments affichés est désormais conservé d'une session à l'autre.
  - Commentaires pour les catégories d'applications qui vous permettent d'ajouter des descriptions des règles d'inclusion et d'exclusion des applications dans une catégorie.
  - Par défaut, la liste des paquets d'installation disponibles affiche désormais uniquement les paquets d'installation des applications Kaspersky dans la langue de l'interface de Kaspersky Security Center Web Console et en anglais.
- Kaspersky Security Center Linux prend en charge l'utilisation de Kaspersky Endpoint Security for Linux 12.4.

- Kaspersky Security Center Linux prend désormais en charge le travail avec les nouvelles versions de système d'exploitation suivantes :
  - Debian GNU/Linux 13 (Trixie)
  - CentOS Stream 10
  - Red Hat Enterprise Linux Server 10.x
- L'Agent d'administration prend désormais en charge le travail avec les nouvelles versions de système d'exploitation suivantes :
  - ALT Workstation 11
  - ALT Server 11
  - ALT Education 11
  - AlterOS 2025
  - SberOS 3.4.0
  - SberOS 3.5.0
  - OSnova 3.*

Kaspersky Security Center 16 Linux

Kaspersky Security Center 16 Linux comprend plusieurs nouvelles fonctionnalités et améliorations :

- Les contrôleurs de domaine FreeIPA et ALD Pro sont pris en charge.
- L'authentification de domaine (authentification unique) est mise en œuvre. La fonctionnalité d'authentification unique vous permet d'activer l'authentification sécurisée dans Kaspersky Security Center 16 Web Console sans avoir à saisir à nouveau le mot de passe sur le réseau de l'entreprise. Pour utiliser l'authentification de domaine, vous devez indiquer les paramètres complémentaires dans le fichier de réponses lors de l'installation de Kaspersky Security Center Web Console.
- Le Serveur d'administration de Kaspersky Security Center 16 Linux est compatible uniquement avec Kaspersky Security Center 16 Web Console. Les versions antérieures de Kaspersky Security Center Web Console ne peuvent pas être utilisées.
- Vous pouvez désormais utiliser les fonctionnalités de Kaspersky Next XDR Optimum avec une licence d'évaluation à condition d'avoir ajouté un Serveur d'administration secondaire, activé ce serveur avec la licence d'évaluation et déployé la clé de licence sur les appareils administrés par le Serveur d'administration secondaire.
- Améliorations de l'expérience utilisateur :
  - La navigation dans les groupes d'administration et les Serveurs d'administration est mise à jour : vous pouvez facilement basculer entre les groupes et les serveurs à partir d'un panneau de navigation unique.
  - Les paramètres de votre profil sont déplacés vers le volet supérieur.

- Les sections suivantes du menu principal sont renommées :
  - La section **Ressources (Appareils)** s'appelle désormais **Gestion des ressources**.
  - La section **Appareils administrés** s'appelle désormais **Ressources (Appareils)**.
  - La section **Liens rapides** s'appelle désormais **Navigation dans la console**.
- Vous pouvez réduire le menu principal à des icônes, si nécessaire.
- La section **Actualités de Kaspersky** est supprimée de **Surveillance** → **Notifications**.

- Les filtres que vous appliquez aux tableaux dans les sections **Opérations** → **Gestion des correctifs** → **Vulnérabilités dans les applications** et **Opérations** → **Gestion des correctifs** → **Mises à jour du logiciel** sont maintenant enregistrés et ne sont pas réinitialisés.
- Kaspersky Security Center Linux prend en charge :
  - Avec Kaspersky NGFW
  - les versions suivantes du système d'exploitation (pour les appareils administrés) :
    - MosOS 15.5 Arbat
    - Microsoft Windows 11 25H2
    - CentOS 6.4
    - CentOS 6.6

Kaspersky Security Center 15.4 Linux sous licence pour Kaspersky Next XDR Optimum

Si vous avez activé le Serveur d'administration sous licence pour Kaspersky Next XDR Optimum et déployé la clé de licence pour Kaspersky Next XDR Optimum dans vos applications administrées, vous pouvez effectuer les actions suivantes :

- Regrouper les alertes par attributs.
- Configurer les intégrations pour répondre aux menaces.

Kaspersky Security Center 15.4 Linux

Kaspersky Security Center 15.4 Linux comprend plusieurs nouvelles fonctionnalités et améliorations :

- Les profils de connexion pour les utilisateurs itinérants avec des appareils Linux sont maintenant disponibles. En utilisant des profils de connexion, vous pouvez configurer les règles pour que les Agents d'administration sur les appareils Linux se connectent au même Serveur d'administration ou à des Serveurs d'administration différents, selon l'emplacement de l'appareil.
- La transmission des clés de chiffrement entre les Serveurs d'administration est désormais disponible.
- Kaspersky Thin Client est désormais pris en charge.
- Le cluster à haute disponibilité intégré Platform V Pangolin est désormais pris en charge.
- Le cluster à haute disponibilité intégré Postgres Pro est désormais pris en charge. Les nœuds de ce cluster de SGBD sont indiqués dans la chaîne de connexion lors de l'installation de Kaspersky Security Center Linux.
- Kaspersky Security Center Linux prend désormais en charge les SGBD suivants :
  - Platform V Pangolin 6.5.1
  - Tantor SE 1C pour Astra Linux Special Edition RUSB.10015-01 (mise à jour opérationnelle 1.8)
  - Jatoba 5
- Prise en charge des versions 8.10.1, 9.0.1 et 9.5.1 de Platform V SberLinux OS Server (SLO).
- L'archive KlAkOAPI.tar.gz est supprimée de l'Aide. L'archive KlAkOAPI.tar.gz se trouve dans le dossier d'installation de Kaspersky Security Center Linux.
- Le bouton **Analyse** est supprimé de la section **Quarantaine**.
- Les informations relatives à la taille, au hachage du fichier et au chemin d'accès ne sont plus disponibles dans la liste des paquets d'installation pour le paquet autonome de l'Agent d'administration ou pour les paquets créés sur les Serveurs d'administration virtuels parce que ces paquets autonomes sont générés au moment du téléchargement.

Kaspersky Security Center 15.3 Linux

Kaspersky Security Center 15.3 Linux comprend plusieurs nouvelles fonctionnalités et améliorations :

- L'utilitaire klcsngtgui est supprimé du kit de distribution Kaspersky Security Center Linux. Nous vous recommandons d'utiliser l'utilitaire klnagchk au lieu de l'utilitaire klcsngtgui.
- L'Agent d'administration prend désormais en charge le travail avec les nouvelles versions de système d'exploitation suivantes :
  - Windows Server 2025
  - Fedora Linux Server 41
  - Fedora Linux Workstation 41
- Kaspersky Security Center Linux prend désormais en charge les SGBD suivants :
  - PostgreSQL 17
  - Postgres Pro 17
- Il est désormais possible de télécharger uniquement les mises à jour requises des bases et des modules logiciels pour les applications de sécurité de Kaspersky à l'aide de Kaspersky Update Utility. Dans la fenêtre des propriétés de la tâche **Téléchargement des mises à jour sur le stockage du Serveur d'administration**, activez l'option **Télécharger automatiquement le fichier de demande de mise à jour**, puis indiquez le chemin d'accès où Kaspersky Security Center Linux créera le fichier de demande de mise à jour contenant les informations sur les mises à jour à télécharger.
- La visualisation des statistiques d'utilisation du serveur proxy KSN est désormais disponible.
- La migration des données du Serveur d'administration de Kaspersky Security Center Windows vers Kaspersky Security Center Linux à l'aide de l'utilitaire klbackup a été mise à jour. Vous pouvez désormais migrer les données du Serveur d'administration stockées dans la base de données Microsoft SQL Server vers PostgreSQL ou Postgres Pro.
- La configuration de l'adresse de connexion au Serveur d'administration est désormais disponible. L'adresse de connexion au Serveur d'administration est utilisée comme adresse par défaut lors de la création des paquets d'installation de l'Agent d'administration et comme adresse du serveur proxy KSN lors de la connexion des appareils administrés à KSN.
- Vous pouvez désormais redémarrer de manière centralisée les appareils administrés.
- Les informations sur les utilisateurs actuellement connectés à l'appareil administré par Linux sont désormais affichées dans la section **Général** → **Sessions** de la fenêtre des propriétés de l'appareil.
- Vous pouvez désormais obtenir un accès à distance aux appareils administrés par Linux et Windows via l'Agent d'administration installé sur ces appareils. La connexion est établie à l'aide de RDP, VNC ou WDS. Après la connexion à l'appareil, l'administrateur obtient l'accès complet aux informations sur cet appareil et peut administrer les applications installées sur celui-ci.

- Téléchargez et exécutez une application (ou un script) pour les diagnostics sur un appareil administré. Vous pouvez maintenant télécharger soit le répertoire ou l'archive contenant le fichier exécutable, soit le fichier exécutable lui-même. Une fois l'application exécutée avec succès, vous pouvez télécharger les résultats de l'exécution.

- Améliorations de l'expérience utilisateur, notamment une nouvelle section **Liens rapides**. Cette section affiche la carte du menu principal et vous offre un accès rapide à toutes les sections de Kaspersky Security Center Web Console. Par défaut, les **Liens rapides** sont définis comme page d'accueil.

Kaspersky Security Center 15.2 Linux

Kaspersky Security Center 15.2 Linux comprend plusieurs nouvelles fonctionnalités et améliorations :

- Nouvelles fonctionnalités pour la gestion des mots de passe des comptes utilisateurs internes :

  - Vous pouvez désormais forcer un utilisateur interne à modifier un mot de passe lors de la première (ou prochaine) tentative de connexion à Kaspersky Security Center Web Console.

  - Nouvelle option pour configurer la période d'expiration du mot de passe pour les comptes des utilisateurs internes.

- Vous pouvez maintenant sauvegarder les données du Serveur d'administration de Kaspersky Security Center Windows et les restaurer dans Kaspersky Security Center Linux à l'aide de l'utilitaire klbackup. La migration peut être effectuée sans perte de données entre SGBD de même type ou de serveur SQL de Microsoft → MySQL ou MariaDB.

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

  - PostgreSQL 16.x

  - Postgres Pro 16.x

- Kaspersky Security Center Linux prend désormais en charge certains types de clusters PostgreSQL et Postgres Pro.

- Prise en charge des nouveaux systèmes d'exploitation et des nouvelles versions des systèmes d'exploitation, y compris les nouvelles versions de M OS (Moscow Electronic School), MosTech et MosTech Server.

- Améliorations de l'expérience utilisateur, y compris :

  - Nouveau bouton **Enregistrer** dans la fenêtre des paramètres de la stratégie. Utilisez ce bouton si vous souhaitez enregistrer les modifications sans fermer la fenêtre des paramètres de la stratégie.

- Vous pouvez désormais gérer l'envoi de fichiers vers des appareils Android, supprimer les fichiers précédemment envoyés et configurer leurs paramètres dans la nouvelle section " Applications et fichiers " du plug-in d'administration Kaspersky Mobile Devices Protection and Management.

- Vous pouvez désormais transférer des paquets d'installation d'applications et des profils de gestion des appareils vers des appareils mobiles sans les connecter directement au Serveur d'administration à l'aide d'un nouveau service de Serveur Web sur une passerelle de connexion.

Kaspersky Security Center 15.1 Linux

Kaspersky Security Center 15.1 Linux comprend plusieurs nouvelles fonctionnalités et améliorations :

- Kaspersky Security Center Web Console prend désormais en charge l'administration des appareils mobiles via le plug-in d'administration Kaspersky Mobile Devices Protection and Management.
- L'extension de configuration des serveurs MDM iOS vous permet d'installer et de configurer les serveurs MDM iOS pour gérer des appareils MDM iOS.
- Vous pouvez maintenant gérer les certificats des appareils mobiles.
- Kaspersky Endpoint Security for Android est désormais pris en charge.
- Kaspersky Security for iOS est désormais pris en charge.
- Kaspersky Endpoint Security for Aurora est désormais pris en charge.
- Gestion des vulnérabilités et des correctifs pour les appareils administrés basés sur Windows. Vous pouvez gérer les mises à jour des logiciels tiers installés sur les appareils administrés fonctionnant sous Windows et corriger les vulnérabilités dans ces logiciels en installant les mises à jour requises.
- Kaspersky Security Center Linux interroge désormais les contrôleurs du domaine page par page au lieu d'interroger l'ensemble du contrôleur du domaine à la fois. Cette mesure permet d'interroger les contrôleurs du domaine qui incluent un grand nombre d'entrées.
- Contrôle évolutif des anomalies. Il s'agit d'une fonctionnalité de Kaspersky Endpoint Security for Windows qui utilise un ensemble de règles pour suivre les comportements atypiques sur les appareils clients et qui vous permet d'interdire les actions anormales.
- Mises à jour transparentes pour les applications Kaspersky administrées installées sur des appareils Windows et sur l'Agent d'administration pour Linux. Vous pouvez gérer le processus d'installation des mises à jour en approuvant les mises à jour qui doivent être installées et en refusant les mises à jour qui ne doivent pas être installées.
- Audit de stratégie étendu. Vous pouvez désormais consulter le contenu d'une révision de la stratégie et enregistrer la révision de la stratégie dans un fichier. Actuellement, ces fonctionnalités ne sont disponibles que pour la stratégie du Serveur d'administration et la stratégie de l'Agent d'administration.
- Cloud Discovery. Cette nouvelle fonctionnalité vous permet de surveiller l'utilisation des services cloud sur les appareils administrés fonctionnant sous Windows et de bloquer l'accès aux services cloud que vous considérez comme indésirable.
- Nouvelle sous-section **Alerte** dans la section **Surveillance** du menu principal. Dans la sous-section **Alerte**, vous pouvez voir des informations sur les détections de menaces sur les appareils des points de terminaison. Les menaces sont détectées par les applications de sécurité de Kaspersky.
- Kaspersky Security Center Linux peut désormais fonctionner comme un module de la solution Kaspersky Managed Detection and Response.
- Prise en charge de Kaspersky Security for Virtualization Light Agent.
- Inventaire matériel étendu des appareils macOS. L'Agent d'administration sur l'appareil macOS envoie l'adresse MAC et le numéro de série de l'appareil au Serveur d'administration.

- Vous pouvez désormais recevoir un rapport sur l'installation à distance lorsque vous installez un logiciel sur les appareils administrés via des scripts personnalisés.

- Lorsque vous exécutez plusieurs scripts personnalisés sur un appareil administré, vous pouvez attribuer une priorité à chaque script pour définir l'ordre d'exécution. Les scripts seront exécutés du plus prioritaire vers le moins prioritaire.

- Pour réduire la quantité de mémoire vive consommée par Kaspersky Endpoint Security for Linux et l'Agent d'administration pour Linux, vous pouvez activer un mode de travail spécial pour l'Agent d'administration pour Linux. Dans ce mode, l'Agent d'administration pour Linux requiert moins de mémoire vive, mais ses fonctionnalités sont limitées.

- Vous pouvez désinstaller les logiciels incompatibles sur les appareils administrés via la tâche *Désinstallation à distance d'une application*.

- Le Rapport d'attaques réseau inclut désormais l'adresse MAC et le port de l'appareil attaquant.

- La longueur maximale du mot de passe pour un utilisateur interne a été portée à 256 caractères.

- Améliorations de l'expérience utilisateur, y compris :

  - Personnalisation du menu principal en ajoutant des sections de Kaspersky Security Center Web Console aux signets pour un accès rapide depuis la section **Signets**.

  - Utilisation des tableaux optimisée. La vue par défaut de chaque tableau contient désormais les colonnes les plus fréquemment utilisées. En outre, vous pouvez désormais sélectionner tous les éléments de la page en cours ou de l'ensemble du tableau, ainsi que trier les éléments de l'ensemble du tableau.

  - Amélioration de la configuration de la diffusion des rapports. Vous pouvez désormais définir jusqu'à 20 adresses email auxquelles envoyer le rapport, ainsi que la planification de la remise du rapport.

- Prise en charge d'une large gamme de systèmes d'exploitation et de nouvelles versions du système d'exploitation.

- Un nouveau guide des tailles a été élaboré et publié dans l'aide en ligne.

- Suite à la révision d'une interface utilisateur, le problème qui entraînait l'apparition de la section **Diagnostic à distance** dans la fenêtre des propriétés du Serveur d'administration a été corrigé.

- Vous pouvez créer une tâche *Exécuter des scripts à distance* pour exécuter un paquet d'installation sur un appareil client et pour installer une application à distance.

- Un utilisateur peut être désigné en tant que propriétaire de l'appareil pendant ou après l'installation de l'Agent d'administration sur un appareil client sous Linux.

- Vous pouvez configurer une sélection d'appareils ou créer une règle de déplacement des appareils en fonction du propriétaire de l'appareil, de l'appartenance du propriétaire de l'appareil à un groupe de sécurité et du rôle du propriétaire de l'appareil.

- Vous pouvez révoquer les droits d'administrateur local des comptes. Cela vous offre un niveau de contrôle supplémentaire sur les comptes utilisateurs. Par exemple, vous pouvez révoquer les droits d'administrateur local à l'issue d'une attribution à usage unique.

- Vous pouvez modifier le mot de passe du compte local, par exemple, si l'utilisateur oublie le mot de passe du compte local ou pour effectuer une modification planifiée du mot de passe.

- La sous-section **Gestion des certificats utilisateurs** permet d'indiquer les certificats racines à installer. Ces certificats peuvent servir, par exemple, à vérifier l'authenticité de sites Internet ou de serveurs Internet.

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 **Ressources (Appareils)** 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 des 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.

Bogues corrigés

Le tableau ci-dessous dresse la liste de tous les problèmes détectés dans les versions précédentes de Kaspersky Security Center Linux et corrigés dans la version actuelle.

Liste des problèmes résolus dans Kaspersky Security Center Linux 16.2

Version de Kaspersky Security Center Linux dans laquelle le problème est apparu pour la première fois	Identifiant du problème	Description du problème
15.1	10071566	Correction d'un problème à cause duquel les modifications apportées à la planification d'une tâche n'étaient pas propagées aux appareils administrés si la planification utilisait le paramètre « Par jours de la semaine ».
15.4	9067754	Correction d'un problème qui entraînait un affichage incorrect des nouveaux événements dans une stratégie créée précédemment après la mise à jour du plug-in Kaspersky Mobile Devices Protection and Management.
16.1	9256000	Correction d'un problème qui empêchait l'affichage des informations relatives aux modules d'application gérés lorsque l'Agent d'administration était installé sous Microsoft Windows XP.

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 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.

Kit de distribution

Sur le site Internet de Kaspersky, vous pouvez télécharger tous les paquets de distribution nécessaires à l'application.

Le kit de distribution de Kaspersky Security Center Linux comprend les fichiers suivants :

Serveur d'administration de Kaspersky Security Center Linux :

- Serveur d'administration à installer sur un appareil fonctionnant sous le système d'exploitation Debian :

  ksc64_16.2.0-<compilation>_amd64.deb

- Serveur d'administration à installer sur un appareil fonctionnant sous le système d'exploitation Red Hat Enterprise Linux :

  ksc64-16.2.0-<compilation>.x86_64.rpm

Kaspersky Security Center Web Console :

- Web Console à installer sur un appareil fonctionnant sous le système d'exploitation Debian :

  ksc-web-console-16.2.<compilation>.x86_64.deb

- Web Console à installer sur un appareil fonctionnant sous le système d'exploitation Red Hat Enterprise Linux :

  ksc-web-console-16.2.<compilation>.x86_64.rpm

Agent d'administration pour Windows :

- L'Agent d'administration doit être installé sur un appareil avec une architecture x86-32 ou x64 :

  ksc_16_16.2.0.<compilation>_NetAgent_<localisation>.zip

- L'Agent d'administration doit être installé sur un appareil avec une architecture ARM :

  klnagent_winarm64-16.2.0.<compilation>-win_<localisation>.zip

- Utilitaire permettant l'installation à distance de l'Agent d'administration sur un appareil équipé d'un système d'exploitation ARM 64 bits :

  ri_utils_arm64.zip

- Utilitaire permettant l'installation à distance de l'Agent d'administration sur un appareil équipé d'un système d'exploitation 32 bits ou 64 bits :

  ri_utils_win32.zip

Agent d'administration pour Linux :

- Agent d'administration à installer sur un appareil fonctionnant sous le système d'exploitation Debian :

  klnagent64_16.2.0-<compilation>_<architecture>.deb

- Agent d'administration à installer sur un appareil fonctionnant sous le système d'exploitation Red Hat Enterprise Linux :

  klnagent64-16.2.0-<compilation>_<architecture>.rpm

- Fichiers pour l'installation à distance de l'Agent d'administration sur un appareil fonctionnant sous le système d'exploitation Debian :

  klnagent-<architecture>-16.2.0.<compilation>-deb_<localisation>.tar.gz

- Fichiers pour l'installation à distance de l'Agent d'administration sur un appareil fonctionnant sous le système d'exploitation Red Hat Enterprise Linux :

  klnagent-<architecture>-16.2.0.<compilation>-rpm_<localisation>.tar.gz

- Paquet de distribution unique pour les Agents d'administration sous Linux :

  klnagent-ALL-16.2.0.<compilation>-ALL_<localisation>.tar.gz

  Ce paquet de distribution unique peut s'avérer utile si vous disposez de nombreux appareils clients dotés d'architectures de processeur différentes et fonctionnant sous divers systèmes d'exploitation Linux. Les versions requises des Agents d'administration seront automatiquement sélectionnées pour être installées sur les appareils.

Plug-in Internet de Kaspersky Endpoint Detection and Response Optimum :

- signed_irp.zip

> Vous ne pouvez télécharger le plug-in Internet qu'à partir du stockage des paquets de distribution des applications destinés à l'installation à distance.

Si vous avez des difficultés à choisir un paquet d'installation pour un Agent d'administration pour Linux, reportez-vous à l'article Comment choisir le paquet d'installation d'un Agent d'administration pour Linux.

Configurations logicielle et matérielle

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

Pour connaître les versions Android et iOS requises pour le déploiement de la protection et la gestion des appareils mobiles, consultez l'aide de Kaspersky Security for Mobile et celle de Kaspersky Secure Mobility Management.

Configuration requise pour le Serveur d'administration

Configuration matérielle minimale requise :

- Processeur cadencé à 2,5 GHz ou plus, 2 cœurs.
- Mémoire vive : 6 Go

  > Vous devez activer le fichier d'échange sur l'appareil sur lequel le Serveur d'administration est installé. La taille minimale du fichier d'échange doit être 1.5 fois supérieure au volume de la mémoire RAM.

- 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 :

> Pour permettre la communication entre les processus dans le système d'exploitation, l'interface de bouclage doit être disponible.

- Debian GNU/Linux 12 (Bookworm) 64 bits
- Debian GNU/Linux 13 (Trixie) 64 bits
- Ubuntu Server 22.04 LTS (Jammy Jellyfish) 64 bits
- Ubuntu Server 24.04 LTS (Noble Numbat) 64 bits
- CentOS Stream 9 64 bits
- CentOS Stream 10 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
- Red Hat Enterprise Linux Server 10.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 Special Edition RUSB.10015-16 (version 1) (mise à jour opérationnelle 1.6) 64 bits
- Astra Linux Special Edition RUSB.10015-17 (mise à jour opérationnelle 1.7.3) 64 bits
- Astra Linux Special Edition RUSB.10015-03 (mise à jour opérationnelle 7.6) 64 bits
- Astra Linux Special Edition RUSB.10015-37 (mise à jour opérationnelle 7.7) 64 bits
- Astra Linux Common Edition (mise à jour opérationnelle 2.12) 64 bits
- ALT SP Server 10 64 bits
- ALT SP Workstation 10 64 bits
- Oracle Linux 7 64 bits
- Oracle Linux 8 64 bits
- Oracle Linux 9 64 bits
- Platform V SberLinux OS Server (SLO) 8.10.1 64 bits
- Platform V SberLinux OS Server (SLO) 9.5.1 64 bits
- Platform V SberLinux OS Server (SLO) 9.6 64 bits
- RED OS 7.3 Server 64 bits
- RED OS 7.3 Édition certifiée 64 bits
- RED OS 8 64 bits
- ROSA COBALT 7.9 64 bits
- M OS (Moscow Electronic School) 12 Server 64 bits
- Mostech Server 64 bits
- MosOS 15.5 Arbat 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 6.7.0
- VMware vSphere 7.0.3
- Microsoft Hyper-V Server 2019 64 bits
- Microsoft Hyper-V Server 2022 64 bits
- Citrix XenServer 7.x

- Citrix XenServer 8.2
- Parallels Desktop 18
- Oracle VM VirtualBox 7.0.12
- KVM (machine virtuelle basée sur le noyau)

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 Standard Edition 8.0 (version 8.0.20 et supérieure) 32 bits / 64 bits
- MySQL Enterprise Edition 8.0 (version 8.0.20 et supérieures) 32 bits / 64 bits
- MySQL Standard Edition 8.4 32 bits / 64 bits
- MySQL Enterprise Edition 8.4 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
- PostgreSQL 15.x 64 bits (cluster Corosync/Pacemaker)
- PostgreSQL 16.x 64 bits
- PostgreSQL 17 64 bits
- PostgreSQL 18 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)
- Postgres Pro 15.x 64 bits (cluster Corosync/Pacemaker)

- Postgres Pro 16.x 64 bits (toutes les éditions)
- Postgres Pro 16.x Enterprise 64 bits (haute disponibilité intégrée du cluster)
- Postgres Pro 17 64 bits (toutes les éditions)
- Postgres Pro 17 Enterprise 64 bits (haute disponibilité intégrée du cluster)
- Postgres Pro 18 64 bits (toutes les éditions)
- Postgres Pro 18 Enterprise 64 bits (haute disponibilité intégrée du cluster)
- Platform V Pangolin 6.5.1 64 bits
- Platform V Pangolin 6.5.1 64 bits (haute disponibilité intégrée au cluster)
- Jatoba 4 64 bits
- Jatoba 5 64 bits
- Tantor SE 1C 64 bits

Les clusters PostgreSQL haute disponibilité sont pris en charge. Pour en savoir plus, consultez l'article suivant : Préparation du cluster de SGBD haute disponibilité pour le fonctionnement de Kaspersky Security Center Linux.

Configuration requise pour Web Console

Serveur de Kaspersky Security Center Web Console

Configuration matérielle minimale requise :

- Processeur : 2 cœurs, cadencé à 2,5 GHz.
- Mémoire vive : 4 Go
- Espace disponible sur le disque : 40 Go requis pour le dossier dans lequel les données de la Web Console sont stockées (/var/opt/kaspersky).

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

> Pour permettre la communication entre les processus dans le système d'exploitation, l'interface de bouclage doit être disponible.

- Debian GNU/Linux 12 (Bookworm)
- Debian GNU/Linux 13 (Trixie)
- Ubuntu Server 22.04 LTS (Jammy Jellyfish)

- Ubuntu Server 24.04 LTS (Noble Numbat)
- CentOS Stream 9
- CentOS Stream 10
- Red Hat Enterprise Linux Server 7.x
- Red Hat Enterprise Linux Server 8.x
- Red Hat Enterprise Linux Server 9.x
- Red Hat Enterprise Linux Server 10.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.10015-16 (version 1) (mise à jour opérationnelle 1.6)
- Astra Linux Special Edition RUSB.10015-01 (mise à jour opérationnelle 1.7)
- Astra Linux Special Edition RUSB.10015-17 (mise à jour opérationnelle 1.7.3)
- Astra Linux Special Edition RUSB.10015-01 (mise à jour opérationnelle 1.8)
- Astra Linux Special Edition RUSB.10015-03 (mise à jour opérationnelle 7.6)
- Astra Linux Special Edition RUSB.10015-37 (mise à jour opérationnelle 7.7)
- Astra Linux Common Edition (mise à jour opérationnelle 2.12)
- ALT SP Server 10
- ALT SP Workstation 10
- Oracle Linux 7
- Oracle Linux 8
- Oracle Linux 9
- Platform V SberLinux OS Server (SLO) 8.10.1
- Platform V SberLinux OS Server (SLO) 9.5.1
- Platform V SberLinux OS Server (SLO) 9.6 64 bits
- RED OS 7.3 Server
- RED OS 7.3 Certified Edition
- RED OS 8

- ROSA COBALT 7.9
- M OS (Moscow Electronic School) 12 Server
- Mostech Server
- MosOS 15.5 Arbat

Plateformes de virtualisation prises en charge :

- VMware vSphere 6.7.0
- VMware vSphere 7.0.3
- Citrix XenServer 7.x
- Citrix XenServer 8.2
- Parallels Desktop 18
- Oracle VM VirtualBox 7.0.12
- Microsoft Hyper-V Server 2019
- Microsoft Hyper-V Server 2022
- KVM (machine virtuelle basée sur le noyau)

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 145.0.7632.26 ou version ultérieure
- Microsoft Edge 145.0.3800.65 ou version ultérieure
- Safari 18.3 (20620.2.4.11.5) sur macOS
- Yandex Browser 25.12.4.1216 ou version ultérieure
- Mozilla Firefox Extended Support Release 140.7.1.2 ou version 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.

Agent d'administration. Plateformes prises en charge

Systèmes d'exploitation. Postes de travail Microsoft Windows	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 Entreprise version 1703, 1709, 1803, 1809 32 bits / 64 bits Microsoft Windows 10 20H2, 21H2 IoT Entreprise 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 TH1 (juillet 2015) Famille/Pro/Pro pour Stations de travail/Entreprise/Éducation 32 bits/64 bits Microsoft Windows 10 TH2 (novembre 2015) Famille/Pro/Pro pour Stations de travail/Entreprise/Éducation 32 bits/64 bits Microsoft Windows 10 RS1 (août 2016) Famille/Pro/Pro pour Stations de travail/Entreprise/Éducation 32 bits/64 bits Microsoft Windows 10 RS2 (avril 2017) Familiale/Pro/Pro pour Stations de travail/Entreprise/Éducation 32 bits/64 bits Microsoft Windows 10 RS3 (Fall Creators Update, v1709) Famille/Pro/Pro pour Stations de travail/Entreprise/Éducation 32 bits/64 bits Microsoft Windows 10 RS4 (mise à jour d'avril 2018, v17134) Famille/Pro/Pro pour Stations de travail/Entreprise/Éducation 32 bits/64 bits Microsoft Windows 10 RS5 (octobre 2018) Famille/Pro pour Stations de travail/Entreprise/Éducation 32 bits/64 bits Microsoft Windows 10 RS6 (mai 2019) Famille/Pro pour Stations de travail/Entreprise/Éducation 64 bits Microsoft Windows 10 19H1, 19H2 Famille/Pro pour les Stations de travail/Entreprise/Éducation 32 bits/64 bits Microsoft Windows 10 20H1 (mise à jour de mai 2020) Famille/Pro/Pro pour Stations de travail/Entreprise/Éducation 32 bits/64 bits Microsoft Windows 10 20H2 (mise à jour d'octobre 2020) Famille/Pro/Pro pour Stations de travail/Entreprise/Éducation 32 bits/64 bits Microsoft Windows 10 21H1 (mise à jour de mai 2021) Famille/Pro/Pro pour Stations de travail/Entreprise/Éducation 32 bits/64 bits Microsoft Windows 10 21H2 (mise à jour d'octobre 2021) Famille/Pro/Pro pour Stations de travail/Entreprise/Éducation 32 bits/64 bits Microsoft Windows 10 22H2 (mise à jour d'octobre 2023) Famille/Pro/Pro pour Stations de travail/Entreprise/Éducation 32 bits/64 bits Microsoft Windows 11 Famille/Pro/Pro pour Stations de travail/Entreprise/Éducation ARM 64 bits Microsoft Windows 11 Famille/Pro/Pro pour Stations de travail/Entreprise/Éducation 64 bits Microsoft Windows 11 22H2 Famille/Pro/Pro pour Stations de travail/Entreprise/Éducation 64 bits Microsoft Windows 11 23H2 Famille/Pro/Pro pour Stations de travail/Entreprise/Éducation 64 bits Microsoft Windows 11 24H2 Famille/Pro/Pro pour Stations de travail/Entreprise/Éducation 64 bits Microsoft Windows 11 25H2 Famille/Pro/Pro pour Stations de travail/Entreprise/Éducation 64 bits Microsoft Windows 8.1 Pro/Entreprise 32 bits / 64 bits Microsoft Windows 8 Pro/Entreprise 32 bits / 64 bits Microsoft Windows 7 Professionnel/Entreprise/Intégral/Édition Familiale basique/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, requiert la mise à jour de sécurité pour Windows XP KB2868626) 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)

Systèmes d'exploitation. Serveurs Microsoft Windows	Microsoft Windows MultiPoint Server 2011 Standard/Premium 64 bits Microsoft 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) Microsoft Windows Server 2003 SP2 Standard/Enterprise 32 bits/64 bits (uniquement pris en charge par l'Agent d'administration version 10.5.1781) Microsoft Windows Server 2003 R2 Standard/Enterprise avec SP2 32 bits/64 bits (uniquement pris en charge par l'Agent d'administration version 10.5.1781) Microsoft Windows Server 2008 Foundation avec Service Pack 2 32 bits / 64 bits Microsoft Windows Server 2008 Standard/Entreprise/Datacenter avec Service Pack 2 32 bits / 64 bits Microsoft Windows Server 2008 R2 Datacenter/Enterprise/Foundation/Standard avec Service Pack 1 et versions ultérieures 64 bits Microsoft Windows Server 2012 Server Core/Datacenter/Essentials/Foundation/Standard 64 bits Microsoft Windows Server 2012 R2 Server Core/Datacenter/Essentials/Foundation/Standard 64 bits Microsoft Windows Server 2016 Datacenter/Standard/Server Core (option d'installation) (LTSB) 64 bits Microsoft Windows Server 2019 Standard/Datacenter/Core 64 bits Microsoft Windows Server 2019 RS5 Essentials/Standard 64 bits Microsoft Windows Server 2022 Standard/Datacenter/Core 64 bits Microsoft Windows Server 2025 Standard/Datacenter/Core 64 bits Microsoft Windows Server 2022 21H2 Standard/Datacenter 64 bits Microsoft Windows Storage Server 2019 64 bits Microsoft Windows Small Business Server 2011 Standard 64 bits Microsoft Windows Small Business Server 2011 Essentials 64 bits Windows Small Business Server 2011 Premium Add-on 64 bits

Systèmes d'exploitation. Linux	Debian GNU/Linux 10.x (Buster) 32 bits / 64 bits Debian GNU/Linux 11.x (Bullseye) 32 bits / 64 bits Debian GNU/Linux 12 (Bookworm) 32 bits / 64 bits Debian GNU/Linux 13 (Trixie) 64 bits Ubuntu Server 10.04 LTS (Lucid Lynx) 32 bits/64 bits Ubuntu Server 16.04 LTS (Xenial Xerus) 32 bits / 64 bits Ubuntu Server 18.04 LTS (Bionic Beaver) 64 bits Ubuntu Server 20.04 LTS (Focal Fossa) 64 bits Ubuntu Server 22.04 LTS (Jammy Jellyfish) 64 bits Ubuntu Server 22.04 LTS ARM 64 bits Ubuntu Server 24.04 LTS (Noble Numbat) 64 bits Ubuntu Desktop 10.04 LTS (Lucid Lynx) 32 bits/64 bits Ubuntu Desktop 16.04 LTS (Xenial Xerus) 32 bits / 64 bits CentOS 5.2 32 bits / 64 bits CentOS 5.4 32 bits / 64 bits CentOS 6.4 32 bits/64 bits CentOS 6.6 32 bits/64 bits CentOS 7.2 et versions ultérieures 64 bits CentOS Stream 8 64 bits CentOS Stream 9 64 bits CentOS Stream 9 ARM 64 bits CentOS Stream 10 64 bits Red Hat Enterprise Linux Server 6.x 32 bits / 64 bits Red Hat Enterprise Linux Server 7.2 et versions ultérieures 64 bits Red Hat Enterprise Linux Server 8.x 64 bits Red Hat Enterprise Linux Server 9.x 64 bits Red Hat Enterprise Linux Server 10.x 64 bits SUSE Linux Enterprise Server 12.5 et versions ultérieures (Tous Service Packs) 64 bits SUSE Linux Enterprise Server 15 (Tous Service Packs) 64 bits SUSE Linux Enterprise Server 15 (Tous Service Packs) ARM 64 bits openSUSE Leap 15 64 bits EulerOS 2.0 SP10 64 bits EulerOS 2.0 SP10 ARM 64 bits Astra Linux Special Edition RUSB.10015-01 (mise à jour opérationnelle 1.4) 32 bits / 64 bits Astra Linux Special Edition RUSB.10015-01 (mise à jour opérationnelle 1.5) 64 bits Astra Linux Special Edition RUSB.10015-01 (mise à jour opérationnelle 1.6) 64 bits Astra Linux Special Edition RUSB.10015-16 (version 1) (mise à jour opérationnelle 1.6) 64 bits Astra Linux Special Edition RUSB.10015-17 (mise à jour opérationnelle 1.7.3) 64 bits Astra Linux Special Edition RUSB.10015-01 (mise à jour opérationnelle 1.7) 64 bits Astra Linux Special Edition RUSB.10015-01 (mise à jour opérationnelle 1.8) 64 bits Astra Linux Special Edition RUSB.10015-03 (mise à jour opérationnelle 7.6) 64 bits Astra Linux Special Edition RUSB.10015-37 (mise à jour opérationnelle 7.7) 64 bits Astra Linux Special Edition RUSB.10152-02 (mise à jour opérationnelle 4.7) ARM 64 bits Astra Linux Common Edition (mise à jour opérationnelle 2.12) 64 bits ALT Workstation 11 64 bits ALT Server 11 64 bits ALT Education 11 64 bits ALT Workstation 10.1 64 bits ALT Server 10.1 64 bits ALT Education 10.1 64 bits ALT SP Server 10 32 bits/64 bits ALT SP Server 10 ARM 64 bits ALT SP Workstation 10 32 bits/64 bits ALT SP Workstation 10 ARM 64 bits ALT 8 SP Server (LKNV.11100-01) 32 bits / 64 bits ALT 8 SP Server (LKNV.11100-02) 32 bits / 64 bits

	ALT 8 SP Server (LKNV.11100-03) 32 bits/64 bits ALT 8 SP Workstation (LKNV.11100-01) 32 bits / 64 bits ALT 8 SP Workstation (LKNV.11100-02) 32 bits / 64 bits ALT 8 SP Workstation (LKNV.11100-03) 32 bits / 64 bits Oracle Linux 7 64 bits Oracle Linux 8 64 bits Oracle Linux 9 64 bits Linux Mint 21.1 et versions ultérieures 64 bits Linux Mint 22.x 64 bits AlterOS 7.5 et suivant 64 bits AlterOS 2025 64 bits GosLinux IC6/7.17 64 bits GosLinux IC6/7.2 64 bits SberOS 3.4.0 64 bits SberOS 3.5.0 64 bits Platform V SberLinux OS Server (SLO) 8.10.1 64 bits Platform V SberLinux OS Server (SLO) 9.1 64 bits Platform V SberLinux OS Server (SLO) 9.5.1 64 bits Platform V SberLinux OS Server (SLO) 9.6 64 bits RED OS 7.3 Server 64 bits RED OS 7.3 Édition certifiée 64 bits RED OS 8 64 bits RED OS 8 ARM 64 bits ROSA Enterprise Linux Server 7.9 64 bits ROSA Enterprise Linux Desktop 7.9 64 bits ROSA COBALT 7.9 64 bits ROSA CHROME 12 64 bits AlmaLinux 8 et versions ultérieures 64 bits AlmaLinux 9 et versions ultérieures 64 bits Rocky Linux 8 et versions ultérieures 64 bits Rocky Linux 9 et versions ultérieures 64 bits Atlant, version Alcyone, version 2022.02 64 bits MSVSPHERE 9.2 SERVER 64 bits MSVSPHERE 9.2 ARM 64 bits MSVSPHERE 9.4 SERVER 64 bits MSVSPHERE 9.4 ARM 64 bits SynthesisM Server 8.6 64 bits SynthesisM Client 8.6 64 bits OSnova 2.* 64 bits OSnova 3.* 64 bits Kylin 10 64 bits EMIAS 1.0 64 bits Amazon Linux 2 64 bits MosOS 15.5 Arbat 64 bits OS MES (Moscow Electronic School) 12 (pour ordinateurs de bureau et ordinateurs portables) 64 bits OS MES (Moscow Electronic School) 12 (pour les panneaux interactifs) 64 bits M OS (Moscow Electronic School) 12 Server 64 bits Mostech 64 bits Mostech Server 64 bits Fedora Linux Server 41 64 bits Fedora Linux Workstation 41 64 bits
Systèmes d'exploitation. macOS	Pour obtenir la liste des systèmes d'exploitation pris en charge, consultez l'aide de Kaspersky Endpoint Security for Mac .

Plateformes de virtualisation	VMware vSphere 6.7.0 VMware vSphere 7.0.3 Citrix XenServer 7.x Citrix XenServer 8.2 Parallels Desktop 18 Oracle VM VirtualBox 7.0.12 Microsoft Hyper-V Server 2019 64 bits Microsoft Hyper-V Server 2022 64 bits KVM (machine virtuelle basée sur le noyau) Consultez la configuration requise pour les applications administrées pour les autres plateformes prises en charge.

Sur les versions de Windows antérieures à Microsoft Windows Server 2008 R2 (versions de serveur) et Microsoft Windows 7 (versions de bureau), l'Agent d'administration ne prend pas en charge les fonctionnalités suivantes :

- Retraduction des mises à jour (utilisée par les points de distribution)
- Proxy KSN (utilisé par les points de distribution)
- Tâche de recherche de vulnérabilités

Sur les appareils exécutant Microsoft 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.

Compatible avec les applications et les solutions de Kaspersky

Kaspersky Security Center Linux prend en charge le déploiement et l'administration centralisés de toutes les applications et solutions Kaspersky actuellement prises en charge. Pour connaître les versions des applications et des solutions, reportez-vous à la page Internet de Application Support Lifecycle.

Applications de Kaspersky prises en charge:

- Kaspersky Endpoint Security for Windows (prend en charge les serveurs de fichiers)
- Kaspersky Endpoint Security for Linux (prend en charge les serveurs de fichiers)
- Kaspersky Endpoint Security for Linux Elbrus Edition
- Kaspersky Endpoint Security for Mac
- Kaspersky Endpoint Security for Android
- Kaspersky Endpoint Security for Aurora
- Kaspersky Security for iOS
- Kaspersky Industrial CyberSecurity for Linux Nodes
- Kaspersky Industrial CyberSecurity for Nodes
- Kaspersky Industrial CyberSecurity for Networks
- Kaspersky Endpoint Agent
- Kaspersky Embedded Systems Security for Windows
- Kaspersky Embedded Systems Security for Linux
- Kaspersky Security for Virtualization Light Agent
- KATA Sandbox (l'un des composants de Kaspersky Anti Targeted Attack Platform)
- Kaspersky Thin Client
- Kaspersky NGFW
- Kaspersky Sandbox

Kaspersky Security Center Linux est inclus dans les solutions suivantes :

- Kaspersky Endpoint Detection and Response Optimum
- Kaspersky Managed Detection and Response
- Kaspersky Next XDR Optimum

Pour connaître les versions des applications et des solutions, reportez-vous à la page Internet de Application Support Lifecycle.

Problèmes connus et restrictions

L'authentification unique (SSO) n'est pas prise en charge pour Kaspersky Industrial CyberSecurity for Networks.

À propos de la compatibilité des modules de Kaspersky Security Center Linux

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

Compatibilité des modules de Kaspersky Security Center Linux

Module	Compatible avec
Serveur d'administration de Kaspersky Security Center 16.2 Linux	• Kaspersky Security Center Web Console des versions suivantes : 16.2, 16.1 • Versions suivantes de l'Agent d'administration de Kaspersky Security Center : 16.2, 16.1, 16, 15.4, 15.3, 15.2, 15.1 et 15
Kaspersky Security Center 16.2 Web Console	Versions suivantes du Serveur d'administration de Kaspersky Security Center Linux : 16.2, 16.1 et 16
Serveur d'administration principal de Kaspersky Security Center 16.2	Serveurs d'administration secondaires : • Versions suivantes de Kaspersky Security Center Linux : 16.2, 16.1, 16, 15.4, 15.3, 15.2, 15.1 et 15 • Versions suivantes de Kaspersky Security Center Windows : 15.1 et 14.2
Serveur d'administration secondaire de Kaspersky Security Center 16.2 Linux	Serveurs d'administration principaux : • Versions suivantes de Kaspersky Security Center Linux : 16.2, 16.1, 16, 15.4, 15.3, 15.2, 15.1 et 15 • Versions suivantes de Kaspersky Security Center Windows : 15.1 et 14.2

Module	Compatible avec
Agent d'administration de Kaspersky Security Center 16.2	Serveurs d'administration : • Versions suivantes de Kaspersky Security Center Linux : 16.2, 16.1, 16, 15.4, 15.3, 15.2, 15.1 et 15 • Versions suivantes de Kaspersky Security Center Windows : 15.1
Sauvegarde et restauration des données du Serveur d'administration de Kaspersky Security Center	La sauvegarde et la restauration des données sont prises en charge depuis les versions suivantes du Serveur d'administration de Kaspersky Security Center Linux : 16.1, 16, 15.4, 15.3, 15.2, 15.1 et 15

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

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

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

Kaspersky propose Kaspersky Security Center en tant que solution sur site pour deux plates-formes : Windows et Linux. Dans la solution pour Windows, vous installez le Serveur d'administration sur un appareil exécutant un système d'exploitation Windows. La solution pour Linux dispose d'une version du Serveur d'administration qui peut être installée sur un appareil Linux. Cette aide en ligne contient des informations sur Kaspersky Security Center. 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 15.1 Windows	Kaspersky Security Center 16.2 Linux
Serveur d'administration		
Emplacement du système de gestion de base de données (SGBD)	Sur site	Sur site (Microsoft SQL n'est pas pris en charge)
Système d'exploitation sur lequel installer le Serveur d'administration	Windows	Linux
Hiérarchie des Serveurs d'administration	✓	✓
Prise en charge des Serveurs d'administration virtuels	✓	✓
Déploiement du cluster de basculement Kaspersky Security Center	✓ Un cluster monosite uniquement	✓ À partir de Kaspersky Security Center 16.2 Linux, les clusters de basculement géo-distribués sont pris en charge

Fonctionnalité ou propriété	Kaspersky Security Center 15.1 Windows	Kaspersky Security Center 16.2 Linux
Utilisation de SNMP pour envoyer les statistiques du Serveur d'administration à des applications tierces	✓	✓
Serveur Web pour la publication des paquets d'installation et d'autres fichiers	✓	✓
Console d'administration		
Type de Console d'administration	Basé sur MMC et sur le Web	Basé sur le Web
Système d'exploitation sur lequel installer la Console d'administration Web	Windows ou Linux	Linux
Se connecter à la console à l'aide de l'authentification de domaine	✓	✓
Gestion des appareils clients et des groupes d'administration		
Nombre maximal d'appareils administrés (par Serveur d'administration)	100 000 (avec le serveur Microsoft SQL)	50 000 (avec PostgreSQL et Postgres Pro)
Sondage réseau	✓	✓
Protection des appareils administrés Windows, macOS et Linux	✓	✓
Protection des appareils mobiles	✓ Gestion de base des appareils mobiles	✓ MDM et utilisation de la fonctionnalité Kaspersky Secure Mobility Management (sous licence)
Gestion de la protection des machines virtuelles	✓	✓
Protection de l'infrastructure Cloud publique	✓	—
Connexion à distance au bureau de l'appareil client	✓	✓
Chiffrement et protection des données	✓ Sur les appareils administrés sous Windows équipés de Kaspersky Endpoint Security for Windows ou Kaspersky Endpoint Security for Mac	✓ Sur les appareils administrés sous Windows équipés de Kaspersky Endpoint Security for Windows ou Kaspersky Endpoint Security for Mac
Prise en charge des clusters et des matrices de serveurs dans les groupes d'administration	✓	✓
Hiérarchie du groupe d'administration	✓	✓
Ajout d'une passerelle de connexion dans la DMZ en tant que point de distribution	✓ (non pris en charge pour Web Console)	✓
Travail avec les utilisateurs		
Création et gestion des comptes utilisateurs	✓	✓
Gestion des applications Kaspersky		
Stratégies d'application	✓	✓
Tâches pour les applications Kaspersky	✓	✓
Kaspersky Security Network	✓	✓
Serveur proxy KSN	✓	✓
Kaspersky Private Security Network	✓	✓
Déploiement centralisé des clés de licence pour les applications Kaspersky	✓	✓
Diagnostic à distance des appareils clients	✓	✓

Fonctionnalité ou propriété	Kaspersky Security Center 15.1 Windows	Kaspersky Security Center 16.2 Linux
Mise à jour automatique des applications Kaspersky	✓	✓
Prise en charge du Contrôle évolutif des anomalies	✓	✓
Administration de la sécurité centrée sur l'appareil	✓	✓
Administration de la sécurité centrée sur l'utilisateur	✓	✓
Administration des systèmes		
Déploiement des systèmes d'exploitation sur les appareils clients	✓	—
Administration des licences tierces	✓	À mettre en œuvre en 2026
Utilisation du Serveur d'administration comme serveur WSUS	✓	✓ (mode de recherche passif de mises à jour Windows uniquement)
Gestion des applications tierces sur les appareils client		
Installation des mises à jour du logiciel tiers et correction des vulnérabilités dans les applications tierces	✓	✓
Importation et exportation de catégories d'applications	✓ (non pris en charge pour Web Console)	À mettre en œuvre en 2026
Surveillance, reporting et audit		
Utilisation des révisions des objets	✓	✓
Comparaison des révisions de stratégies	✓	✓
Consultation et utilisation des alertes détectées par Kaspersky Endpoint Detection and Response Optimum	✓	✓
Notifications sur les événements survenus sur les appareils administrés	✓	✓
Surveillance de l'état des stratégies et des tâches	✓	✓
Intégrations		
Intégration de Kaspersky Managed Detection and Response	✓	✓
Intégration avec les systèmes SIEM	✓	✓ L'intégration prête à l'emploi avec KUMA doit être mise en œuvre en 2026
Agrégation des alertes et exécution des actions de réponse à l'aide d'Active Directory, de KASAP et de Kaspersky TIP Sandbox	—	✓ Vous devez activer le Serveur d'administration sous une licence pour Kaspersky Next XDR Optimum, puis déployez la clé de licence pour Kaspersky Next XDR Optimum dans les applications que vous administrez

À propos de Kaspersky Next Expert View

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 Next Expert View. Cette console dispose d'une interface semblable à l'interface de Kaspersky Security Center Web Console.

L'interface et la documentation de Kaspersky Next Expert View sont disponibles dans les langues suivantes :

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

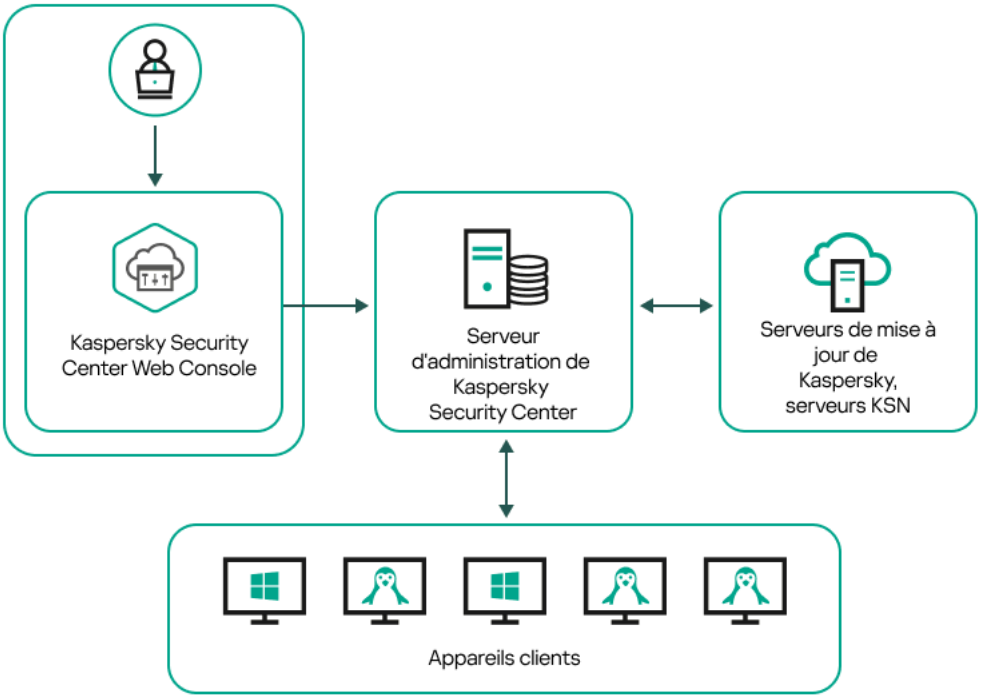
Plus d'informations à propos de Kaspersky Next Expert View et ses caractéristiques sont disponibles dans la documentation de Kaspersky Next Expert View et dans la documentation de Kaspersky Endpoint Security for Business.

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

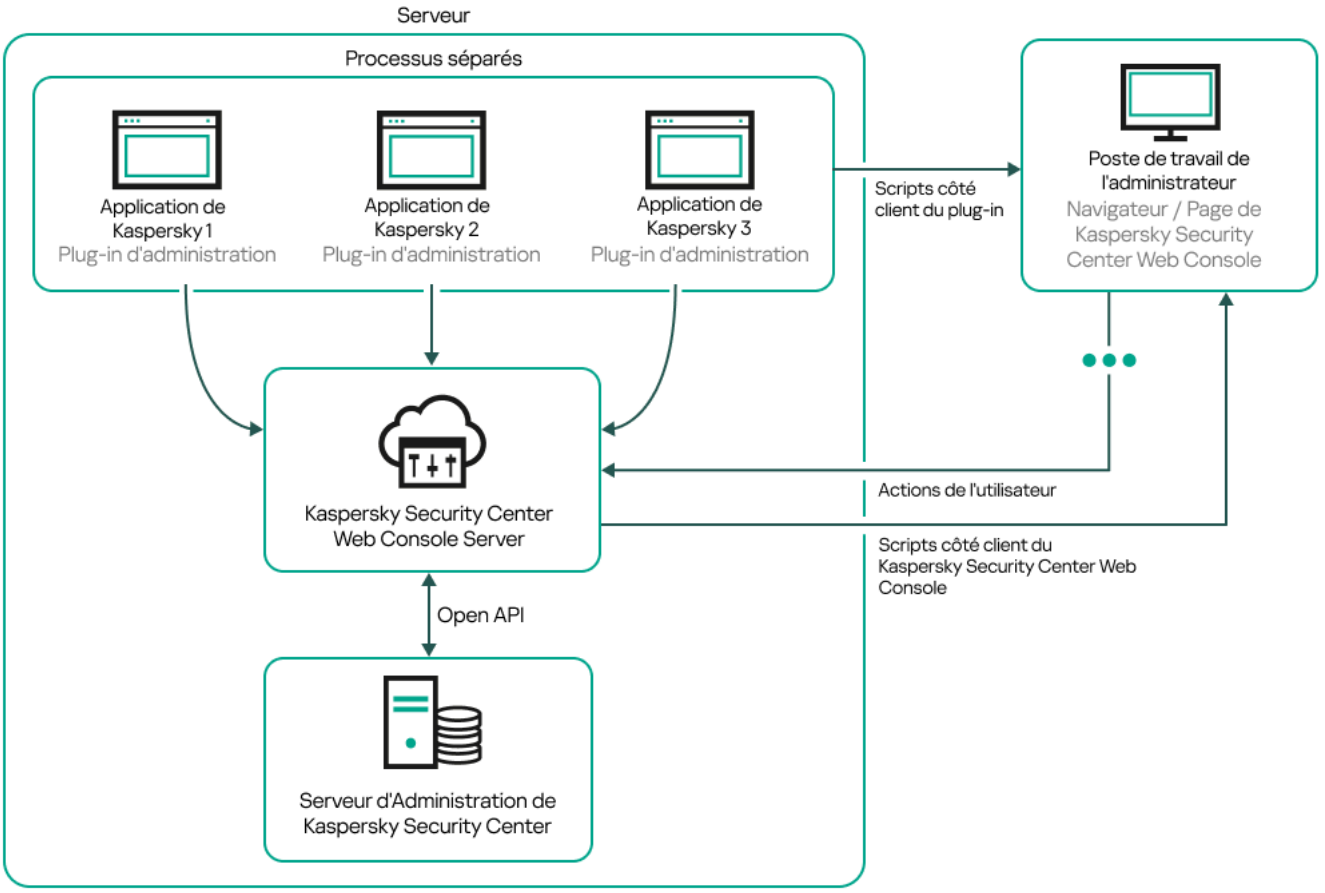


Diagramme de déploiement du Serveur d'administration de Kaspersky Security Center Linux et de Kaspersky Security Center Web Console

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 port	Nom du processus qui a ouvert le port	Protocole	Destination du port	Zone de fonctionnement
8060	klcsweb	TCP	Transfert des paquets d'installation publiés aux appareils client.	Publication des paquets d'installation. Vous pouvez modifier le numéro de port par défaut dans la section **Serveur 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 de port par défaut pour les connexions entrantes des Agents d'administration lors de la configuration des ports de connexion pendant l'installation de Kaspersky Security Center Linux. Vous pouvez modifier le port par défaut pour les connexions entrantes des Serveurs d'administration secondaires lors de la création de la hiérarchie des 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. L'utilitaire klakaut et son système d'aide se trouvent dans le dossier d'installation de Kaspersky Security Center Linux. 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 provenant du Gestionnaire des identités et des accès (IAM) vers le Serveur d'administration ; réception des connexions vers le 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.

Numéro de port	Nom du processus qui a ouvert le port	Protocole	Destination du port	Zone de fonctionnement
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 et est fermé par défaut. Pour des raisons de sécurité, nous vous recommandons d'utiliser le port TCP 13000.
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 est exécuté sur l'appareil)	ksnproxy	UDP	Réception des requêtes des appareils administrés au serveur proxy KSN	Serveur proxy KSN. Vous pouvez modifier le numéro de port par défaut dans la fenêtre des propriétés du Serveur d'administration.
17111 (uniquement si le service KSN Proxy est exécuté sur l'appareil)	ksnproxy	HTTPS	Réception des requêtes des appareils administrés au serveur proxy KSN	Serveur proxy KSN. Vous pouvez modifier le numéro de port par défaut dans la fenêtre des propriétés du Serveur d'administration.
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**).
13292 (uniquement si vous administrez des appareils mobiles)	klserver	TCP (TLS)	Réception des connexions des appareils mobiles	Administration des appareils mobiles. Vous pouvez modifier le numéro de port par défaut dans la fenêtre des propriétés du Serveur d'administration de la Console d'administration ou de Kaspersky Security Center Web Console.
19170	klserver	HTTPS (TLS)	Connexion en tunnel aux appareils administrés à l'aide de l'utilitaire klsctunnel	Connexion à distance aux appareils administrés à l'aide de Kaspersky Security Center Web Console. Vous pouvez modifier le numéro de port par défaut dans la fenêtre des propriétés du Serveur d'administration (**Général** → **Ports de connexion** → **Tunnel de connexion RDP**).
4444	kliam	HTTPS	Authentification en utilisant le protocole OpenID Connect	Échange de jetons d'authentification entre le navigateur et le Gestionnaire des identités et des accès (IAM).
9050	kliam	HTTPS	Connexion au Serveur d'administration via IAM	Échange de jetons d'authentification entre Kaspersky Security Center Web Console et IAM.

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 MDM iOS™ (uniquement si vous administrez des appareils mobiles).

Port utilisé par le serveur MDM iOS

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

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

Ports utilisés par le serveur de Kaspersky Security Center Web Console

Numéro de port	Nom du processus qui a ouvert le port	Protocole	Destination du port	Zone de fonctionnement
8080	Node.js : JavaScript côté serveur	TCP (TLS)	Réception des connexions du navigateur vers Kaspersky Security Center Web Console	Kaspersky Security Center Web Console. Vous pouvez modifier le numéro de port par défaut lors de l'installation de Kaspersky Security Center Web Console. Si vous installez Kaspersky Security Center Web Console sur le système d'exploitation ALT Linux, 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	Transfert des mises à jour des applications depuis l'Agent d'administration vers les applications Kaspersky installées localement à l'aide du composant 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.
17111 (uniquement si le service KSN Proxy est exécuté sur l'appareil)	ksnproxy	HTTPS	Réception des requêtes des appareils administrés au serveur proxy KSN	Serveur proxy KSN. Vous pouvez modifier le numéro de port par défaut dans les propriétés du point de distribution.
13295 (uniquement si vous utilisez le point de distribution comme serveur push)	klnagent	TCP (TLS)	Réception des connexions des appareils mobiles	Serveur push. Vous pouvez modifier le numéro de port par défaut dans les propriétés du point de distribution.
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.
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.

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

Ports utilisés sur 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

Le tableau ci-dessous indique le port qui doit être ouvert sur les appareils clients sur lesquels l'Agent d'administration n'est pas installé.

Port utilisé sur l'appareil client non défini

Numéro de port	Protocole	Destination du port	Zone de fonctionnement
22	SSH	Connexion à un appareil client via le protocole SSH	Installation à distance d'applications Kaspersky.

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, 2003	Service d'administration de Kaspersky Security Center Web Console	HTTPS	Ports de l'API utilisés pour recevoir les requêtes du " Service d'administration de Kaspersky Security Center Web Console " s'exécutant sur le même appareil.	Mise à jour des composants de Kaspersky Security Center Web Console
2005	Kaspersky Security Center Web Console	HTTPS	Port de l'API utilisé pour recevoir les requêtes du " Service d'administration de Kaspersky Security Center Web Console " s'exécutant sur le même appareil.	Exécution des processus node 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
4222	Kaspersky Security Center Web Console NATS	HTTPS	Ports API du courtier de messages basé sur NATS utilisés pour la communication entre les processus de Kaspersky Security Center Web Console et des plug-ins d'administration Le port 8222 est utilisé pour surveiller les NATS.	Interaction entre Kaspersky Security Center Web Console et les plug-ins d'administration
4444	Gestionnaire des identités et des accès (IAM)	HTTPS	Port utilisé par le protocole d'authentification OpenID Connect.	Échange de jetons d'authentification entre Kaspersky Security Center Web Console et le Gestionnaire des identités et des accès (IAM)
9050	IAM	HTTPS	Port utilisé par IAM.	Interaction entre Kaspersky Security Center Web Console et IAM

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 Linux 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 l'article suivant : 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.
- Utilisation de Kaspersky Security Center Linux par les prestataires de services. Il suffit au prestataire de services d'installer Kaspersky Security Center Linux 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 :

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

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

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

Serveur Web de Kaspersky Security Center Linux

Le Serveur Web de Kaspersky Security Center Linux (si après le Serveur Web) est un module de Kaspersky Security Center Linux. Le Serveur Web est utilisé pour publier les paquets d'installation autonomes ainsi que les fichiers du dossier partagé.

Les paquets d'installation créés sont publiés automatiquement sur le Serveur Web et sont supprimés après le premier chargement. L'administrateur peut transférer à l'utilisateur le lien formé à l'aide d'un moyen commode quelconque, par exemple, via email.

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

Paramètres du Serveur Web

Pour permettre la configuration approfondie du Serveur Web, les propriétés du Serveur Web prévoient la possibilité de remplacer les ports pour les protocoles HTTP (8060) et HTTPS (8061). De plus, outre la substitution des ports, il est possible de substituer le certificat serveur pour le protocole HTTPS et de remplace le nom de domaine complet du Serveur Web pour le protocole HTTP.

Paramètres du Serveur Web sur une passerelle de connexion

Un service de Serveur Web distinct est mise en œuvre sur un point de distribution en mode passerelle de connexion, ce qui permet de travailler avec des appareils mobiles connectés à Kaspersky Security Center Linux. Ce service est chargé de transférer les paquets d'installation d'applications et les profils de gestion des appareils vers les appareils sans les connecter directement au Serveur d'administration. Les fichiers sont transférés au fur et à mesure que le service traite les demandes de fichiers HTTP/HTTPS sur une passerelle de connexion.

Le service de Serveur Web sur une passerelle de connexion est installé en même temps que l'Agent d'administration Linux. Pour utiliser cette fonctionnalité, vous devez désigner un appareil qui servira de point de distribution en mode passerelle de connexion pour être utilisé comme Serveur Web, puis définir les paramètres correspondants. Pour obtenir des informations détaillées sur la configuration des paramètres du Serveur Web sur une passerelle de connexion, consultez l'aide de Kaspersky Secure Mobility Management.

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.

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)
- Site Internet de Kaspersky

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

- Le nom " Agent d'administration de Kaspersky "
- Configuré de manière à démarrer automatiquement au démarrage du système d'exploitation
- Utilisation du compte root

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

- 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

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

- Le nom " com.kaspersky.klnagent.core "
- Configuré de manière à démarrer automatiquement au démarrage du système d'exploitation
- Utilisation du compte root

Les noms des processus de service :

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

- Pour les appareils Windows :
  - klnagent
- Pour macOS :
  - com.kaspersky.klnagent

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 macOS :
  - Systèmes 64 bits : /Library/Application Support/Kaspersky Lab/klnagent/Binaries/klnagent

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.

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. Le nombre d'appareils pouvant être gérés par un Serveur d'administration dépend de la configuration de l'appareil qui héberge le Serveur d'administration et des restrictions SGBD.

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 d'administration à partir du site 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. Vous pouvez également sélectionner les appareils détectés sur le réseau par le Serveur d'administration.

- 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.

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.

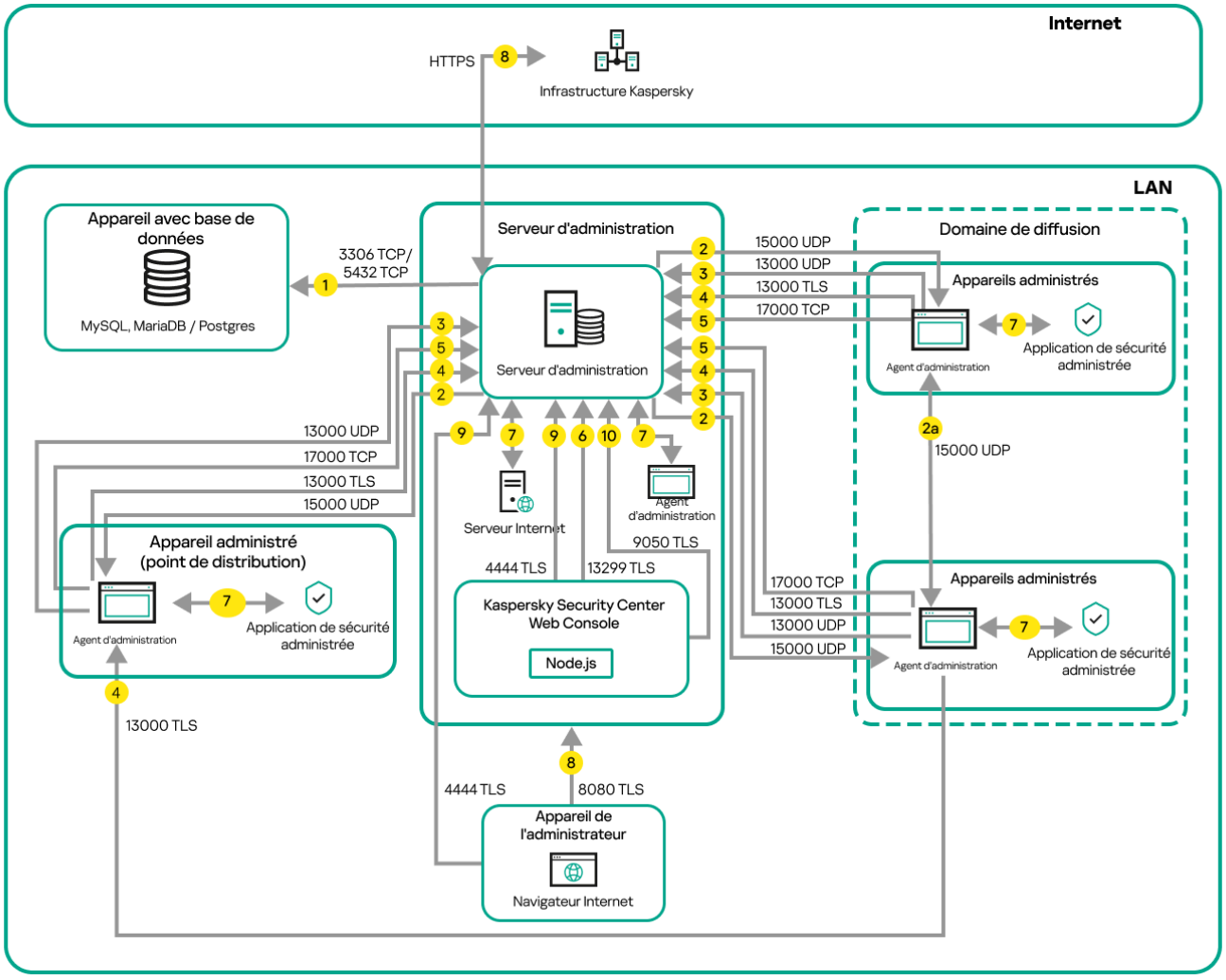
- Le Serveur d'administration virtuel peut analyser le réseau uniquement à l'aide des points de distribution qui y sont connectés.

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 un réseau local (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.

   Le module Gestionnaire des identités et des accès (IAM) se connecte au Serveur d'administration 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.

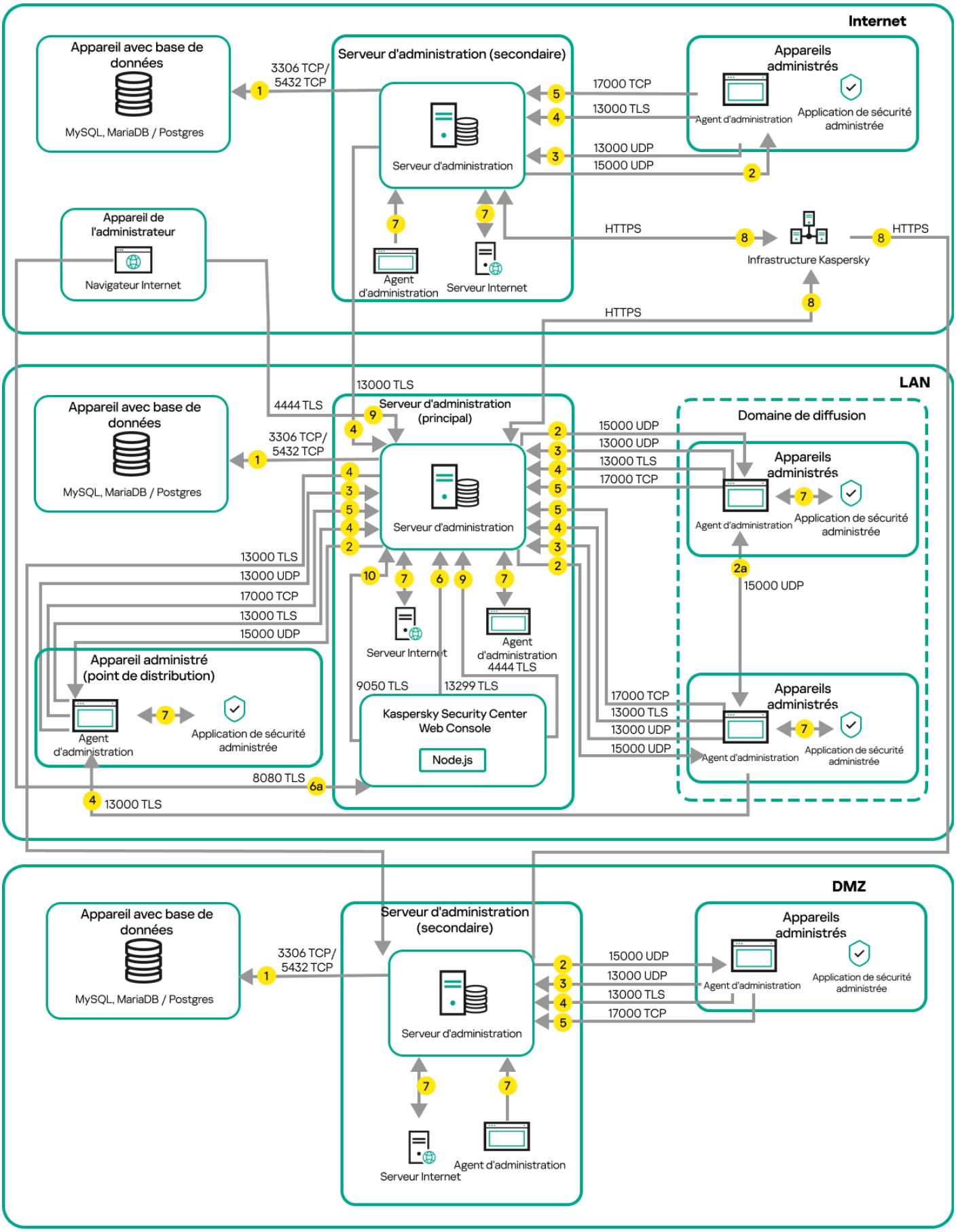
   Si vous ne voulez pas que votre Serveur d'administration accède à Internet, vous devez gérer ces données manuellement.

9. Kaspersky Security Center Web Console Server et le navigateur (utilisé avec Kaspersky Security Center Web Console) se connectent au Serveur d'administration via le protocole d'authentification OpenID Connect par le port TLS 4444.

10. Kaspersky Security Center Web Console Server se connecte au Serveur d'administration via le port TLS 9050.

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.

   Le module Gestionnaire des identités et des accès (IAM) se connecte au Serveur d'administration 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.

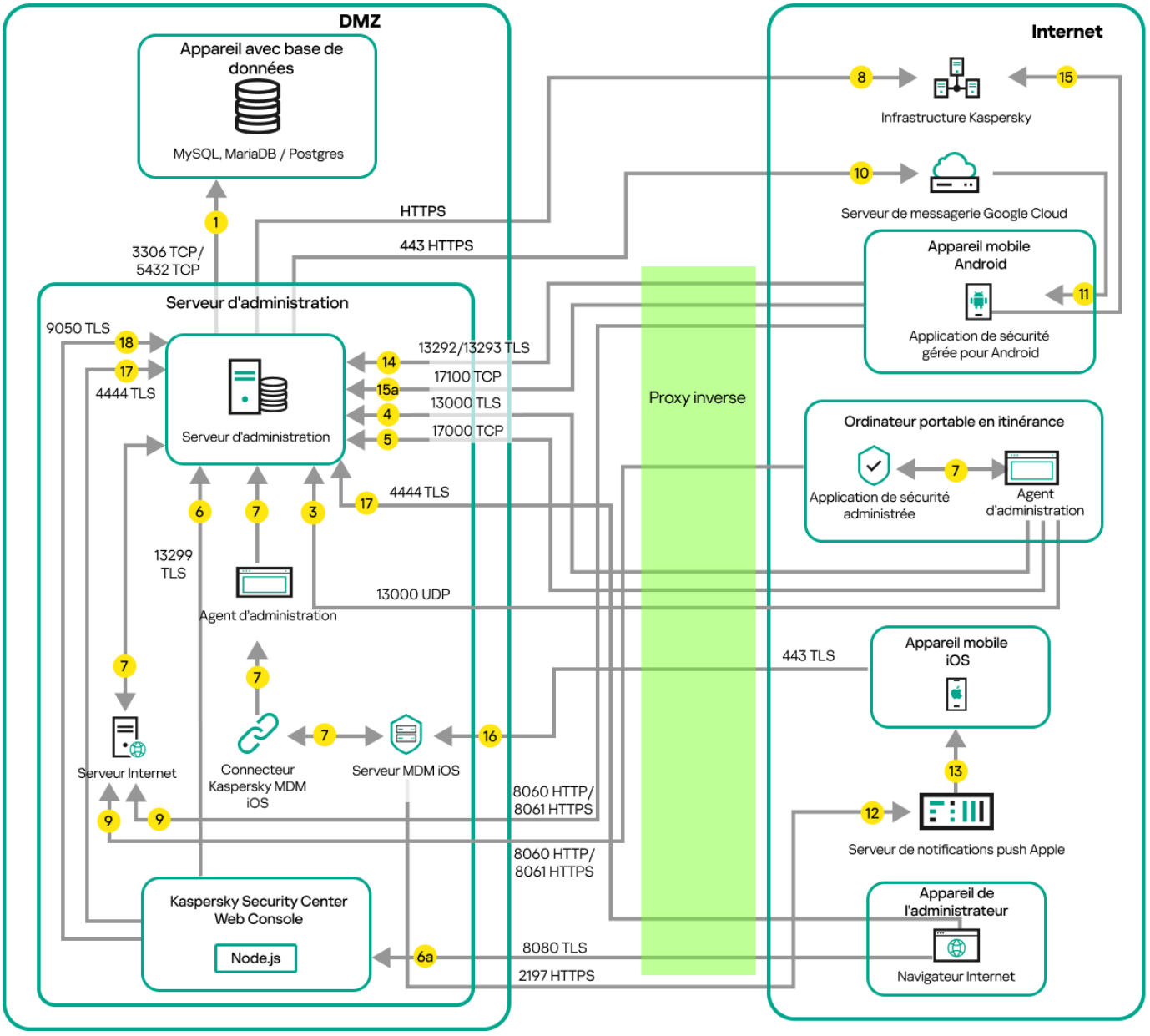
   Si vous ne voulez pas que votre Serveur d'administration accède à Internet, vous devez gérer ces données manuellement.

9. Kaspersky Security Center Web Console Server et le navigateur (utilisé avec Kaspersky Security Center Web Console) se connectent au Serveur d'administration via le protocole d'authentification OpenID Connect par le port TLS 4444.

10. Kaspersky Security Center Web Console Server se connecte au Serveur d'administration via le port TLS 9050.

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.

   Le module Gestionnaire des identités et des accès (IAM) se connecte au Serveur d'administration 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.

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

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

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

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

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

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

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

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

17. Kaspersky Security Center Web Console Server et le navigateur (utilisé avec Kaspersky Security Center Web Console) se connectent au Serveur d'administration via le protocole d'authentification OpenID Connect par le port TLS 4444.

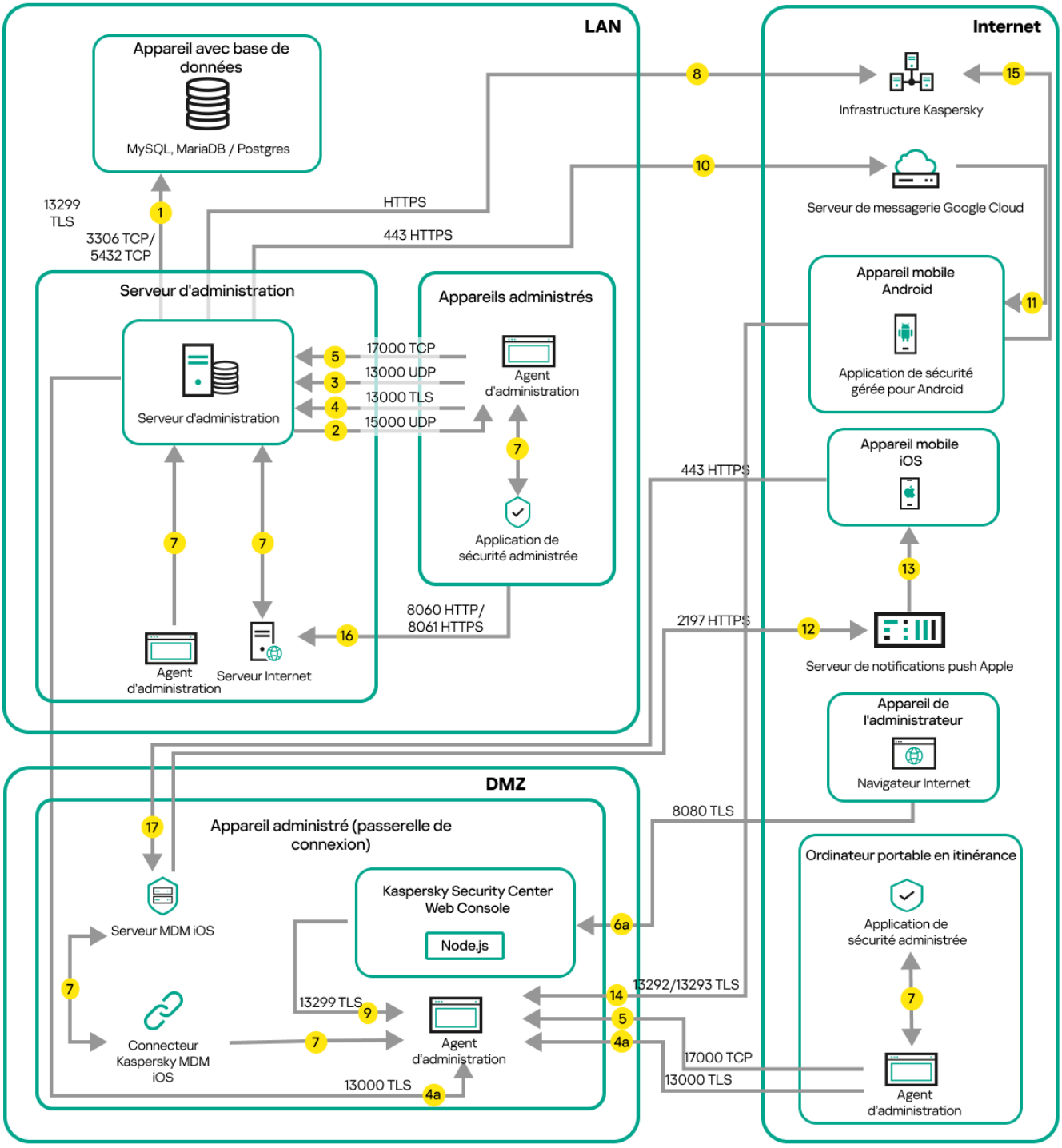
18. Kaspersky Security Center Web Console Server se connecte au Serveur d'administration via le port TLS 9050.

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.

Pour ce schéma de déploiement, l'authentification de domaine (authentification unique) fournie par le Gestionnaire des identités et des accès (IAM) n'est pas prise en charge.



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 ni 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.

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

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

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

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

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

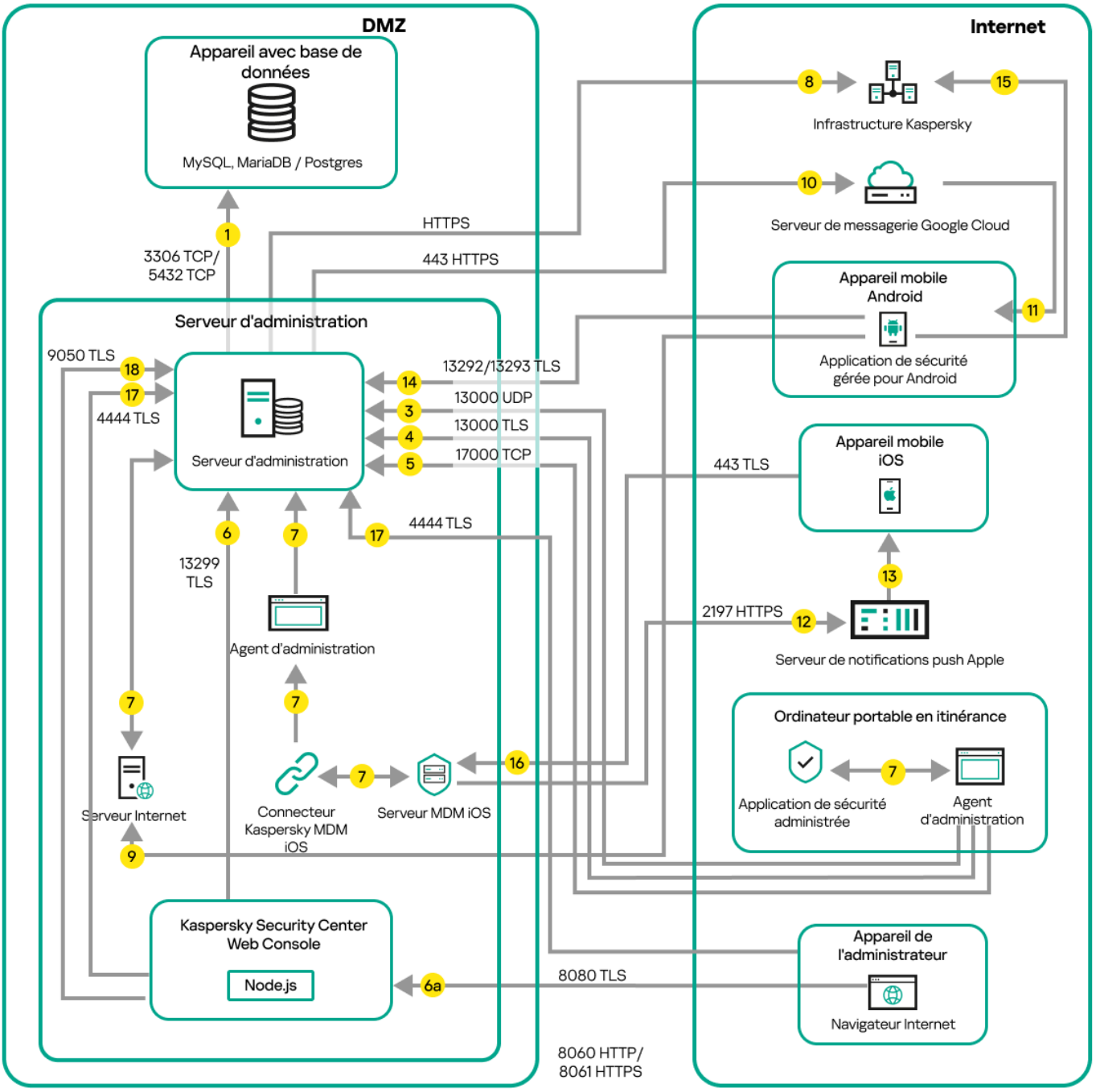
15. Pour les appareils mobiles uniquement : les données de l'appareil mobile sont transférées vers l'infrastructure de Kaspersky.

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

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

Serveur d'administration en DMZ, appareils administrés sur Internet

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

   Le module Gestionnaire des identités et des accès (IAM) se connecte au Serveur d'administration 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.

10. Pour les appareils mobiles Android uniquement : les données du Serveur d'administration sont transférées aux serveurs Google. Cette connexion sert à notifier aux appareils mobiles Android qu'ils doivent se connecter au Serveur d'administration. Ensuite, les notifications push sont envoyées aux appareils mobiles. Le service FCM fonctionne également sur le port HTTPS 443.

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

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

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

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

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

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

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

17. Kaspersky Security Center Web Console Server et le navigateur (utilisé avec Kaspersky Security Center Web Console) se connectent au Serveur d'administration via le protocole d'authentification OpenID Connect par le port TLS 4444.

18. Kaspersky Security Center Web Console Server se connecte au Serveur d'administration via le port TLS 9050.

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.

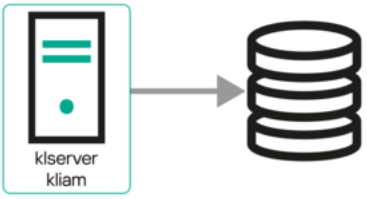
Conventions utilisées dans les schémas d'interaction

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

Icône	Valeur
	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 et du Gestionnaire des identités et des accès (IAM) sont stockées dans des bases de données distinctes au sein du même SGBD.



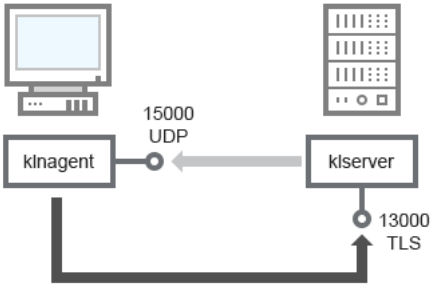
Serveur d'administration, Gestionnaire des identités et des accès et SGBD

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. Le port de connexion d'IAM au SGBD est indiqué par l'utilisateur lors de l'installation de Kaspersky Security Center Linux.

Le Serveur d'administration ne supprime pas automatiquement la base de données du Serveur d'administration et la base de données IAM lors de la désinstallation ou du déplacement du serveur vers un autre appareil. Le cas échéant, vous devez supprimer les bases de données manuellement.

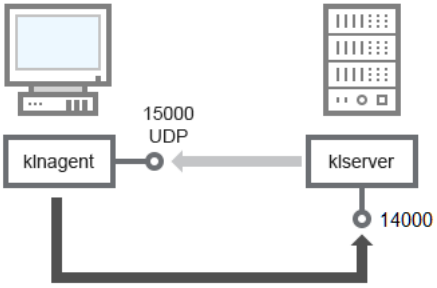
Serveur d'administration et appareil client : administration de l'application de sécurité

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)

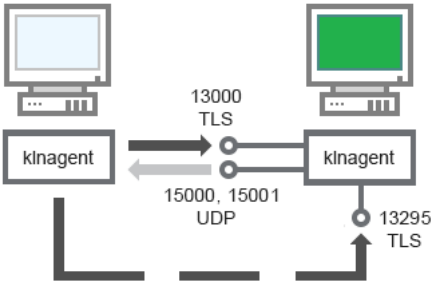
Pour avoir des explications sur les schémas, cf. tableau ci-après.

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.

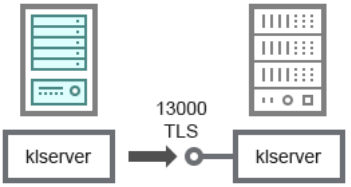
Mise à niveau du logiciel par un point de distribution (trafic)

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.



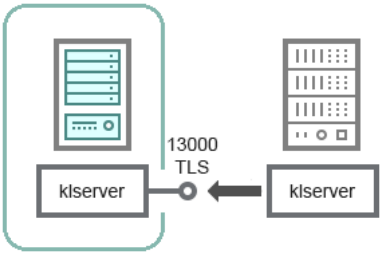
Hiérarchie des Serveurs d'administration : Serveur d'administration principal et Serveur d'administration secondaire

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

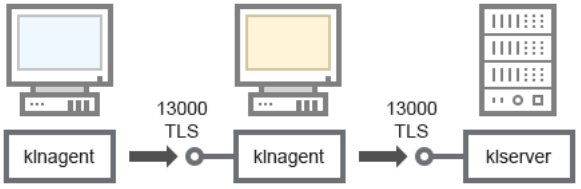
Le schéma illustre une hiérarchie de Serveurs d'administration dans laquelle le Serveur d'administration secondaire, situé dans la zone démilitarisée, reçoit une connexion d'un Serveur d'administration principal (les explications du schéma sont reprises dans le tableau ci-après). En cas de regroupement 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



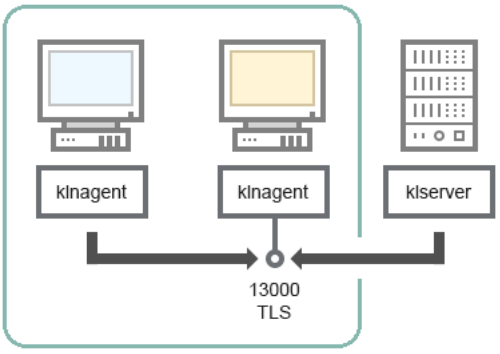
Serveur d'administration, passerelle de connexion dans un segment du réseau et appareil client

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



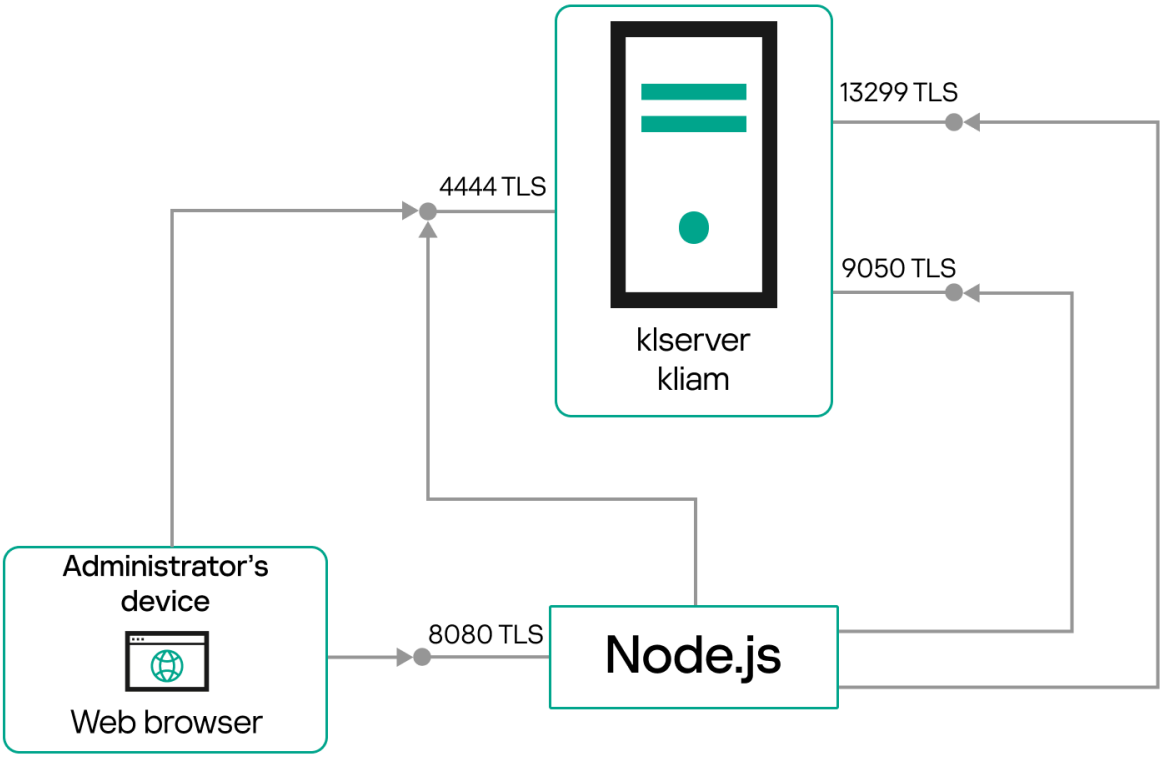
Serveur d'administration et passerelle de connexion et appareil client dans la zone démilitarisée

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

Serveur d'administration, 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 depuis Kaspersky Security Center Web Console et le Gestionnaire des identités et des accès (IAM) vers le Serveur d'administration via 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
Serveur d'administration	4444	kliam	TCP (TLS)	Réception des connexions de Kaspersky Security Center Web Console Server et du navigateur (utilisé avec Kaspersky Security Center Web Console) vers le Serveur d'administration avec IAM via le protocole d'authentification OpenID Connect
Serveur d'administration	9050	kliam	TCP (TLS)	Réception des connexions de Kaspersky Security Center Web Console vers IAM

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 de la société**

   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. Vous pouvez exporter des tâches et des stratégies pour les importer après la réinstallation. Consultez les articles suivants : Exportation d'une tâche, Exportation d'une stratégie.

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.

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 de l'utilitaire klbackup. Conservez la copie de sauvegarde des données 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

Liste de contrôle de renforcement

Déploiement du Serveur d'administration

- Installez le Serveur d'administration sur un serveur physique ou virtuel dédié.
- N'utilisez pas le serveur dédié pour exécuter d'autres services.

- N'installez pas le Serveur d'administration (ci-après dénommé " le Serveur ") sur les appareils suivants :
  - Contrôleur de domaine
  - Serveur de terminaux
  - Appareil de l'utilisateur

Sécurité des connexions

- Configurez un pare-feu pour restreindre l'accès à l'appareil serveur sur tous les ports et protocoles, à l'exception des ports requis par le serveur. Autorisez l'accès à l'appareil serveur uniquement à partir d'appareils de confiance.
- Configurez une liste d'autorisation d'adresses IP pour les ports serveur utilisés pour connecter Kaspersky Security Center Web Console (également appelée " Web Console ") au Serveur.
- Configurez le pare-feu pour autoriser l'accès au Serveur via Web Console uniquement à partir d'appareils de confiance.
- Configurez le protocole TLS version 1.2 ou ultérieure sur le Serveur.
- Configurez un pare-feu pour restreindre l'accès à l'appareil sur lequel le SGBD serveur est installé.
- Configurez l'authentification SSL entre le Serveur et le SGBD (MySQL ou PostgreSQL).

Comptes et authentification

- Configurez l'authentification à deux facteurs (TOTP, RFC 6238) pour l'accès au Serveur.
- N'installez pas l'application d'authentification sur le même appareil que celui à partir duquel la connexion au Serveur via Web Console est établie.
- Utilisez l'authentification à plusieurs facteurs (MFA) pour accéder à l'appareil serveur à l'aide d'un jeton, d'une carte à puce ou d'une autre méthode.
- Créez un groupe d'administration dédié pour l'appareil serveur et définissez une stratégie de sécurité spécifique pour celui-ci.
- Limitez le nombre d'utilisateurs ayant le rôle d'administrateur principal.
- Configurez les droits d'accès aux fonctionnalités du serveur en fonction des rôles des utilisateurs et des groupes.
- Autorisez l'installation à distance d'applications uniquement pour un compte utilisateur distinct.
- Réalisez un audit régulier de tous les utilisateurs de l'appareil serveur.

Gestion de la protection du Serveur d'administration

- Installez une application de sécurité sur l'appareil du Serveur :
  - Pour un serveur physique – Kaspersky Endpoint Security
  - Pour un serveur virtuel – Kaspersky Security for Virtualization
- Créez et appliquez une stratégie distincte pour la protection du Serveur (différente des stratégies de sécurité pour les autres appareils administrés).
- Activez tous les modules de protection disponibles dans l'application de sécurité.

Configuration des stratégies et des tâches pour les applications administrées

- Créez et appliquez des stratégies à tous les appareils administrés ou au groupe comprenant les nouveaux appareils administrés pour les applications suivantes :
  - Agent d'administration
  - Kaspersky Endpoint Security for Windows/Linux/macOS
  - Kaspersky Endpoint Agent (ou autres applications Kaspersky)
- Activez la protection par mot de passe contre la protection désactivée ou la désinstallation des applications Kaspersky.
- Verrouillez les paramètres des stratégies (fermez le " cadenas ") pour empêcher leur réattribution sur les appareils administrés.
- Créez une tâche d'analyse complète programmée pour tous les appareils.
- Activez l'utilisation de Kaspersky Security Network (KSN) et acceptez la dernière Déclaration de KSN.
- Configurez la recherche d'appareils et spécifiez le groupe d'administration par défaut pour les nouveaux appareils détectés.
- Limitez l'utilisation des règles automatiques de déplacement des appareils entre les groupes d'administration.
- Protégez les points de distribution contre tout accès non autorisé.
- Évitez d'attribuer automatiquement des points de distribution dans les petits réseaux ou les réseaux à haute importance.

Maintenance du Serveur d'administration

- Ne supprimez pas et ne désactivez pas les tâches suivantes :
  - Sauvegarde
  - Maintenance du Serveur d'administration
- Installez régulièrement les mises à jour du système d'exploitation et des logiciels tiers.

Transfert d'événements vers des systèmes tiers

- Configurez la surveillance et le signalement des événements de sécurité.
- Configurez l'exportation des événements vers un système SIEM.
- Configurez les notifications du Serveur pour :
  - Événements de l'audit
  - Événements critique
  - Événements d'échec et avertissements

Recommandations de sécurité pour les systèmes d'information des tiers

- Appliquez les recommandations de sécurité CIS Benchmarks aux systèmes d'exploitation, SGBD et hyperviseurs utilisés.
- Pour Astra Linux, suivez les recommandations de sécurité de la version correspondante de Red Book.
- Pour RED OS, suivez les recommandations fournies dans la documentation officielle RED OS.

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.

Interaction de la sécurité avec un SGBD externe

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

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

Par défaut, l'utilisateur de Kaspersky Security Center Linux peut se connecter à Kaspersky Security Center Linux depuis n'importe quel appareil sur lequel Kaspersky Security Center Web Console ou les applications OpenAPI sont installés. Vous pouvez configurer le Serveur d'administration afin que les utilisateurs puissent s'y connecter uniquement à partir d'appareils avec des adresses IP autorisées. Par exemple, si un intrus tente de se connecter à Kaspersky Security Center 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.

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

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

Sécurité de la connexion au contrôleur de domaine pendant le sondage

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

Comptes et authentification

Avant de suivre ces étapes, créez une copie de sauvegarde des données 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, puis enregistrez-la dans une localisation sûre. Conservez la copie de sauvegarde des données dans une localisation sûre.

Utilisation de l'authentification à deux facteurs avec le Serveur d'administration

Kaspersky Security Center Linux utilise l'authentification à deux facteurs lors de la connexion à Kaspersky Security Center Web Console sur la base de la norme RFC 6238 (TOTP : algorithme de mot de passe unique calculé en fonction du temps).

Chaque fois que vous vous connectez à Kaspersky Security Center Web Console, vous saisissez votre nom d'utilisateur et votre mot de passe, ainsi qu'un code de sécurité à usage unique. Pour recevoir un code de sécurité à usage unique, vous devez installer une application d'authentification sur votre ordinateur ou sur votre appareil mobile.

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

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

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

Pour garantir une protection complète à l'aide de l'authentification à deux facteurs, il est nécessaire de sécuriser non seulement le Serveur d'administration, mais également l'appareil sur lequel il est installé.

Lorsque vous vous connectez à l'appareil sur lequel le Serveur d'administration est installé (via SSH, RDP ou d'autres protocoles), nous vous recommandons d'utiliser l'authentification à plusieurs facteurs (MFA) avec un jeton, une carte à puce ou un autre mode d'authentification.

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 256 caractères.
- Le mot de passe doit compter des caractères d'au moins trois des groupes ci-dessous :
  - Lettres majuscules (A–Z)

- Lettre minuscules (a-z)
- Chiffres (0–9)
- Caractères spéciaux (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)

- Le mot de passe ne peut pas contenir d'espaces, de caractères Unicode ou de la combinaison " . " et " @ " lorsque " . " est placé devant " @ ".

Par défaut, le nombre maximal de tentatives de saisie du mot de passe autorisées est égal à 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.

Configuration des options de modification du mot de passe des comptes utilisateurs internes

Pour modifier le mot de passe d'un compte utilisateur interne, il est recommandé de configurer les paramètres suivants :

- Période de rotation des mots de passe
- Heure de l'avertissement préliminaire sur la nécessité de modifier le mot de passe
- Valeur de l'option **L'utilisateur doit changer son mot de passe lors de la première connexion**

Protection du compte contre les modifications non autorisées

Il est recommandé d'activer une option complémentaire pour protéger le compte utilisateur interne du Serveur d'administration contre les modifications non autorisées. Cette protection doit être configurée séparément pour chaque utilisateur interne.

Groupe d'administration dédié au Serveur d'administration

Pour le Serveur d'administration

Il est recommandé de créer un groupe d'administration dédié. 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 principal

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 ou du Serveur d'administration virtuel. 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 contre la sécurité associées à une éventuelle compromission d'un 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.

- Applications de sécurité recommandées. Si le Serveur d'administration est installé sur un appareil avec d'autres logiciels, nous vous recommandons de prendre en compte les recommandations de cet éditeur de logiciel sur la compatibilité des 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. Un point de distribution peut exécuter les mêmes méthodes de recherche d'appareils que le Serveur d'administration.

Placement des points de distribution sur le réseau de l'organisation utilisés pour :

- Réduire la charge sur le Serveur d'administration
- Optimisation du trafic
- Accorder au Serveur d'administration un accès aux appareils situés dans des parties difficiles d'accès du réseau

Compte tenu des capacités disponibles, nous recommandons de protéger les appareils qui font office de points de distribution contre tout type d'accès non autorisé (y compris physiquement).

Restriction de l'attribution automatique des points de distribution

Pour simplifier l'administration et maintenir le fonctionnement du réseau, nous vous recommandons d'utiliser l'attribution automatique des points de distribution. Cependant, pour les réseaux industriels et les petits réseaux, nous vous déconseillons d'attribuer automatiquement des points de distribution, car, par exemple, les informations privées des comptes utilisés pour transmettre les tâches d'installation à distance peuvent être transférées aux points de distribution au moyen de le système d'exploitation.

Pour les réseaux industriels et les petits réseaux, vous pouvez désigner manuellement des appareils comme points de distribution.

Vous pouvez également consulter le Rapport d'activité des points de distribution.

Exigences de sécurité pour les appareils des utilisateurs de Kaspersky Security Center Linux

Les appareils des utilisateurs de Kaspersky Security Center Linux doivent faire l'objet d'exigences particulières en matière de sécurité. Il est conseillé de protéger ces appareils contre tout type d'accès non autorisé (y compris physique).

Voici quelques-uns des appareils utilisés par les utilisateurs de Kaspersky Security Center Linux :

- Appareils à partir desquels les utilisateurs de Kaspersky Security Center Linux se connectent à Kaspersky Security Center Web Console à l'aide d'un navigateur.
- Les appareils à partir desquels les applications qui interagissent avec le Serveur d'administration via OpenAPI sont connectés à Kaspersky Security Center Linux.

Exigences de sécurité pour les appareils sur lesquels le programme d'installation de Kaspersky Security Center Web Console est installé

Les appareils sur lesquels Kaspersky Security Center Web Console est installé sont utilisés pour gérer Kaspersky Security Center Linux. Des exigences particulières doivent donc s'appliquer à la sécurité de ces appareils. Il est conseillé de protéger ces appareils contre tout type d'accès non autorisé (y compris physique).

Configuration de la protection des applications administrées

Stratégies d'application administrées

Nous vous recommandons de créer une stratégie pour chaque type d'applications utilisées et de 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.

Recommandations de sécurité pour les systèmes d'information des tiers

Recommandations de sécurité de CIS Benchmarks

Si vous utilisez des versions de systèmes d'exploitation, de plateformes de virtualisation ou de serveurs de base de données prises en charge par le Serveur d'administration et l'Agent d'administration, nous vous recommandons d'appliquer les pratiques exemplaires en matière de sécurité de l'information du Center for Internet Security (CIS), le cas échéant, afin de paramétrer au mieux ces systèmes d'information.

Le Centre pour la sécurité d'Internet (CIS) est une organisation à but non lucratif qui se consacre à l'amélioration de la sécurité dans le domaine des technologies de l'information. Le CIS élabore et diffuse notamment des normes de sécurité comme CIS Controls et CIS Benchmarks. Celles-ci constituent un ensemble de recommandations et de pratiques permettant d'assurer la sécurité des systèmes d'information.

Le portail CIS contient des recommandations pour les versions des systèmes d'information suivants prises en charge par le Serveur d'administration et l'Agent d'administration :

- Les systèmes d'exploitation des catégories suivantes :
  - Windows pour les ordinateurs de bureau
  - Windows pour les serveurs
  - Debian
  - Ubuntu
  - CentOS
  - Oracle Linux
  - Red Hat Enterprise Linux
  - SUSE Linux Enterprise Server
  - macOS
- Plateformes de virtualisation VMware
- Serveurs de bases de données :
  - Microsoft SQL Server
  - MySQL
  - MariaDB
  - PostgreSQL

Recommandations de sécurité pour le système d'exploitation Astra Linux

Si vous utilisez le système d'exploitation Astra Linux, il convient de suivre les recommandations de sécurité décrites dans le livre rouge pour la version correspondante d'Astra Linux.

Recommandations de sécurité pour le système d'exploitation RED OS

Si vous utilisez le système d'exploitation RED OS, il convient de suivre les recommandations de sécurité du guide de l'administrateur décrites dans la documentation officielle de RED OS.

Recommandations relatives à l'utilisation des applications de sécurité de Kaspersky

Utilisation du mot de passe KLAdmin dans Kaspersky Endpoint Security for Windows

Le compte KLAdmin est un compte administrateur avec un accès libre à Kaspersky Endpoint Security for Windows. Le compte KLAdmin a le droit d'effectuer toute action protégée par mot de passe dans Kaspersky Endpoint Security for Windows, y compris supprimer l'application. Les autorisations du compte KLAdmin ne peuvent pas être révoquées. Vous pouvez définir le mot de passe du compte KLAdmin dans les propriétés de la stratégie de Kaspersky Endpoint Security for Windows. L'administrateur de Kaspersky Endpoint Security for Windows est entièrement responsable de la protection du mot de passe du compte KLAdmin. Si votre organisation a sa propre stratégie de mot de passe, suivez les instructions de cette stratégie. Plus le mot de passe est long et complexe, plus il est fiable.

Voici nos recommandations pour protéger l'organisation contre le vol du mot de passe KLAdmin :

- **Exigences générales**

  N'utilisez pas le nom du compte ou une partie de son nom comme mot de passe.

- **Longueur minimale du mot de passe requise**

  Créez un mot de passe d'au moins 10 caractères.

- **Conditions d'utilisation de plusieurs types de caractères**

  Définissez un mot de passe complexe qui contient des caractères de différentes catégories : lettres minuscules et majuscules, chiffres et caractères spéciaux.

- **Conditions d'expiration du mot de passe**

  Définissez une date d'expiration minimum du mot de passe de 90 jours. Le nouveau mot de passe ne doit correspondre à aucun des 24 derniers mots de passe.

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 < chemin vers 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**

   Utilisez l'utilitaire klscflag pour créer les indicateurs de serveur et indiquez le chemin d'accès aux fichiers de certificat comme valeur :

   ```
   klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_CA -v < chemin vers ca-cert.pem> -t
   s
   ```

   ```
   klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_CERT -v < chemin vers server-
   cert.pem> -t s
   ```

   ```
   klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_KEY -v < chemin vers server-key.pem>
   -t s
   ```

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

   Exécutez la commande suivante :

   ```
   klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_SSL_CA -v < chemin vers psql.crt>
   -t s
   ```

   Authentification SSL bidirectionnelle

   Utilisez l'utilitaire klscflag pour créer les indicateurs de serveur et indiquez le chemin d'accès aux fichiers de certificat comme valeur.

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

   Exécutez les commande suivantes :

   ```
   klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_SSL_CA -v < chemin vers
   psql.crt> -t s
   klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_SSL_CERT -v < chemin vers
   postgres.crt> -t s
   ```

```
klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_SSL_KEY -v <chemin vers postgres.key> -t s
```

Si `postgres.key` requiert une phrase secrète, créez un indicateur KLSRV_POSTGRES_OPT_TLS_PASPHRASE et indiquez la phrase secrète comme valeur :

```
klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_TLS_PASPHRASE -v <phrase secrète> -t s
```

7. **Relancer le service du Serveur d'administration**

Préparatifs du déploiement

Cette section décrit comment choisir l'option de déploiement de Kaspersky Security Center Linux , la configuration de Kaspersky Security Center Linux et un SGBD en fonction des besoins de votre organisation.

Il existe plusieurs options de déploiement des composants de Kaspersky Security Center Linux sur le réseau d'une organisation, en fonction des critères suivants :

- 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

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. article "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. article "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 l'intégration avec l'infrastructure à clés publiques (PKI) de l'entreprise

- Pour attribuer les valeurs souhaitées des champs du certificat
- Pour garantir la robustesse souhaitée du chiffrement du certificat

Sélection de la configuration 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.

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 l'article suivant pour plus de détails : Activation d'un serveur push.

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 distinct est attribué et intégré à la hiérarchie générale des Serveurs d'administration. 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.

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®.

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.
Tantor (voir versions prises en charge)	Utilisez ce SGBD si vous prévoyez d'utiliser un seul Serveur d'administration pour moins de 50 000 appareils. Le SGBD Tantor est pris en charge uniquement sur Astra Linux Special Edition RUSB.10015-01 (mise à jour opérationnelle 1.8).

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 que 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
- Administration des 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).

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

Pour configurer correctement le serveur MariaDB x64 afin qu'il fonctionne avec Kaspersky Security Center, vous devez utiliser les paramètres par défaut du serveur, à l'exception des paramètres indiqués dans cet article.

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=< 80 % de la RAM allouée au SGBD ; consultez la documentation
de votre SGBD pour obtenir des recommandations >
innodb_thread_concurrency=20
innodb_flush_log_at_trx_commit=0
innodb_lock_wait_timeout=300
max_allowed_packet=32M
max_connections=151
max_prepared_stmt_count=12800
table_open_cache=60000
table_open_cache_instances=4
table_definition_cache=60000
sql_mode="STRICT_TRANS_TABLES,NO_AUTO_CREATE_USER,NO_ENGINE_SUBSTITUTION"
```

   La valeur de `innodb_buffer_pool_size` ne doit pas être inférieure à 80 % de la taille de base de données KAV attendue. Notez que la mémoire indiquée est allouée au démarrage du serveur. Si la taille de la base de données est inférieure à la taille de la mémoire tampon indiquée, seule la mémoire requise est allouée. Si vous utilisez MariaDB 10.4.3 ou une version antérieure, la taille réelle de la mémoire allouée est supérieure d'environ 10 % à la taille de la mémoire tampon indiquée. Pour obtenir des recommandations sur la configuration du paramètre `innodb_buffer_pool_size` ainsi que d'autres informations, consultez 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 MariaDB. Assurez-vous que le paramètre `innodb_file_per_table` présente la valeur `1`.

   Pour MariaDB 10.1, saisissez également les lignes suivantes dans la section [mysqld] :

```
innodb_file_format='Barracuda'
```

```
innodb_default_row_format=dynamic
innodb_large_prefix=1
```

Pour MariaDB 10.6, saisissez également les lignes suivantes dans la section [mysqld] :

```
optimizer_prune_level=0
optimizer_search_depth=8
```

Par défaut, les modules complémentaires d'optimisation `join_cache_incremental`, `join_cache_hashed` et `join_cache_bka` sont activés. Si ces modules complémentaires ne sont pas activés, vous devez les activer.

Pour vérifier si les modules complémentaires d'optimisation sont activés :

1. Dans la console client MariaDB, exécutez la commande :

   ```
   SELECT @@optimizer_switch;
   ```

2. 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.

Pour assurer la stabilité du service MariaDB systemd en cas de charge, augmentez la limite par défaut des fichiers qui peuvent être ouverts (descripteurs de fichiers).

Pour augmenter la limite des descripteurs de fichiers :

1. Exécutez la commande suivante :

   ```
   sudo systemctl edit mariadb.service
   ```

2. Spécifiez la limite du nombre de descripteurs de fichiers dans le paramètre `LimitNOFILE` de la section `[Service]` :

   ```
   LimitNOFILE=1048576
   ```

3. Exécutez la commande suivante pour vous assurer que les paramètres sont indiqués correctement :

   ```
   sudo systemd-analyze verify mariadb.service
   ```

4. Exécutez la commande suivante pour recharger le processus systemd :

   ```
   sudo systemctl daemon-reload
   ```

5. Exécutez la commande suivante pour redémarrer le service MariaDB :

   ```
   sudo systemctl restart mariadb.service
   ```

La limite des descripteurs de fichiers est désormais augmentée.

Configuration du serveur PostgreSQL ou Postgres Pro pour fonctionner avec Kaspersky Security Center Linux

Pour configurer correctement le serveur PostgreSQL ou Postgres Pro afin qu'il fonctionne avec Kaspersky Security Center Linux, vous devez utiliser les paramètres par défaut du serveur, à l'exception des paramètres indiqués dans cet article.

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`

Sur le système d'exploitation ALT Linux, le chemin d'accès par défaut est
`/var/lib/pgsql/data/postgresql.conf`

Paramètres recommandés pour PostgreSQL et Postgres Pro :

- `max_connections = 151`

  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.

- `shared_buffers` = N

  N = 25 % de la taille estimée de la RAM du SGBD. Si le SGBD est installé sur un appareil aux côtés du Serveur d'administration, le calcul doit se baser sur la RAM allouée au SGBD, et non sur la RAM totale de l'appareil.

  Si la RAM est inférieure à 1 Go, laissez la valeur par défaut.

- `temp_buffers = 24MB`

- `work_mem = 16MB`

- `maintenance_work_mem = 128MB`

- `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

- `max_parallel_workers_per_gather = 0`

- `standard_conforming_strings` = `on`

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`

Actualisez la configuration ou redémarrez le serveur SGBD après la mise à jour du fichier de configuration.

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 l'article suivant 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.

Pour en savoir plus sur la configuration d'un cluster de SGBD à haute disponibilité, consultez l'article suivant : Préparation du cluster de SGBD haute disponibilité pour le fonctionnement de Kaspersky Security Center Linux.

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

Pour configurer correctement le serveur MySQL x64 afin qu'il fonctionne avec Kaspersky Security Center, vous devez utiliser les paramètres par défaut du serveur, à l'exception des paramètres indiqués dans cet article.

Si vous utilisez le 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.cnf :
```
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=< 80 % de la RAM allouée au SGBD ; consultez la documentation
de votre SGBD pour obtenir des recommandations >
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 obtenir des recommandations sur la configuration du paramètre `innodb_buffer_pool_size` ainsi que d'autres informations, consultez 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`.

Préparation du cluster de SGBD haute disponibilité pour le fonctionnement de Kaspersky Security Center Linux

Kaspersky Security Center Linux prend en charge les clusters à haute disponibilité suivants :

- Platform V Pangolin
- Haute disponibilité intégrée à Postgres Pro
- Patroni (avec un équilibreur de charge HAProxy en option)

Le type de réplication doit être défini sur " synchrone ".

Si vous utilisez le modèle Patroni version 3.3.1 ou antérieure pour PostgreSQL, assurez-vous que le paramètre `synchronous_standby_names` est appliqué correctement.

Pour vérifier que la réplication synchrone est utilisée, exécutez la requête suivante sur le nœud principal :

```
SELECT application_name, client_addr, client_hostname, client_port, sync_state FROM pg_stat_replication;
```

Si la colonne `sync_state` d'un nœud affiche des valeurs autres que `sync` ou `potential`, le cluster utilise la réplication asynchrone, qui n'est pas prise en charge. Pour résoudre ce problème, effectuez une des opérations suivantes :

Effectuez la mise à jour de Patroni vers la version 3.3.2 ou une version ultérieure.

Dans le fichier de configuration de Patroni, repérez la sous-section `dcs` de la section `bootstrap` et définissez le paramètre `synchronous_mode` sur `true` :

```
bootstrap:
dcs:
<...>
synchronous_mode: true
```

Une configuration minimale recommandée pour un cluster de SGBD haute disponibilité doit inclure au moins trois nœuds :

Pour préparer un cluster de SGBD haute disponibilité pour le fonctionnement de Kaspersky Security Center Linux, procédez comme suit :

1. Configurez le serveur PostgreSQL ou Postgres Pro pour qu'il fonctionne avec Kaspersky Security Center Linux.

2. Si vous souhaitez que le Serveur d'administration détecte automatiquement les adresses des nœuds du cluster, il vous suffit d'indiquer le nom DNS ou l'adresse IP du nœud de contrôle ou du nœud de réplique lors de l'installation. Pour ce faire :

   a. Modifiez le fichier de configuration /etc/pangolin-manager/postgres.yml (si vous utilisez Platform V Pangolin) ou /etc/postgresql/<VERSION>/main/postgresql.conf (si vous utilisez le cluster Postgres Pro Built-in High Availability) sur tous les nœuds du cluster de SGBD haute disponibilité en ajoutant la ligne suivante à la section `postgresql` :

   `log_hostname=1`

   Pour les autres paramètres du fichier de configuration, vous pouvez utiliser les valeurs recommandées pour PostgreSQL et Postgres Pro.

   b. Après avoir modifié le fichier de configuration, redémarrez le service du cluster de SGBD sur tous les nœuds du cluster de SGBD haute disponibilité.

   c. Vérifiez que l'utilisateur de la base de données dispose du privilège `pg_read_all_stats`. Vous pouvez accorder ce privilège à l'aide de la commande suivante :

   `GRANT pg_read_all_stats TO "%1";`

   où `%1` est le nom de l'utilisateur de la base de données.

   Le nom d'utilisateur est indiqué lors du programme d'installation du Serveur d'administration dans le paramètre `KLSRV_UNATT_DBMS_LOGIN`.

   d. Configurez l'équilibreur de charge pour la base de données IAM. Consultez la documentation relative à l'équilibreur de charge que vous avez choisi.

Le cluster de SGBD haute disponibilité est prêt à fonctionner avec Kaspersky Security Center Linux.

Installation de Kaspersky Security Center Linux

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

Avant de procéder à l'installation, vous devez effectuer les opérations suivantes :

- Installez le SGBD pour Kaspersky Security Center Linux. Vous pouvez choisir l'un des SGBD 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.

Après avoir installé le SGBD, suivez les instructions correspondantes :

- Configuration du serveur PostgreSQL ou Postgres Pro pour fonctionner avec Kaspersky Security Center Linux

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

  Si vous souhaitez que le Serveur d'administration détecte automatiquement les adresses des nœuds du cluster, il vous suffit d'indiquer le nom DNS ou l'adresse IP du nœud de contrôle ou du nœud de réplique lors de l'installation. Pour ce faire, assurez-vous d'avoir effectué l'étape 2 de la procédure Préparation d'un cluster de SGBD haute disponibilité pour une utilisation avec Kaspersky Security Center Linux.

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

  Configuration du compte SGBD pour travailler avec MySQL et MariaDB

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

  Configuration du compte SGBD pour travailler avec MySQL et MariaDB

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

  Si vous utilisez 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 du Serveur d'administration.

- Assurez-vous que le serveur DNS est disponible sur le réseau.

- Téléchargez le fichier d'installation dans la langue souhaitée depuis le site Internet de Kaspersky. Choisissez le fichier d'installation correspondant à la distribution Linux installée sur votre appareil : ksc64_<version_number>_amd64.deb ou ksc64-<version_number>.x86_64.rpm.

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

Pendant l'installation du Kaspersky Security Center Linux:

1. Créez un groupe " kladmins " et des comptes sans privilèges " ksc " et " ksciam ". Les comptes doivent être membres du groupe " kladmins ". Pour ce faire, exécutez les commandes suivantes en séquence :

   `adduser ksc`

   `groupadd kladmins`

   `gpasswd -a ksc kladmins`

   `usermod -g kladmins ksc`

   `adduser ksciam`

   `gpasswd -a ksciam kladmins`

   `usermod -g kladmins ksciam`

2. Sur serveur SGBD, créez une base de données pour IAM. Le nom de la base de données doit être différent de celui de la base de données que vous avez installée pour fonctionner avec Kaspersky Security Center Linux. Le Serveur d'administration ne supprime pas automatiquement la base de données IAM lors de la désinstallation ou du déplacement du serveur vers un autre appareil. Vous devez supprimer la base de données manuellement.

   - Pour PostgreSQL, exécutez la commande suivante :

     ```
     sudo -i -u postgres psql -U postgres -c "CREATE DATABASE <iam_db_name>;"
     ```

   - Pour MariaDB, exécutez la commande suivante :

     ```
     sudo mysql -u root -p -e "CREATE DATABASE <iam_db_name>;"
     ```

3. Si vous utilisez un cluster de SGBD haute disponibilité, procédez comme suit :

   a. Accordez à l'utilisateur 'ksc' le privilège `pg_read_all_stats` :

   ```
   GRANT pg_read_all_stats TO "ksc";
   ```

   b. Modifiez le fichier de configuration /etc/pangolin-manager/postgres.yml (si vous utilisez Platform V Pangolin) ou /etc/postgresql/main/postgresql.conf (si vous utilisez le cluster Postgres Pro Built-in High Availability) sur tous les nœuds du cluster de SGBD haute disponibilité. Ajoutez la ligne suivante à la section `postgresql` si vous souhaitez indiquer uniquement le nom DNS ou l'adresse IP du nœud principal ou du nœud de réplique lors de la connexion du cluster à Kaspersky Security Center Linux :

   ```
   log_hostname: '1'
   ```

   c. Après avoir modifié le fichier de configuration /etc/pangolin-manager/postgres.yml, redémarrez le service du cluster de SGBD sur tous les nœuds du cluster de SGBD haute disponibilité (à l'exception du nœud arbitre) comme suit :

   ```
   systemctl restart pangolin-manager.service
   ```

   ou

   ```
   systemctl restart postgresql-<version>
   ```

4. Si besoin, 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 <max_number_of_opened_files>`

   `ksc hard nofile <max_number_of_opened_files>`

   Par défaut, les limites des descripteurs de fichiers sont spécifiées lors de l'installation. La limite des fichiers souples est de 32 768 fichiers, la limite des fichiers fixes est de 131 072 fichiers.

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

```
sudo apt-get install /<path>/ksc64_<version_number>_amd64.deb
```

```
sudo yum install /<path>/ksc64-<version_number>.x86_64.rpm
```

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

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

7. 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 du CLUF. 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 si 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.

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

   a. Sélectionnez **Standard** comme mode d'installation du Serveur d'administration.

   b. Saisissez le FQDN ou le nom DNS du Serveur d'administration. Ce nom sera utilisé par d'autres appareils pour se connecter au Serveur d'administration.

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

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

      - Si vous avez entre 1 et 100 appareils administrés, saisissez 1.
      - Si vous avez entre 101 et 1 000 appareils administrés, saisissez 2.
      - Si vous avez plus de 1 000 appareils administrés, saisissez 3.

      Ce paramètre est utilisé pour retarder de manière automatiquement aléatoire le démarrage des tâches afin d'optimiser la charge du réseau. La liste ci-dessous indique l'intervalle dans lequel le décalage est calculé :

      - De 1 à 100 appareils administrés, valeur 1. Le décalage n'est pas utilisé.
      - De 101 à 1 000 appareils administrés, valeur 2. Le décalage est de 5 minutes.
      - Plus de 1 000 appareils administrés, valeur 3. Le décalage est de 10 minutes.

   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. 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.

i. Saisissez le nom DNS ou l'adresse IP de l'appareil sur lequel la base de données du Serveur d'administration est installée. 127.0.0.1 par défaut pour une installation locale du SGBD.

Pour utiliser un cluster de basculement haute disponibilité, procédez de l'une des manières suivantes :

- Saisissez les noms DNS ou les adresses IP et les ports de tous les nœuds au format suivant :

```
<fqdn1>:<port>,<fqdn2>:<port>,<...><fqdnX>:<port>;
```

- Indiquez uniquement le nom DNS ou l'adresse IP du nœud principal ou du nœud de réplique.

j. Saisissez le numéro de port de la base de données. Ce port sert à communiquer avec le Serveur d'administration. Cette étape est ignorée si vous avez saisi les noms DNS ou les adresses IP et les ports de tous les nœuds du cluster à haute disponibilité à l'étape 8.h.

Par défaut, les ports suivants sont utilisés :

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

k. Saisissez le nom de la base de données.

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

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

n. Saisissez le FQDN ou le nom DNS du serveur IAM. Si vous n'indiquez pas cette variable, le nom DNS de l'appareil sur lequel le Serveur d'administration est installé est utilisé.

Saisissez la valeur que vous avez indiquée à l'étape 8b.

o. Saisissez le nom du compte pour lancer le service IAM. Le compte doit faire partie du groupe de sécurité saisi. Par défaut, le compte ksciam est utilisé.

p. Sélectionnez le SGBD que vous avez installé et qui doit fonctionner avec le service IAM :

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

q. Saisissez l'adresse du SGBD IAM qui sera utilisé par le service IAM.

Pour utiliser un cluster haute disponibilité, procédez de l'une des manières suivantes :

- Saisissez les noms DNS ou les adresses IP et les ports de tous les nœuds au format suivant :

  ```
  <fqdn1>:<port>,<fqdn2>:<port>,<...><fqdnX>:<port>;
  ```

- Indiquez uniquement le nom DNS ou l'adresse IP de l'équilibreur de charge.

r. Saisissez le numéro de port du SGBD IAM. Ce port sert à communiquer avec le service IAM. Cette étape est ignorée si vous avez saisi les noms DNS ou les adresses IP et les ports de tous les nœuds du cluster haute disponibilité à l'étape 8.p.

   Par défaut, les ports suivants sont utilisés :

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

s. Saisissez le nom de la base de données IAM qui sera utilisée par le service IAM. Le nom de la base de données utilisée par le service IAM doit être différent de la base de données utilisée par le Serveur d'administration.

t. Saisissez l'identifiant de connexion du compte de la base de données que vous utilisez pour accéder à la base de données IAM.

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

   Attendez que les services soient ajoutés et lancés automatiquement :

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

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

Si vous passez cette étape, vous pouvez utiliser la commande suivante pour créer un autre utilisateur ultérieurement :

```
/opt/kaspersky/ksc64/sbin/kladduser -n kscadmin -p <password>
```

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

Si le Serveur d'administration n'a pas accès au dépôt des paquets de distribution des applications pour l'installation à distance, téléchargez les dépendances nécessaires à la création des paquets d'installation permettant d'installer des applications sur des appareils Windows comme suit :

1. Créez l'indicateur RIUtilsArchiveDirUsed en exécutant la commande suivante :

   `/opt/kaspersky/ksc64/sbin/klscflag -fset -pv klserver -n RIUtilsArchiveDirUsed -t d -v 1`

2. Exécutez la commande suivante pour redémarrer le service du Serveur d'administration :

   `systemctl restart kladminserver_srv.service`

3. Téléchargez les modules supplémentaires « Fichiers pour l'installation à distance via Kaspersky Security Center » depuis le site Internet de Kaspersky.

   Les archives téléchargées portent les noms suivants :

   - ri_utils_win32.zip
   - ri_utils_arm64.zip

   Ne renommez pas les archives.

4. Placez les archives dans le répertoire /var/opt/kaspersky/klnagent_srv/1093/.working/ri_utils_archives.

Le Serveur d'administration dispose désormais des dépendances requises.

Installation de l'Agent 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.

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`
- `systemctl status kliam_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 :

- Installez le SGBD pour Kaspersky Security Center Linux. Vous pouvez choisir l'un des SGBD 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.

  Après avoir installé le SGBD, suivez les instructions correspondantes :

  - Configuration du serveur PostgreSQL ou Postgres Pro pour fonctionner avec Kaspersky Security Center Linux

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

    Si vous souhaitez que le Serveur d'administration détecte automatiquement les adresses des nœuds du cluster, il vous suffit d'indiquer le nom DNS ou l'adresse IP du nœud de contrôle ou du nœud de réplique lors de l'installation. Pour ce faire, assurez-vous d'avoir effectué l'étape 2 de la procédure Préparation d'un cluster de SGBD haute disponibilité pour une utilisation avec Kaspersky Security Center Linux.

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

    Configuration du compte SGBD pour travailler avec MySQL et MariaDB

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

    Configuration du compte SGBD pour travailler avec MySQL et MariaDB

- Assurez-vous que votre appareil sur lequel le SGBD est installé ne comporte pas de comptes utilisateurs SGBD portant les noms suivants :

  - client
  - iam
  - ksc
  - locker
  - pat
  - scope
  - voltron

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

  Si vous utilisez 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 du Serveur d'administration.

- Téléchargez le fichier d'installation dans la langue souhaitée depuis le site Internet de Kaspersky. Choisissez le fichier d'installation correspondant à la distribution Linux installée sur votre appareil : ksc64_[numéro_de_version]_amd64.deb ou ksc64-[numéro_de_version].x86_64.rpm.

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. Créez un groupe 'kladmins' et des comptes non privilégiés 'ksc', qui doivent être membres 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`

   `adduser ksciam`

   `gpasswd -a ksciam kladmins`

   `usermod -g kladmins ksciam`

3. Sur serveur SGBD, créez une base de données pour IAM. Le nom de la base de données doit être différent de celui de la base de données que vous avez installée pour fonctionner avec Kaspersky Security Center Linux. Le Serveur d'administration ne supprime pas automatiquement la base de données IAM lors de la désinstallation ou du déplacement du serveur vers un autre appareil. Vous devez supprimer la base de données manuellement.

   - Pour PostgreSQL, exécutez la commande suivante :

     ```
     sudo -i -u postgres psql -U postgres -c "CREATE DATABASE <iam_db_name>;"
     ```

   - Pour MariaDB, exécutez la commande suivante :

     ```
     sudo mysql -u root -p -e "CREATE DATABASE <iam_db_name>;"
     ```

4. Créez le fichier de réponses (au format TXT) et ajoutez-y une liste de variables au format `VARIABLE_NAME=variable_value`. Ajoutez chaque variable 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-get install /<path>/ksc64_[version_number]_amd64.deb -y
```

```
yum install /<path>/ksc64-[version_number].x86_64.rpm -y
```

   Dans l'environnement utilisateur :

```
sudo -E apt-get install /<path>/ksc64_[version_number]_amd64.deb -y
```

```
sudo -E yum install /<path>/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 à l'aide d'un compte disposant des privilèges root et indiquez un mot de passe d'au moins 8 caractères :

```
/opt/kaspersky/ksc64/sbin/kladduser -n kscadmin -p <password>
```

8. Installez Kaspersky Security Center Web Console.

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. Paramètre facultatif. La valeur par défaut est de 14000.	Numéro de port
KLSRV_UNATT_PORT_SRV_SSL	Non	Le numéro de port SSL du Serveur d'administration. Paramètre facultatif. La valeur par défaut est de 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. Paramètre facultatif. La valeur par défaut est de 13299.	Numéro de port
KLSRV_UNATT_PORT_GUI	Non	Le numéro du port pour travailler avec l'utilitaire klakaut. Paramètre facultatif. La valeur par défaut est de 13291. L'utilitaire klakaut et son système d'aide se trouvent dans le dossier d'installation de Kaspersky Security Center Linux. 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. Ce paramètre permet d'optimiser la charge du réseau. Paramètre facultatif. La valeur par défaut est de 1.	`1` pour 1 à 100 appareils administrés. `2` pour 101 à 1 000 appareils administrés. `3` pour plus de 1 000 appareils administrés.

`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 du serveur de base de données. Pour utiliser un cluster à haute disponibilité intégré PostgreSQL ou Postgres Pro ou un cluster de SGBD Platform V Pangolin, saisissez les noms DNS ou les adresses IP ainsi que les ports de tous les nœuds au format suivant : `<fqdn1>:<port>,<fqdn2>:<port>,<...> <fqdnX>:<port>;` Si vous souhaitez utiliser un cluster de SGBD Platform V Pangolin, vous pouvez également indiquer uniquement le nom DNS ou l'adresse IP du nœud principal ou du nœud de réplique lors de la définition de l'adresse du SGBD.	Nom DNS ou adresse IP statique du serveur de base de données.

`KLSRV_UNATT_DBMS_PORT`	Oui	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. Le nom de la base de données doit être différent du nom de la base de données IAM spécifié dans la variable `KLSRV_UNATT_DB_IAM_NAME`.	`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_IAM_ADDRESS`	Oui	Les navigateurs des utilisateurs seront redirigés vers cette adresse grâce à OpenIDConnect. Entrez le nom de domaine complet du serveur IAM. Vous devez utiliser le nom DNS du Serveur d'administration qui a été indiqué dans le paramètre `KLSRV_UNATT_SERVERADDRESS`.	FQDN
`KLSRV_UNATT_KLIAMUSER`	Oui	Nom du compte pour démarrer le service IAM. Le compte doit être membre du groupe de sécurité spécifié dans la variable `KLSRV_UNATT_KLADMINSGROUP`.	ksciam

`KLSRV_UNATT_DBMS_IAM_TYPE`	Oui	Le type de système de gestion de base de données IAM : MySQL (MariaDB) ou Postgres.	`mysql`
			ou
			`postgres`

`KLSRV_UNATT_DBMS_IAM_INSTANCE`	Oui	L'adresse du serveur de base de données IAM. Pour utiliser un cluster à haute disponibilité intégré PostgreSQL ou Postgres Pro ou un cluster de SGBD Platform V Pangolin, saisissez les noms DNS ou les adresses IP ainsi que les ports de tous les nœuds au format suivant : `<fqdn1>:<port>,<fqdn2>:<port>,<...> <fqdnX>:<port>;` Si vous souhaitez utiliser un cluster de SGBD Platform V Pangolin, vous pouvez également indiquer uniquement le nom DNS ou l'adresse IP du nœud principal ou du nœud de réplique lors de la définition de l'adresse du SGBD.	Adresse IP

KLSRV_UNATT_DBMS_IAM_PORT	Oui	Le port du serveur de base de données IAM. La valeur par défaut pour MySQL (MariaDB) est 3306 ; la valeur par défaut pour Postgres est 5432.	3306 ou 5432
KLSRV_UNATT_DBMS_IAM_LOGIN	Oui	Le nom d'utilisateur qui a accès à la base de données IAM. Si la base de données IAM est de type MySQL (MariaDB) et possède les deux paramètres suivants : • gtid_mode=ON • gtid_purged=ON|AUTO assurez-vous que l'utilisateur indiqué possède l'un des privilèges SGBD suivants : • RELOAD • FLUSH_TABLES	
KLSRV_UNATT_DBMS_IAM_PASSWORD	Oui	Le mot de passe de l'utilisateur ayant accès dans la base de données IAM.	
KLSRV_UNATT_DB_IAM_NAME	Oui	Nom de la base de données IAM. Le nom de la base de données IAM doit être différent du nom de la base de données spécifié dans la variable KLSRV_UNATT_DB_NAME. Spécifiez une base de données vide créée manuellement.	iamdb
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_EXT_RESOURCE_MANAGEMENT	Non	La configuration du cluster de basculement. Si le paramètre est omis dans le fichier de réponse, la valeur par défaut est utilisée. Valeurs possibles : 0 : Un cluster de basculement dont les nœuds sont situés dans un seul centre de données (valeur par défaut). 2 : Un cluster de basculement géo-distribué dont les nœuds sont situés dans différents centres de données.	0 ou 2
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

Si le Serveur d'administration n'a pas accès au dépôt des paquets de distribution des applications pour l'installation à distance, téléchargez les dépendances nécessaires à la création des paquets d'installation permettant d'installer des applications sur des appareils Windows comme suit :

1. Créez l'indicateur RIUtilsArchiveDirUsed en exécutant la commande suivante :

   ```
   /opt/kaspersky/ksc64/sbin/klscflag -fset -pv klserver -n RIUtilsArchiveDirUsed -t d -v 1
   ```

2. Exécutez la commande suivante pour redémarrer le service du Serveur d'administration :

   ```
   systemctl restart kladminserver_srv.service
   ```

3. Téléchargez les modules supplémentaires « Fichiers pour l'installation à distance via Kaspersky Security Center » depuis le site Internet de Kaspersky.

   Les archives téléchargées portent les noms suivants :

   - ri_utils_win32.zip
   - ri_utils_arm64.zip

   Ne renommez pas les archives.

4. Placez les archives dans le répertoire /var/opt/kaspersky/klnagent_srv/1093/.working/ri_utils_archives.

Le Serveur d'administration dispose désormais des dépendances requises.

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 :

- Installation d'un SGBD.
- Téléchargez la clé de l'application kaspersky_astra_pub_key.gpg.
- Téléchargez le fichier d'installation ksc64_[numéro_de_version]_amd64.deb à partir du site 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. Créez un groupe " kladmins " et des comptes sans privilèges " ksc " et " ksciam ". Les comptes doivent être membres du groupe " kladmins ". Pour ce faire, exécutez les commandes suivantes en séquence :

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

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

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

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

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

9. 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 du CLUF. 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 si 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.

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

    a. Saisissez le FQDN ou le nom DNS du Serveur d'administration.

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

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

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

- Si vous avez entre 1 et 100 appareils administrés, saisissez 1.
- Si vous avez entre 101 et 1 000 appareils administrés, saisissez 2.
- Si vous avez plus de 1 000 appareils administrés, saisissez 3.

Ce paramètre est utilisé pour retarder de manière automatiquement aléatoire le démarrage des tâches afin d'optimiser la charge du réseau. La liste ci-dessous indique l'intervalle dans lequel le décalage est calculé :

- De 1 à 100 appareils administrés, valeur 1. Le décalage n'est pas utilisé.
- De 101 à 1 000 appareils administrés, valeur 2. Le décalage est de 5 minutes.
- Plus de 1 000 appareils administrés, valeur 3. Le décalage est de 10 minutes.

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. 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.

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

j. 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

k. Saisissez le nom de la base de données.

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

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

n. Saisissez le FQDN ou le nom DNS du serveur IAM.

Saisissez la valeur que vous avez indiquée à l'étape 10a.

o. Saisissez le nom du compte pour lancer le service kliam. Le compte doit faire partie du groupe de sécurité saisi.

p. Sélectionnez le SGBD que vous avez installé et qui doit fonctionner avec le service IAM :

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

q. Saisissez l'adresse du SGBD que le service IAM va utiliser.

r. Saisissez le numéro de port de la base de données. Ce port sert à communiquer avec le service IAM. Par défaut, les ports suivants sont utilisés :

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

s. Saisissez le nom de la base de données que le service IAM va utiliser. Le nom de la base de données utilisée par le service IAM doit être différent de la base de données utilisée par le Serveur d'administration.

t. Saisissez l'identifiant de connexion du compte root de la base de données que vous utilisez pour accéder à la base de données IAM.

u. Saisissez le mot de passe du compte root de la base de données que vous utilisez pour accéder à la base de données IAM.

Attendez que les services soient ajoutés et lancés automatiquement :

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

v. 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 256 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.

Pour télécharger les dépendances nécessaires à la création de paquets d'installation d'applications pour les appareils Windows :

1. Créez l'indicateur RIUtilsArchiveDirUsed en exécutant la commande suivante :

   ```
   /opt/kaspersky/ksc64/sbin/klscflag -fset -pv klserver -n RIUtilsArchiveDirUsed -t d -v 1
   ```

2. Exécutez la commande suivante pour redémarrer le service du Serveur d'administration :

   ```
   systemctl restart kladminserver_srv.service
   ```

3. Téléchargez les modules supplémentaires « Fichiers pour l'installation à distance via Kaspersky Security Center » depuis le site Internet de Kaspersky.

   Les archives téléchargées portent les noms suivants :

   - ri_utils_win32.zip
   - ri_utils_arm64.zip

   Ne renommez pas les archives.

4. Placez les archives dans le répertoire /var/opt/kaspersky/klnagent_srv/1093/.working/ri_utils_archives.

Le Serveur d'administration dispose désormais des dépendances requises.

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`
- `# systemctl status kliam_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-<numéro de build>.x86_64.deb
- Pour les systèmes d'exploitation basés sur RPM : ksc-web-console-<numéro de build>.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. 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 : `/etc/ksc-web-console-setup.json`.

   Exemple de fichier de réponse contenant l'ensemble minimal de paramètres

   L'ensemble des paramètres du fichier de réponse dépend de la version du Serveur d'administration auquel Kaspersky Security Center Web Console se connecte :

   - Serveur d'administration 16 ou versions ultérieures

     Exemple de fichier de réponse avec l'ensemble minimal de paramètres pour se connecter au Serveur d'administration version 16 ou version ultérieure :

```
{
    "address": "ksc-web-console.example.com",
    "port": 8080,
    "trusted":  {
        "Administration Server v16": {
            "iamHost": "ksc16.example.com",
            "iamOAuthPort": 4444,
            "iamProxyPort": 9050,
            "iamCertPath": "/var/opt/kaspersky/klnagent_srv/iam/main_certificate.pem",
            "iamPATPath": "/var/opt/kaspersky/klnagent_srv/iam/initial_token.txt",
            "kscPort": 13299,
            "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
        }
    },
    "certDomain":"ksc-web-console.example.com",
    "acceptEula": true
}
```

- Serveur d'administration 15.4 ou versions ultérieures

  Exemple de fichier de réponse avec l'ensemble minimal de paramètres pour se connecter au Serveur d'administration version 15.4 ou version antérieure :

```
{
    "address": "ksc-web-console.example.com",
    "port": 8080,
    "trusted":  {
         "Administration Server v15.4": {
             "kscHost": "ksc.example.com",
             "kscPort": 13299,
             "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
         }
    },
    "certDomain":"ksc-web-console.example.com",
    "acceptEula": true
}
```

Vous pouvez installer Kaspersky Security Center Web Console soit sur le même appareil que le Serveur d'administration, soit sur un autre appareil. Si Kaspersky Security Center Web Console est installé sur un autre appareil, l'adresse de Kaspersky Security Center Web Console (définie par `address`) et l'adresse du Serveur d'administration (définie par `iamHost` ou `kscHost`) diffèrent. Si Kaspersky Security Center Web Console est installé sur le même appareil qui héberge le Serveur d'administration, ces paramètres ont les mêmes valeurs.

La valeur `iamHost` doit correspondre à l'adresse IAM spécifiée lors de l'installation du Serveur d'administration. Pour obtenir l'adresse IAM indiquée, exécutez la commande suivante sur l'appareil sur lequel le Serveur d'administration est installé :

```
grep "iam_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml
```

Pour en savoir plus, consultez l'article : [Paramètres d'installation de Kaspersky Security Center Web Console](#).

Vous pouvez ajouter plusieurs Serveurs d'administration de différentes versions à la liste des serveurs approuvés. Dans ce cas, les Serveurs peuvent utiliser différentes méthodes d'authentification.

Nous vous recommandons d'indiquer les numéros de port supérieurs à 1024. Si vous voulez que Kaspersky Security Center Web Console fonctionne sur les ports inférieurs à 1024, après l'installation, vous devez vous assurer que vous avez l'utilitaire setcap, puis exécutez la commande suivante :

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

Si vous ne disposez pas de l'utilitaire setcap, vous pouvez l'installer. **Cliquez sur ce lien pour voir les commandes**.

Pour les systèmes d'exploitation Debian et Ubuntu, exécutez l'une des commandes suivantes :

- `sudo apt-get install libcap2-bin`
- `sudo apt install libcap2-bin`

Pour SUSE Linux Enterprise Server et Red Hat Enterprise Linux, exécutez la commande suivante :

- `sudo zypper install libcap-progs`

Lorsque vous installez Kaspersky Security Center Web Console sur le système d'exploitation ALT Linux, 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 apt-get install ksc-web-console-<numéro de compilation>.x86_64.deb
     ```
   - Pour installer Kaspersky Security Center Web Console à partir d'un fichier .rpm, exécutez la commande suivante :
     ```
     sudo yum install ksc-web-console-<numéro de compilation>.x86_64.rpm
     ```
     ou
     ```
     sudo alien -i ksc-web-console-<numéro de build>.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 yum install ksc-web-console-<numéro de compilation>.x86_64.rpm
       ```
     - Pour les appareils exécutant un système d'exploitation basé sur Debian :
       ```
       sudo apt-get install ksc-web-console-<numéro de compilation>.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.

Si le certificat commun du Serveur d'administration est remplacé par un autre certificat provenant d'une sauvegarde ou à l'aide de l'utilitaire klsetsrvcert, vous devez supprimer, puis réinstaller Kaspersky Security Center Web Console. Dans le cas contraire, l'accès à Web Console sera restreint.
Si, après la réinstallation, vous ne parvenez pas à vous connecter à Web Console, vérifiez la configuration du Serveur IAM.

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. Vous devez nommer ce fichier ksc-web-console-setup.json et le placer dans le répertoire suivant : /etc/ksc-web-console-setup.json.

L'ensemble des paramètres du fichier de réponse dépend de la version du Serveur d'administration auquel Kaspersky Security Center Web Console se connecte.

- Serveur d'administration 16 ou versions ultérieures

  Le Serveur d'administration version 16 ou version ultérieure inclut le Gestionnaire des identités et des accès (IAM) qui permet l'authentification de domaine avec authentification unique (SSO) dans Kaspersky Security Center Web Console. Pour que Kaspersky Security Center Web Console puisse se connecter au Serveur d'administration, même si vous n'utilisez pas l'authentification unique, le fichier de réponse doit contenir les paramètres d'interaction avec le module IAM.

  Exemple de fichier de réponses pour l'installation de Web Console en vue d'une connexion au Serveur d'administration version 16 ou ultérieure. Dans cet exemple, Web Console et le Serveur d'administration sont installés sur des appareils différents :

```
{
    "address": "ksc-web-console.example.com",
    "port": 8080,
    "defaultLangId": 1049,
    "enableLog": true,
    "trusted":  {
        "Administration Server v16": {
    "iamHost": "ksc16.example.com",
    "iamOAuthPort": 4444,
    "iamProxyPort": 9050,
    "iamCertPath": "/var/opt/kaspersky/klnagent_srv/iam/main_certificate.pem",
    "iamPATPath": "/var/opt/kaspersky/klnagent_srv/iam/initial_token.txt",
    "kscPort": 13299,
    "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
        }
    },
    "acceptEula": true,
    "certPath": "/root/server.crt",
    "keyPath": "/root/key-without-passphrase.pem",
    "webConsoleAccount": "Group1:User1",
    "managementServiceAccount": "Group1:User2",
    "serviceWebConsoleAccount": "Group1:User3",
    "pluginAccount": "Group1:User4",
    "natsMessageQueueAccount": "Group1:User6"
}
```

- Serveur d'administration 15.4 ou versions ultérieures

  Le Serveur d'administration 15.4 et les versions antérieures prennent uniquement en charge l'authentification via la définition du nom et du mot de passe de l'utilisateur interne ou l'utilisateur du domaine.

  Exemple de fichier de réponses pour l'installation de Web Console en cas de connexion au Serveur d'administration 15.4 ou version antérieure :

```
{
    "address": "ksc-web-console.example.com",
    "port": 8080,
    "defaultLangId": 1049,
    "enableLog": true,
    "trusted":  {
        "Administration Server v15.4": {
    "kscHost": "ksc.example.com",
    "kscPort": 13299,
    "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
```

```
        }
    },
    "acceptEula": true,
    "certPath": "/root/server.crt",
    "keyPath": "/root/key-without-passphrase.pem",
    "webConsoleAccount": "Group1:User1",
    "managementServiceAccount": "Group1:User2",
    "serviceWebConsoleAccount": "Group1:User3",
    "pluginAccount": "Group1:User4",
    "natsMessageQueueAccount": "Group1:User6"
}
```

Les paramètres `webConsoleAccount`, `managementServiceAccount`, `serviceWebConsoleAccount`, `pluginAccount, natsMessageQueueAccount`, `certPath` et `keyPath` sont facultatifs. Vous pouvez omettre ces paramètres dans le fichier de réponses.

Si vous souhaitez utiliser un certificat personnalisé, spécifiez les paramètres `certPath` et `keyPath`. Si vous ne spécifiez aucun paramètre ou si vous n'en spécifiez qu'un seul, le navigateur Internet continue de vous indiquer que votre connexion n'est pas privée.

> Pour des raisons de sécurité, Mer vous déconseille de spécifier les paramètres `webConsoleAccount`, `managementServiceAccount`, `serviceWebConsoleAccount`, `pluginAccount` et `natsMessageQueueAccount`.
> Si vous décidez de spécifier ces paramètres, veillez à ce que les comptes utilisateurs que vous configurez 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.
> Les paramètres `webConsoleAccount`, `managementServiceAccount`, `serviceWebConsoleAccount`, `pluginAccount` et `natsMessageQueueAccount` ne doivent pas être utilisés séparément : spécifiez une valeur pour chacun d'entre eux ou pour aucun d'entre eux.

Vous pouvez installer Kaspersky Security Center Web Console soit sur le même appareil que le Serveur d'administration, soit sur un autre appareil. Si Kaspersky Security Center Web Console est installé sur un autre appareil, l'adresse de Kaspersky Security Center Web Console (définie par `address`) et l'adresse du Serveur d'administration (définie par `iamHost` ou `kscHost`) diffèrent. Si Kaspersky Security Center Web Console est installé sur le même appareil qui héberge le Serveur d'administration, ces paramètres ont les mêmes valeurs.

La valeur `iamHost` doit correspondre à l'adresse IAM spécifiée lors de l'installation du Serveur d'administration. Pour obtenir l'adresse IAM indiquée, exécutez la commande suivante sur l'appareil sur lequel le Serveur d'administration est installé :

```
grep "iam_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml
```

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
```

Si vous ne disposez pas de l'utilitaire setcap, vous pouvez l'installer. **Cliquez sur ce lien pour voir les commandes**.

Pour les systèmes d'exploitation Debian et Ubuntu, exécutez l'une des commandes suivantes :

- `sudo apt-get install libcap2-bin`
- `sudo apt install libcap2-bin`

Pour SUSE Linux Enterprise Server et Red Hat Enterprise Linux, exécutez la commande suivante :

- `sudo zypper install libcap-progs`

Lorsque vous installez Kaspersky Security Center Web Console sur le système d'exploitation ALT Linux, 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 l'appareil (FQDN ou nom d'hôte) sur lequel Kaspersky Security Center Web Console est installé (requis). Si vous installez Kaspersky Security Center Web Console sur le Serveur de Kaspersky Security Center, utilisez l'adresse que vous avez spécifiée lors de l'installation de Kaspersky Security Center Linux. Si vous installez Kaspersky Security Center Web Console sur un autre appareil, indiquez l'adresse de l'appareil (FQDN ou nom d'hôte) qui sera utilisée par le navigateur Internet pour se connecter à Kaspersky Security Center Web Console Server.	Valeur de chaîne. Exemple : `"ksc.example.com"`
`port`	Port utilisé par Kaspersky Security Center Web Console pour recevoir les connexions provenant des navigateurs Internet (requis).	Valeur numérique. La valeur recommandée est 8080 (sauf p d'exploitation ALT Linux).
`defaultLangId`	Langue de l'interface utilisateur (par défaut, `1033`). Si nécessaire, vous pouvez modifier la langue de l'interface de Kaspersky Security Center Web Console.	Code numérique de la langue : • Allemand : `1031` • Anglais : `1033` • Espagnol : `1034` • Espagnol (Mexique) : `2058` • Français : `1036` • Italien : `1040` • Japonais : `1041` • Kazakh : `1087` • Polonais : `1045` • Portugais (Brésil) : `1046` • Russe : `1049` • Turc : `1055` • Chinois simplifié : `2052` • Chinois traditionnel : `1028` Si aucune valeur n'est spécifiée, c'est l'ang est utilisé.
`enableLog`	Pour activer ou pas la journalisation des traces de Kaspersky Security Center Web Console. Nous vous recommandons de modifier la valeur par défaut du paramètre uniquement si un expert du support de Kaspersky vous le demande.	Valeur booléenne : • `true` : la journalisation est activée. • `false` : le journal est désactivé (séle défaut).

Paramètre	Description	Valeurs possibles

`trusted`	Liste des adresses des Serveurs d'administration de confiance auxquels Kaspersky Security Center Web Console peut se connecter. Vous pouvez ajouter plusieurs Serveurs d'administration de différentes versions à la liste des serveurs approuvés.
	
	Pour Serveur d'administration 16 ou versions ultérieures :
	
	• Le nom du Serveur d'administration qui s'affiche dans la fenêtre de connexion.
	• `iamHost` est l'adresse (FQDN ou nom d'hôte) du Serveur d'administration, qui comprend le module IAM (à partir de Kaspersky Security Center Linux version 16), et auquel se connecte Kaspersky Security Center Web Console.
	La valeur `iamHost` doit correspondre à l'adresse IAM spécifiée lors de l'installation du Serveur d'administration. Pour obtenir l'adresse IAM indiquée, exécutez la commande suivante sur l'appareil sur lequel le Serveur d'administration est installé : `grep "iam_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml`
	• `iamOAuthPort` est le port utilisé pour échanger les jetons d'authentification via le protocole d'authentification OpenID Connect (la valeur par défaut est 4444). Ce port est utilisé à la fois pour la communication entre Kaspersky Security Center Web Console Server et le Serveur d'administration, et entre le navigateur (utilisé avec Kaspersky Security Center Web Console) et le Serveur d'administration.
	• `iamProxyPort` est le port utilisé pour connecter Kaspersky Security Center Web Console Server au Serveur d'administration (la valeur par défaut est 9050).
	• `iamCertPath` est le chemin d'accès au certificat IAM. Le certificat IAM est créé automatiquement lors de la première exécution du Serveur d'administration. Le certificat se trouve sur l'appareil sur lequel le Serveur d'administration est installé. Le chemin par défaut vers le certificat : /var/opt/kaspersky/klnagent_srv/iam/main_certificate.pem. La rotation du certificat IAM auto-signé est effectuée automatiquement.
	• `iamPATPath` est le chemin d'accès au jeton utilisé pour l'enregistrement de Kaspersky Security Center Web Console en tant que client OAuth dans IAM. Ce fichier est généré automatiquement lors de la première exécution du Serveur d'administration. Le jeton se trouve sur l'appareil sur lequel le Serveur d'administration est installé. Le chemin par défaut vers le jeton : /var/opt/kaspersky/klnagent_srv/iam/initial_token.txt. Le jeton est valide indéfiniment et ne nécessite pas de rotation.
	• `kscPort` est le port utilisé pour connecter Kaspersky Security Center Web Console au Serveur d'administration via OpenAPI (la valeur par défaut est 13299).
	• `kscCertPath` est le chemin d'accès au certificat du Serveur d'administration. Le certificat se trouve sur l'appareil sur lequel le Serveur d'administration est installé. Chemin d'accès par défaut au fichier du certificat : /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer.
		La section du fichier JSON au format suiv
		
		`"trusted": {`
		`"Administration Server v16": {`
		`"iamHost": "ksc-iam.example.com",`
		`"iamOAuthPort": 4444,`
		`"iamProxyPort": 9050,`
		`"iamCertPath": "/var/opt/kaspersky/klnagent_srv/iam/main_c`
		`"iamPATPath": "/var/opt/kaspersky/klnagent_srv/iam/initia`
		`"kscPort": 13299,`
		`"kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/`
		`},`
		`"Administration Server v15.4": {`
		`"kscHost": "ksc.example.com",`
		`"kscPort": 13299,`
		`"kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/`
		`}`
		`}`
		
		Vous pouvez indiquer n'importe quel nom d'administration au lieu de `Administrat` `v16` et `Administration Server v15.`

Paramètre	Description	Valeurs possibles
	Pour Serveur d'administration 15.4 ou versions antérieures : • Le nom du Serveur d'administration qui s'affiche dans la fenêtre de connexion. • `kscHost` est l'adresse (FQDN ou nom de l'hôte) du Serveur d'administration auquel Kaspersky Security Center Web Console se connecte. • `kscPort` est le port OpenAPI utilisé pour connecter Kaspersky Security Center Web Console Server au Serveur d'administration (la valeur par défaut est 13299). • `kscCertPath` est le chemin d'accès au certificat du Serveur d'administration. Le certificat se trouve sur l'appareil sur lequel le Serveur d'administration est installé. Chemin d'accès par défaut au fichier du certificat : /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer. Lors de l'installation de Kaspersky Security Center Web Console sur un appareil autre que celui sur lequel est installé le Serveur d'administration, copiez le fichier du certificat du Serveur d'administration (spécifié par `kscCertPath`), le fichier du certificat IAM (spécifié par `iamCertPath`) et le fichier du jeton (spécifié par `iamPATPath`) depuis l'appareil avec le Serveur d'administration installé vers l'appareil cible. Spécifiez le chemin d'accès local à ces fichiers dans le fichier de réponses du programme d'installation de Web Console.	
`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 : • `true` : je confirme que j'ai entièreme Contrat de licence utilisateur final, qu comprends et que j'accepte toutes s • `false` : je n'accepte pas les conditio de licence (sélectionné par défaut). Si aucune valeur n'est indiquée, le progran d'installation de Kaspersky Security Cent Console affiche le CLUF et vous demand acceptez ou non les conditions du CLUF.
`certDomain`	Si vous souhaitez générer un nouveau certificat auto-signé, utilisez ce paramètre pour spécifier le FQDN pour la connexion du navigateur à Kaspersky Security Center Web Console.	Valeur de chaîne.
`certPath`	Utilisez ce paramètre pour spécifier le chemin d'accès au certificat personnalisé de Kaspersky Security Center Web Console qui est approuvé dans votre infrastructure et qui répond aux exigences relatives aux certificats personnalisés. Vous ne pouvez spécifier qu'une seule clé privée (`keyPath`) pour un certificat ou pour une chaîne de certificats.	Valeur de chaîne. Les certificats chiffrés ne sont pas pris e Kaspersky Security Center Web Console Sur l'appareil sur lequel Kaspersky Securit Console doit être installé, spécifiez le che fichier de certificat au format d'encodage Exemple : `/root/server.crt`
`keyPath`	Utilisez ce paramètre pour spécifier le chemin d'accès à la clé privée associée au certificat personnalisé de Kaspersky Security Center Web Console spécifié dans le paramètre `certPath`.	Valeur de chaîne. Le fichier avec la clé privée ne doit pas êt Sur l'appareil sur lequel Kaspersky Securit Console doit être installé, spécifiez le che fichier clé au format d'encodage PEM. Exemple : `/root/key-without-passph`
`webConsoleAccount`	Nom du compte à partir duquel le service Kaspersky Security Center Web Console est exécuté.	Valeur de chaîne au format suivant : `"< n groupe >:< nom d'utilisateur >"`. Exemple : `"Group1:User1"`. Si aucune valeur n'est indiquée, le progran d'installation de Kaspersky Security Cent Console crée un nouveau compte avec le défaut `user_management_%uid%`.

Paramètre	Description	Valeurs possibles
`managementServiceAccount`	Nom du compte à partir duquel le service d'administration de Kaspersky Security Center Web Console est exécuté.	Valeur de chaîne au format suivant : `"< n groupe >:< nom d'utilisateur >"`. Exemple : `"Group1:User2"`. Si aucune valeur n'est indiquée, le progran d'installation de Kaspersky Security Cent Console crée un nouveau compte avec le 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 : `"< n groupe >:< nom d'utilisateur >"`. Exemple : `"Group1:User3"`. Si aucune valeur n'est indiquée, le progran d'installation de Kaspersky Security Cent Console crée un nouveau compte avec le 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 : `"< n groupe >:< nom d'utilisateur >"`. Exemple : `"Group1:User4"`. Si aucune valeur n'est indiquée, le progran d'installation de Kaspersky Security Cent Console crée un nouveau compte avec le défaut `user_web_plugin_%uid%`.
`natsMessageQueueAccount`	Nom du compte à partir duquel le service Kaspersky Security Center Web Console NATS est exécuté.	Valeur de chaîne au format suivant : `"< n groupe >:< nom d'utilisateur >"`. Exemple : `"Group1:User6"`. Si aucune valeur n'est indiquée, le progran d'installation de Kaspersky Security Cent Console crée un nouveau compte avec le défaut `user_message_queue_%uid%`.

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. 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 : `/etc/ksc-web-console-setup.json`.

   Exemple de fichier de réponse contenant l'ensemble minimal de paramètres

L'ensemble des paramètres du fichier de réponse dépend de la version du Serveur d'administration auquel Kaspersky Security Center Web Console se connecte :

- Serveur d'administration 16 ou versions ultérieures

  Exemple de fichier de réponse avec l'ensemble minimal de paramètres pour se connecter au Serveur d'administration version 16 ou version ultérieure :

```
{
    "address": "ksc-web-console.example.com",
    "port": 8080,
    "trusted":  {
        "Administration Server v16": {
            "iamHost": "ksc16.example.com",
            "iamOAuthPort": 4444,
            "iamProxyPort": 9050,
            "iamCertPath": "/var/opt/kaspersky/klnagent_srv/iam/main_certificate.pem",
            "iamPATPath": "/var/opt/kaspersky/klnagent_srv/iam/initial_token.txt",
            "kscPort": 13299,
            "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
        }
    },
    "certDomain":"ksc-web-console.example.com",
    "acceptEula": true
}
```

- Serveur d'administration 15.4 ou versions ultérieures

  Exemple de fichier de réponse avec l'ensemble minimal de paramètres pour se connecter au Serveur d'administration version 15.4 ou version antérieure :

```
{
    "address": "ksc-web-console.example.com",
    "port": 8080,
    "trusted":  {
         "Administration Server v15.4": {
             "kscHost": "ksc.example.com",
             "kscPort": 13299,
             "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
         }
    },
    "certDomain":"ksc-web-console.example.com",
    "acceptEula": true
}
```

Vous pouvez installer Kaspersky Security Center Web Console soit sur le même appareil que le Serveur d'administration, soit sur un autre appareil. Si Kaspersky Security Center Web Console est installé sur un autre appareil, l'adresse de Kaspersky Security Center Web Console (définie par `address`) et l'adresse du Serveur d'administration (définie par `iamHost` ou `kscHost`) diffèrent. Si Kaspersky Security Center Web Console est installé sur le même appareil qui héberge le Serveur d'administration, ces paramètres ont les mêmes valeurs.

La valeur `iamHost` doit correspondre à l'adresse IAM spécifiée lors de l'installation du Serveur d'administration. Pour obtenir l'adresse IAM indiquée, exécutez la commande suivante sur l'appareil sur lequel le Serveur d'administration est installé :

```
grep "iam_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml
```

Pour en savoir plus, consultez l'article : [Paramètres d'installation de Kaspersky Security Center Web Console](#).

Vous pouvez ajouter plusieurs Serveurs d'administration de différentes versions à la liste des serveurs approuvés. Dans ce cas, les Serveurs peuvent utiliser différentes méthodes d'authentification.

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 Web de Kaspersky.

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

     ```
     sudo apt-get install ksc-web-console-<numéro_compilation>.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 apt-get install ksc-web-console-<numéro_compilation>.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.

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.

Le cluster de basculement Kaspersky Security Center Linux prend en charge deux configurations :

- Un cluster de basculement dont les nœuds sont situés dans un seul centre de données.
- Un cluster de basculement géo-distribué dont les nœuds sont situés dans différents centres de données.

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.

Utilisez la fonctionnalité syslog pour le dépannage.

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 s'est arrêté de manière inattendue. Les services Kaspersky Security Center Linux sont les suivants : klnagent_klfoc, kladminserver_klfoc, klactprx_klfoc, klwebsrv_klfoc.
- La connexion réseau entre le nœud actif et le stockage sur le serveur de fichiers a été interrompue ou coupée (uniquement pour le cluster situé dans un seul centre de données).

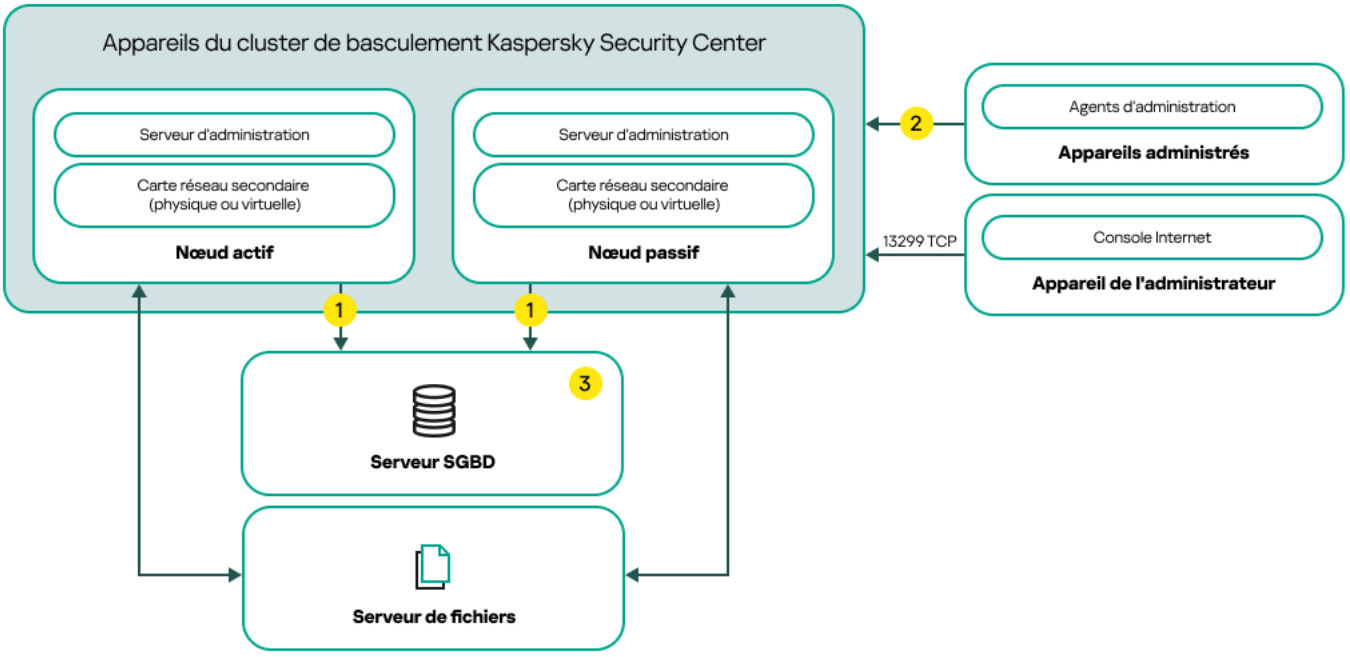
Cluster de basculement Kaspersky Security Center Linux. Schémas de déploiement

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

- Cluster de basculement Kaspersky Security Center Linux déployé au sein d'un seul centre de données :
  - Un système qui utilise une carte réseau secondaire et un SGBD installé sur un appareil dédié.
  - Un système qui utilise un équilibreur de charge tiers et un SGBD installé sur un appareil dédié.
- Cluster de basculement Kaspersky Security Center Linux, géo-distribué et déployé dans plusieurs centres de données.

Cluster de basculement Kaspersky Security Center Linux

Un système qui utilise une carte réseau secondaire et un SGBD installé sur un appareil dédié



Un système qui utilise une carte réseau secondaire et un SGBD installé sur un appareil dédié

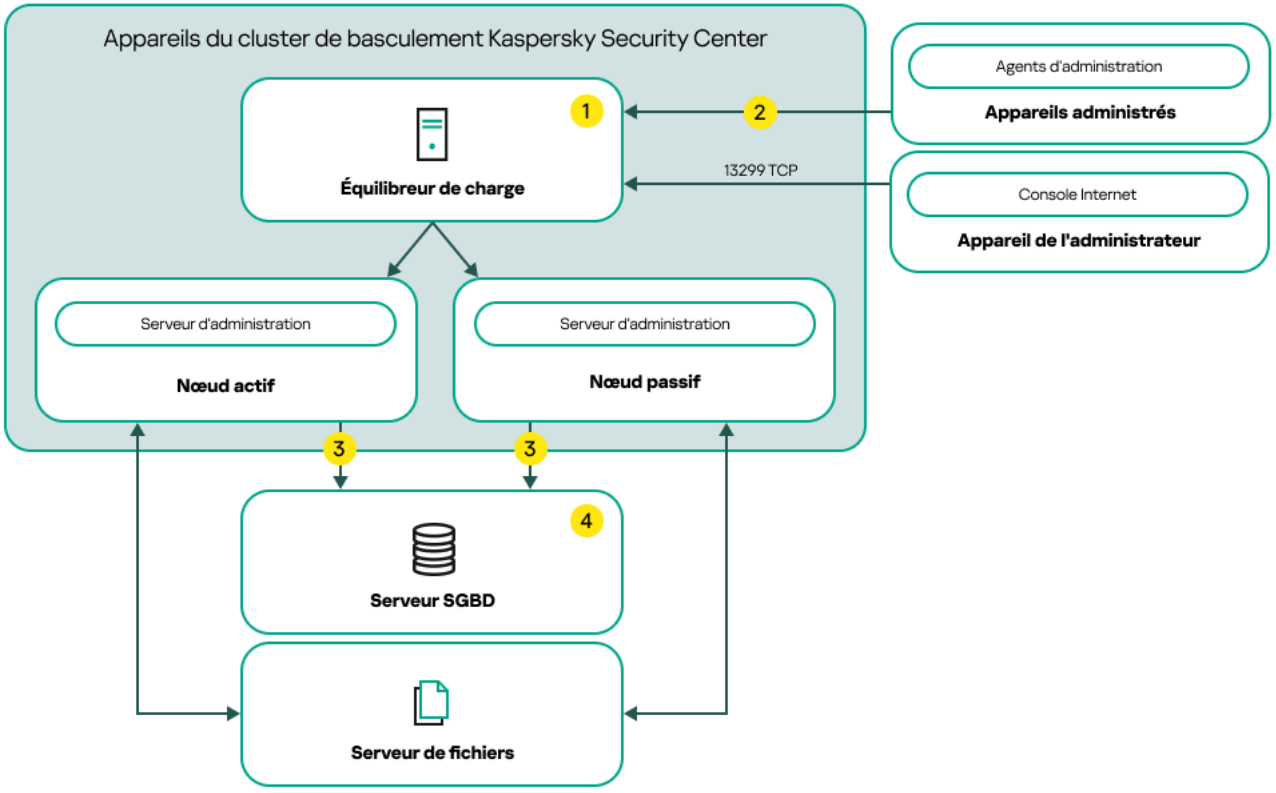
Légende du schéma :

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 Ouvrez les ports suivants sur les appareils équipés du Serveur d'administration pour vous connecter aux appareils gérés : 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 système qui utilise un équilibreur de charge tiers et un SGBD installé sur un appareil dédié



Un système qui utilise un équilibreur de charge tiers et un SGBD installé sur un appareil dédié

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 Ouvrez les ports suivants sur les appareils équipés du Serveur d'administration pour vous connecter aux appareils gérés : 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.

Cluster de basculement Kaspersky Security Center Linux géo-distribué

Ce schéma de déploiement vous permet d'assurer la haute disponibilité de tous les modules. Dans cette configuration, le Serveur d'administration, le SGBD et Kaspersky Security Center Web Console sont installés sur les deux nœuds du cluster.

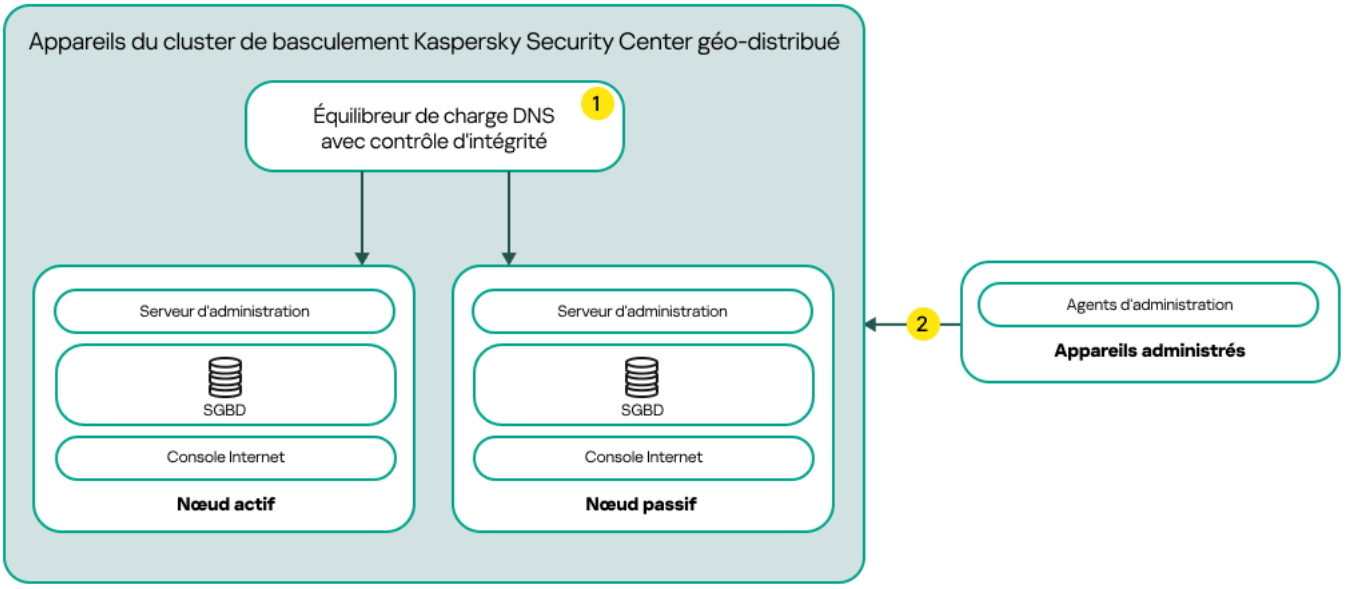


Schéma de déploiement du cluster de basculement Kaspersky Security Center Linux géo-distribué

1 Équilibreur de charge DNS avec contrôle d'intégrité, qui doit être déployé de votre côté avant l'installation du cluster de basculement Kaspersky Security Center Linux géo-distribué.

L'équilibreur de charge DNS vérifie régulièrement l'état des nœuds du cluster. Lorsque vous accédez au cluster via son nom de domaine, l'équilibreur de charge DNS renvoie toujours l'adresse IP du nœud actif.

2 Ouvrez les ports suivants sur les appareils équipés du Serveur d'administration pour vous connecter aux appareils gérés : TCP 13000, UDP 13000 et TCP 17000.

Cluster de basculement Kaspersky Security Center Linux

Cette section contient des informations générales sur le cluster de basculement Kaspersky Security Center Linux déployé au sein d'un seul centre de données, ainsi que des instructions pour la préparation et le 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.

Le déploiement des applications Kaspersky se déroule par étapes :

> Il est recommandé de suivre la séquence des étapes décrites dans ce scénario.

1. **Vérification de la configuration matérielle requise**

   Assurez-vous que vous disposez d'un matériel conforme aux conditions requises pour le cluster de basculement.

2. **Choisir le schéma de déploiement**

   Choisissez le schéma de déploiement. Cette opération a une incidence sur les étapes suivantes du déploiement.

3. **Préparation des comptes utilisateurs pour les services de Kaspersky Security Center Linux**

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

   1. Créez un groupe `kladmins`. Exécutez les commande suivantes :

      `sudo groupadd kladmins`

      `sudo groupmod -g <nouveau_GUID> kladmins`

      Assurez-vous que le groupe a le même GID sur les trois appareils. Exécutez la commande suivante :

      `getent group kladmins`

      Si le GID est différent, vous pouvez utiliser la commande suivante pour spécifier le GID :

      `sudo groupmod -g <nouveau_GUID> kladmins`

   2. Créez un compte utilisateur `ksc`. Attribuez des comptes utilisateurs au groupe `kladmins`. Exécutez les commande suivantes :

      `sudo adduser ksc`

      `sudo usermod -u <nouveau_UID> ksc`

      `sudo gpasswd -a ksc kladmins`

      `sudo usermod -g kladmins ksc`

      Assurez-vous que le compte utilisateur a le même identifiant unique (UID) sur les trois appareils. Exécutez la commande suivante :

      `getent passwd ksc`

      Si l'UID est différent, vous pouvez utiliser la commande suivante pour spécifier l'UID :

      `sudo usermod -u <nouveau_UID> ksc`

   3. Créez un compte utilisateur `rightless`. Attribuez des comptes utilisateurs au groupe `kladmins`. Exécutez les commande suivantes :

`sudo adduser rightless`

`sudo usermod -u <nouveau_UID> rightless`

`sudo gpasswd -a rightless kladmins`

`sudo usermod -g kladmins rightless`

Assurez-vous que le compte utilisateur a le même identifiant unique (UID) sur les trois appareils. Exécutez la commande suivante :

`getent passwd rightless`

Si l'UID est différent, vous pouvez utiliser la commande suivante pour spécifier l'UID :

`sudo usermod -u <nouveau_GUID> rightless`

4. Créez un compte utilisateur `ksciam`. Attribuez des comptes utilisateurs au groupe `kladmins`. Exécutez les commande suivantes :

   `sudo adduser ksciam`

   `sudo usermod -u <nouveau_UID> ksciam`

   `sudo gpasswd -a ksciam kladmins`

   `sudo usermod -g kladmins ksciam`

   Assurez-vous que le compte utilisateur a le même identifiant unique (UID) sur les trois appareils. Exécutez la commande suivante :

   `getent passwd ksciam`

   Si l'UID est différent, vous pouvez utiliser la commande suivante pour spécifier l'UID :

   `sudo usermod -u <nouveau_UID> ksciam`

5. Si nécessaire, augmentez la limite par défaut des fichiers pouvant être ouverts (descripteurs de fichiers) pour les comptes utilisés pour la fonction des services de Kaspersky Security Center Linux. 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 <nombre_maximum_de_fichiers_ouverts>`

   `ksc hard nofile <nombre_maximum_de_fichiers_ouverts>`

   Par défaut, les limites des descripteurs de fichiers sont spécifiées lors de l'installation. La limite des fichiers souples est de 32 768 fichiers, la limite des fichiers fixes est de 131 072 fichiers.

4 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

5 Installation du SGBD

Installez le SGBD pour Kaspersky Security Center Linux. Vous pouvez choisir l'un des SGBD 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.

Après avoir installé le SGBD, suivez les instructions correspondantes :

- Configuration du serveur PostgreSQL ou Postgres Pro pour fonctionner avec Kaspersky Security Center Linux
- Configuration du serveur MariaDB x64 pour fonctionner avec Kaspersky Security Center Linux

Créez manuellement une base de données pour IAM. Le Serveur d'administration ne supprime pas automatiquement la base de données IAM lors de la désinstallation ou du déplacement du serveur vers un autre appareil. Vous devez supprimer la base de données manuellement.

- Pour PostgreSQL, exécutez la commande suivante :

  `sudo -i -u postgres psql -U postgres -c "CREATE DATABASE <iam_db_name>;"`

- Pour MariaDB, exécutez la commande suivante :

  `sudo mysql -u root -p -e "CREATE DATABASE <iam_db_name>;"`

Sur l'appareil sur lequel le SGBD est installé, configurez la connexion aux appareils qui fonctionneront comme nœuds actifs et passifs.

6. **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

7. **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 l'appareil que vous souhaitez utiliser comme nœud actif, puis l'installer sur le nœud passif.

   Instructions pratiques : Installation de Kaspersky Security Center Linux sur les nœuds du cluster de basculement Kaspersky Security Center Linux.

8. **Installation de Kaspersky Security Center Web Console**

   Installez Kaspersky Security Center Web Console sur un appareil distinct qui n'est pas un nœud de cluster.

   Spécifiez le cluster de basculement comme adresse du Serveur d'administration dans le fichier de réponse.

   Le certificat du Serveur d'administration se trouve à l'emplacement suivant : /mnt/KlFocDataShare_klfoc/1093/cert/klserver.cer

   Copiez le fichier de certificat sur l'appareil sur lequel Kaspersky Security Center Web Console est en cours d'installation. Spécifiez le chemin d'accès local au certificat dans le fichier de réponse.

9. **Test du cluster de basculement**

   Vérifiez que vous avez correctement configuré le cluster de basculement et qu'il fonctionne correctement. Par exemple, vous pouvez exécuter la commande suivante pour lancer le basculement vers le nœud passif :

   `/opt/kaspersky/ksc64/sbin/klfoc -failover --stp klfoc`

   Utilisez la commande suivante pour vérifier que le service d'administration du cluster de basculement présente la valeur `Active: active (running)` sur les deux nœuds :

   `systemctl status klfocsvc_klfoc`

Utilisez les commandes suivantes pour vérifier que d'autres services du cluster de basculement présente la valeur `Active: active (running)` sur le nœud actif. Sur le nœud passif, les services du cluster de basculement doivent présenter la valeur `Active: inactive (dead)` ou `Active: failed (Result: signal)`.

- `systemctl status klnagent_klfoc`
- `systemctl status kladminserver_klfoc`
- `systemctl status klactprx_klfoc`
- `systemctl status klwebsrv_klfoc`

Le cluster de basculement Kaspersky Security Center Linux est déployé.

Cluster de basculement Kaspersky Security Center Linux. 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.

  Configuration des appareils qui agiront comme nœuds actifs et passifs

Matériel	Valeur
Processeur	16 noyaux, 2500 MHz
Mémoire vive	32 Go
Espace disque	500 Go, 300 IOPS ou plus
Contrôleur d'interface réseau	1 Gbit/s

  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.

- Un appareil sur lequel vous souhaitez installer la Web Console de Kaspersky Security Center Linux.

  Configuration de l'appareil pour 10 administrateurs système maximum

Matériel	Valeur
Processeur	2 noyaux, 2 500 MHz
Mémoire vive	4 Go
Espace disque	40 Go, 150 IOPS ou plus

  Configuration de l'appareil pour plus de 10 administrateurs système

Matériel	Valeur
Processeur	4 noyaux, 2500 MHz
Mémoire vive	8 Go
Espace disque	40 Go, 150 IOPS ou plus

- Un serveur de fichiers qui prend en charge le protocole CIFS/SMB, version 2.0 ou ultérieure. Vous devez fournir un appareil dédié qui fera office de serveur de fichiers.

Configuration d'un serveur de fichiers

Matériel	Valeur
Processeur	16 noyaux, 2500 MHz
Mémoire vive	32 Go
Espace disque	500 Go, 500 IOPS ou plus
Contrôleur d'interface réseau	10 Gbit/s

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

- 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.

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

   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
   ```

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.

   Assurez-vous que les dossiers suivants n'existent pas :

   - `/mnt/KlFocStateShare`

   - `/mnt/KlFocDataShare_klfoc`

   Si l'un de ces dossiers existe, supprimez-le de manière récursive.

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 770 /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 systemctl start nfs-server
```

Activez le démarrage automatique en exécutant la commande suivante :

```
sudo systemctl enable rpcbind
```

Vous pouvez spécifier des dossiers personnalisés, mais nous vous recommandons d'utiliser les noms de dossiers suggérés pour faciliter l'utilisation de l'aide en ligne.

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

Avant de continuer, assurez-vous d'avoir terminé les étapes précédentes du Scénario : Déploiement du cluster de basculement Kaspersky.

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

Configuration des dossiers communs

Pour configurer les dossiers communs :

1. 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 :

```
yum install nfs-utils
```

```
apt install nfs-kernel-server
```

2. Créez des points de montage en exécutant les commandes suivantes :

```
mkdir -p /mnt/KlFocStateShare
```

```
mkdir -p /mnt/KlFocDataShare_klfoc
```

3. Faites correspondre les points de montage et les dossiers partagés :

`sudo sh -c "echo <serveur de fichier>:/mnt/KlFocStateShare /mnt/KlFocStateShare nfs vers=4,soft,timeo=50,retrans=2,auto,user,rw 0 0 >> /etc/fstab"`

`sudo sh -c "echo <serveur de fichier>:/mnt/KlFocDataShare_klfoc /mnt/KlFocDataShare_klfoc nfs vers=4,noauto,user,rw,exec 0 0 >> /etc/fstab"`

Ici, `{serveur de fichier}` est le nom de domaine complet du serveur de fichiers contenant les dossiers partagés.

4. Montez les dossiers partagés en exécutant les commandes suivantes :

   `mount /mnt/KlFocStateShare`

   `mount /mnt/KlFocDataShare_klfoc`

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

   Exécutez la commande suivante :

   `ls -la /mnt/`

Configuration des cartes réseau

Une carte réseau secondaire peut être physique ou virtuelle. Si vous avez choisi un schéma de déploiement avec une carte réseau secondaire, effectuez la procédure correspondante sur les deux nœuds :

- Utilisez une carte réseau secondaire virtuelle basée sur une carte réseau physique (technologie MACVLAN) :

  1. Installez le paquet iputils-arping. En fonction de votre distribution Linux, exécutez l'une des commandes suivantes :

     - `yum install iputils`

     ou

     - `apt install iputils-arping`

  2. Pour vous assurer que NetworkManager est utilisé pour gérer la carte réseau physique, exécutez la commande suivante :

     `nmcli device status`

     Si la sortie de la commande indique que la carte réseau physique n'est pas gérée, configurez NetworkManager pour gérer la carte réseau physique. Les étapes de configuration exactes dépendent de votre distribution Linux.

  3. Pour identifier les interfaces, utilisez la commande suivante :

     `ip a`

  4. Pour créer un profil de configuration, exécutez la commande suivante :

     `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 secondaire physique ou créez un appareil TAP virtuel à l'aide d'un hyperviseur. Dans ce scénario, désactivez le logiciel NetworkManager.

  1. Connectez la carte réseau secondaire à un nœud.

  2. Installez le paquet iputils-arping. En fonction de votre distribution Linux, exécutez l'une des commandes suivantes :

     - `yum install iputils`

     ou

     - `apt install iputils-arping`

  3. Pour supprimer la connexion NetworkManager pour l'interface cible, exécutez la commande suivante :

     `nmcli con del <nom de la connexion>`

     Pour vérifier la connexion à l'interface cible, exécutez la commande suivante :

     `nmcli con show`

  4. Modifiez le fichier NetworkManager.conf. Recherchez la section du fichier clé et affectez l'interface cible au paramètre `unmanaged-devices` :

     `[keyfile]`

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

  5. Relancez le NetworkManager :

     `systemctl reload NetworkManager`

     Pour vous assurer que l'interface cible n'est plus administrée, exécutez la commande suivante :

     `nmcli dev status`

Configuration de l'équilibreur de charge

Si vous avez choisi un schéma de déploiement avec un équilibreur de charge, suivez les instructions ci-dessous pour le configurer.

Pour configurer l'équilibreur de charge, procédez comme suit :

1. Préparez un appareil Linux dédié sur lequel nginx ou un autre équilibreur de charge est installé.

2. Configurez le répartiteur de charge. Définissez le nœud actif comme serveur principal et le nœud passif comme serveur de sauvegarde.

3. Sur le serveur nginx, ouvrez tous les ports du Serveur d'administration de Kaspersky Security Center conformément à l'article suivant : Ports utilisés par Kaspersky Security Center Linux.

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

> La disponibilité des nœuds du cluster de basculement doit être déterminée par la disponibilité des principaux ports de connexion au Serveur d'administration. Le nœud passif n'accepte aucune connexion externe jusqu'à ce qu'un changement se produise.

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

Avant de continuer, assurez-vous d'avoir terminé les étapes précédentes du Scénario : Déploiement du cluster de basculement Kaspersky.

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.

En fonction de la distribution Linux installée sur votre appareil, vous devez utiliser l'un des fichiers d'installation suivants :

- ksc64_[numéro_version]_amd64.deb
- ksc64-[numéro_version].x86_64.rpm

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

Si vous utilisez RED OS version 7.3.4 ou une version ultérieure, ou MSVSPHERE version 9.2 ou une version ultérieure, vous devez installer le paquet libxcrypt-compat sur les deux nœuds.

Installation sur le nœud actif

Pour installer Kaspersky Security Center Linux sur le nœud actif :

1. Assurez-vous que l'appareil sur lequel vous voulez installer Kaspersky Security Center Linux fonctionne sur une des distributions Linux supportées.
2. Si vous utilisez une carte réseau secondaire, saisissez son nom lorsque vous y êtes invité. Vous pouvez saisir la commande suivante pour afficher toutes les interfaces réseau :

   ```
   ip addr
   ```

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-get install /<path>/ksc64_<numéro_version>_amd64.deb`
   - `sudo yum install /<path>/ksc64-<numéro_version>.x86_64.rpm`

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

   `/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 du CLUF. 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 si 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, indiquez les paramètres suivants :

   a. Saisissez le chemin d'accès local au point de montage du partage d'état : `/mnt/KlFocStateShare`

   b. Saisissez le chemin d'accès local au point de montage du partage de données : `/mnt/KlFocDataShare_klfoc`

   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. Saisissez le FQDN ou le nom DNS de la carte réseau secondaire, ou le FQDN ou le nom DNS de l'équilibreur de charge externe.

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

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

      - Si vous avez entre 1 et 100 appareils administrés, saisissez 1.
      - Si vous avez entre 101 et 1 000 appareils administrés, saisissez 2.
      - Si vous avez plus de 1 000 appareils administrés, saisissez 3.

      Ce paramètre est utilisé pour retarder de manière automatiquement aléatoire le démarrage des tâches afin d'optimiser la charge du réseau. La liste ci-dessous indique l'intervalle dans lequel le décalage est calculé :

      - De 1 à 100 appareils administrés, valeur 1. Le décalage n'est pas utilisé.
      - De 101 à 1 000 appareils administrés, valeur 2. Le décalage est de 5 minutes.
      - Plus de 1 000 appareils administrés, valeur 3. Le décalage est de 10 minutes.

   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 administrateur de la base de données que vous utilisez pour accéder à la base de données.

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

q. Saisissez le FQDN ou le nom DNS du serveur IAM.

Saisissez la valeur que vous avez indiquée à l'étape 7e.

r. Saisissez le nom du compte pour lancer le service IAM. Le compte doit faire partie du groupe de sécurité saisi. Par défaut, le compte ksciam est utilisé.

s. Sélectionnez le SGBD que vous avez installé et qui doit fonctionner avec le service IAM :

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

t. Saisissez l'adresse du SGBD IAM qui sera utilisé par le service IAM.

u. Saisissez le numéro de port du SGBD IAM. Ce port sert à communiquer avec le service IAM. Par défaut, les ports suivants sont utilisés :

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

v. Saisissez le nom de la base de données IAM qui sera utilisée par le service IAM. Le nom de la base de données utilisée par le service IAM doit être différent de la base de données utilisée par le Serveur d'administration.

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

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

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

- klfocsvc_klfoc
- kladminserver_klfoc
- klwebsrv_klfoc
- klactprx_klfoc
- klnagent_klfoc
- kliam_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 256 caractères.

   Si vous ignorez cette étape, vous pouvez créer le compte ultérieurement en exécutant la commande suivante :

   ```
   /opt/kaspersky/ksc64/sbin/kladduser -n kscadmin -p <mot de passe>
   ```

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

   - `sudo apt-get install /<path>/ksc64_<numéro_version>_amd64.deb`
   - `sudo yum install /<path>/ksc64-<numéro_version>.x86_64.rpm`

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

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

4. 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 du CLUF. 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 si 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.

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

6. Lorsque vous y êtes invité, saisissez le chemin d'accès local au point de montage du partage d'état : `/mnt/KlFocStateShare`

Kaspersky Security Center Linux est installé sur le nœud secondaire.

Vérification du service

Utilisez la commande suivante pour vérifier que le service d'administration du cluster de basculement présente l'état `Active: active (running)` :

```
systemctl status klfocsvc_klfoc
```

Utilisez les commandes suivantes pour vérifier que les autres services du cluster de basculement à l'état `Active: inactive (dead)` :

- `systemctl status klnagent_klfoc`
- `systemctl status kladminserver_klfoc`
- `systemctl status klactprx_klfoc`
- `systemctl status klwebsrv_klfoc`
- `systemctl status kliam_klfoc`

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 :

Sur le nœud actif, exécutez l'une des commandes suivantes :

- Pour arrêter le cluster, exécutez la commande suivante : `/opt/kaspersky/ksc64/sbin/klfoc -stopcluster --stp klfoc`
- Pour démarrer le cluster, exécutez la commande suivante : `/opt/kaspersky/ksc64/sbin/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`.
10. Pour vous assurer que le nœud actuel est actif, exécutez les commandes suivantes pour vérifier si les services sont exécutés :

    `systemctl status klnagent_klfoc.service`

    `systemctl status kladminserver_klfoc.service`

    `systemctl status klactprx_klfoc.service`

    `systemctl status klwebsrv_klfoc.service`

`systemctl status kliam_klfoc.service`

Ces services sont exécutés sur le nœud actif et non sur le nœud passif.

Le nœud est entretenu et attaché au cluster de basculement.

Réinstallation d'un nœud de cluster de basculement

Pour réinstaller un nœud de cluster de basculement, procédez comme suit :

1. Créez une copie de sauvegarde du Serveur d'administration.
2. Passez le nœud actif en mode maintenance.
3. S'il est nécessaire de conserver le système d'exploitation actuel, procédez comme suit.

   Si vous souhaitez remplacer l'appareil ou le système d'exploitation, ignorez cette étape.

   a. Pour arrêter le cluster de basculement, exécutez la commande suivante :

   `klfoc -stopcluster --stp klfoc`

   b. Pour arrêter de force les services du cluster de basculement, exécutez les commandes suivantes :

   `sudo systemctl stop klfocsvc_klfoc`

   `systemctl status kl*klfoc*`

   c. Pour démonter les répertoires du cluster de basculement, exécutez les commandes suivantes :

   `sudo umount /mnt/KlFocDataShare_klfoc`

   `sudo umount /mnt/KlFocStateShare`

   d. Pour désinstaller Kaspersky Security Center Linux, exécutez l'une des commandes suivantes en fonction de votre distribution Linux :

   - `sudo dpkg --remove ksc64`

   ou

   - `sudo yum remove ksc64`

   e. Effectuez toutes les étapes des instructions suivantes pour le nœud passif :

      1. Préparation des nœuds pour un cluster de basculement Kaspersky Security Center Linux.
      2. Installation de Kaspersky Security Center Linux sur les nœuds du cluster de basculement Kaspersky Security Center Linux.

4. Quittez le mode maintenance. Passez à l'étape 6 (arrêt du cluster de basculement) de l'instruction Démarrage et arrêt manuels des nœuds de cluster.

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.

> Kaspersky Security Center Web Console ne peut pas être installé sur des nœuds de cluster. Nous recommandons d'installer Kaspersky Security Center Web Console sur un serveur distinct.

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 `trusted` pour permettre à Kaspersky Security Center Web Console de se connecter au cluster de basculement de Kaspersky Security Center Linux.

   Composants du **paramètre d'installation** `trusted`

   Si vous vous connectez au cluster de basculement de Kaspersky Security Center Linux à l'aide de l'authentification de domaine avec l'authentification unique, précisez le paramètre d'installation approuvé comme suit : si vous connectez Kaspersky Security Center Web Console au Serveur d'administration version 16 ou ultérieure, l'authentification de domaine avec l'authentification unique (SSO) fournie par le Gestionnaire des identités et des accès (IAM) sera utilisée. Dans ce cas, précisez le paramètre d'installation `trusted` comme suit :

   ```
   "trusted":  {
     "<nom du Serveur d'administration>": {
       "iamHost": "ksc-iam.example.com",
       "iamOAuthPort": 4444,
       "iamProxyPort": 9050,
       "iamCertPath": "<dossier de données partagé>/iam/main_certificate.pem",
       "iamPATPath": "<dossier de données partagé>/iam/initial_token.txt",
       "kscPort": 13299,
       "kscCertPath": "<dossier de données partagé>/1093/cert/klserver.cer"
     }
   }
   ```

   où :

   - `<nom du Serveur d'administration>` est le nom du cluster de basculement Kaspersky Security Center Linux qui s'affichera dans la fenêtre de connexion de Kaspersky Security Center Web Console.

   - `iamHost` est l'adresse de l'appareil sur lequel le Serveur d'administration et IAM sont installés. Si vous avez créé la carte réseau virtuelle lors de la préparation des nœuds du cluster, utilisez le FQDN ou le nom d'hôte de la carte comme adresse du cluster de basculement Kaspersky Security Center Linux. Dans le cas contraire, indiquez le FQDN ou le nom d'hôte du répartiteur de charge tiers que vous utilisez.

     La valeur `iamHost` doit correspondre à l'adresse IAM spécifiée lors de l'installation du Serveur d'administration. Pour obtenir l'adresse IAM indiquée, exécutez la commande suivante sur l'appareil sur lequel le Serveur d'administration est installé :

```
grep "iam_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml
```

- `iamOAuthPort` est le port utilisé pour échanger les jetons d'authentification via le protocole d'authentification OpenID Connect (la valeur par défaut est 4444). Ce port est utilisé à la fois pour la communication entre Kaspersky Security Center Web Console Server et le Serveur d'administration, et entre le navigateur (utilisé avec Kaspersky Security Center Web Console) et le Serveur d'administration.

- `iamProxyPort` est le port utilisé pour connecter Kaspersky Security Center Web Console Server au Serveur d'administration (la valeur par défaut est 9050).

- `iamCertPath` est le chemin d'accès au certificat IAM. Le certificat IAM est créé automatiquement lors de la première exécution du Serveur d'administration. Le certificat se trouve sur l'appareil sur lequel le Serveur d'administration est installé. Le chemin par défaut vers le certificat est le suivant : `< dossier de données partagé >/iam/main_certificate.pem`. Le certificat se trouve dans le stockage de données partagé du cluster de basculement Kaspersky Security Center Linux. La rotation du certificat IAM auto-signé est effectuée automatiquement.

- `iamPATPath` est le chemin d'accès au jeton utilisé pour l'enregistrement de Kaspersky Security Center Web Console en tant que client OAuth dans IAM. Ce fichier est généré automatiquement lors de la première exécution du Serveur d'administration. Le jeton se trouve sur l'appareil sur lequel le Serveur d'administration est installé. Le chemin par défaut vers le jeton est le suivant : <dossier de données partagé>/iam/jeton_initial.txt. Le jeton se trouve dans le stockage de données partagé du cluster de basculement Kaspersky Security Center Linux. Le jeton est valide indéfiniment et ne nécessite pas de rotation.

- `kscPort` est le port OpenAPI utilisé par Kaspersky Security Center Web Console pour se connecter au Serveur d'administration (la valeur par défaut est 13299).

- `kscCertPath` est le certificat du Serveur d'administration qui 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 : `< dossier de données partagé >\1093\cert\klserver.cer`.

  Copiez le fichier de certificat du Serveur d'administration (spécifié par `kscCertPath`), le fichier de certificat IAM (spécifié par `iamCertPath`) et le fichier du jeton (spécifié par `iamPATPath`) depuis le stockage partagé des données sur l'appareil sur lequel vous installez Kaspersky Security Center Web Console. Indiquez le chemin d'accès local au certificat du Serveur d'administration.

Si vous connectez Kaspersky Security Center Web Console à la version 15.4 ou toute version antérieure du Serveur d'administration, l'authentification s'effectuera en précisant le nom et le mot de passe de l'utilisateur du domaine ou de l'utilisateur interne. Dans ce cas, précisez le paramètre d'installation de confiance comme suit :

```
"trusted":  {
  "<nom du Serveur d'administration>": {
    "kscHost": "ksc.example.com",
    "kscPort": 13299,
    "kscCertPath": "<dossier de données partagé>/1093/cert/klserver.cer"
  }
}
```

où :

- `< nom du Serveur d'administration >` est le nom du cluster de basculement Kaspersky Security Center Linux qui s'affichera dans la fenêtre de connexion de Kaspersky Security Center Web Console.
- `kscHost` est l'adresse du Serveur d'administration (FQDN ou nom d'hôte). Si vous avez créé la carte réseau virtuelle lors de la préparation des nœuds du cluster, utilisez l'adresse de la carte comme adresse du cluster de basculement Kaspersky Security Center Linux. Dans le cas contraire, indiquez l'adresse du répartiteur de charge tiers que vous utilisez.
- `kscPort` est le port OpenAPI utilisé par Kaspersky Security Center Web Console pour se connecter au Serveur d'administration (la valeur par défaut est 13299).
- `kscCertPath` est le certificat du Serveur d'administration qui 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 : `< dossier de données partagé >\1093\cert\klserver.cer`. Copiez le fichier de certificat du stockage de données partagé sur l'appareil sur lequel vous installez Kaspersky Security Center Web Console. Indiquez le chemin d'accès local au certificat du Serveur d'administration.

3. Continuez avec l'installation standard de Kaspersky Security Center Web Console.

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

Cluster de basculement Kaspersky Security Center Linux géo-distribué

Cette section contient des informations générales sur le cluster de basculement Kaspersky Security Center Linux géo-distribué, ainsi que des instructions pour la préparation et le déploiement de ce cluster de basculement géo-distribué au sein de votre réseau pour les configurations suivantes :

- Nœuds de cluster fonctionnant sous Ubuntu avec le SGBD PostgreSQL
- Nœuds de cluster fonctionnant sous SberLinux avec le SGBD Platform V Pangolin

Cluster géo-distribué fonctionnant sous Ubuntu avec le SGBD PostgreSQL

En suivant ce scénario, vous pouvez préparer votre infrastructure et déployer un cluster de basculement Kaspersky Security Center Linux géo-distribué.

Prérequis

- Déployez un équilibreur de charge DNS haute disponibilité avec contrôle d'intégrité.
- Assurez-vous que les nœuds actifs et passifs du cluster sont deux appareils dont les configurations matérielles et logicielles sont identiques.
  - Configuration matérielle :
    - Processeur : 16 noyaux, 2 500 MHz
    - RAM : 32 Go
    - Espace disque : 500 Go avec 300 IOPS ou plus
    - Contrôleur d'interface réseau : 1 Gbit/s
  - Configuration logicielle :
    - Système d'exploitation : Ubuntu Server 24.04 LTS (Noble Numbat) 64 bits
    - SGBD : PostgreSQL 17 64 bits

Étapes

Le cluster de basculement Kaspersky Security Center Linux déployé dans un seul centre de données ne peut pas être mis à niveau vers un cluster de basculement géo-distribué.

Le déploiement du cluster de basculement Kaspersky Security Center Linux géo-distribué se déroule par étapes :

1. **Préparation d'un système de fichiers pour les nœuds d'un cluster de basculement**

   Préparez le système de fichiers sur les deux nœuds du cluster. La préparation consiste à créer des volumes logiques LVM et à configurer des répertoires comme points de montage.

2. **Configuration d'un système de fichiers en cluster répliqué**

   Installez les utilitaires DRBD et configurez les ressources DRBD pour la réplication des données entre les nœuds du cluster de basculement. Ensuite, créez un système de fichiers répliqué sur le nœud actif du cluster.

3. **Installation et configuration de Corosync et Pacemaker sur les nœuds du cluster de basculement**

   Installez Corosync et Pacemaker afin d'assurer la communication au sein du cluster et la gestion des ressources pour garantir la haute disponibilité.

4. **Installation et configuration du SGBD PostgreSQL**

   Installez et configurez PostgreSQL sur les nœuds du cluster.

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

   Installez Kaspersky Security Center Linux sur les nœuds du cluster, puis configurez le chiffrement entre ces nœuds.

6. **Installation de Kaspersky Security Center Web Console sur les nœuds du cluster de basculement**

   Installez Kaspersky Security Center Web Console sur les deux nœuds du cluster de basculement afin d'assurer une haute disponibilité.

Préparation d'un système de fichiers pour les nœuds d'un cluster

Dans un premier temps, pour préparer le déploiement du cluster de basculement Kaspersky Security Center Linux géo-distribué, vous devez configurer le système de fichiers sur les deux nœuds du cluster. La préparation consiste à créer des volumes logiques LVM et à configurer des répertoires comme points de montage. Effectuez la procédure ci-dessous sur les deux nœuds du cluster.

Pour préparer un système de fichiers sur les nœuds du cluster, procédez comme suit :

1. Créez un volume logique LVM pour les données et la base de données du Serveur d'administration :

   ```
   lvcreate -L <volume size> -n klfocdata <volume group name>
   ```

   Créez un volume logique LVM distinct pour stocker le fichier de réponse :

   ```
   lvcreate -L <volume size> -n klfocstate <volume group name>
   ```

   où :

   - `volume group name` est le nom du groupe de volumes utilisé par LVM.
   - `klfocdata` et `klfocstate` sont des noms de volumes logiques. Ces volumes logiques sont créés au sein du groupe de volumes

     Nous vous recommandons d'utiliser ces noms de volume pour des raisons de cohérence, mais vous pouvez définir des noms personnalisés si nécessaire.
   - `volume size` la taille du volume. Nous vous recommandons de réserver au moins 500 Go pour les données et la base de données du Serveur d'administration. Le volume nécessaire au stockage du fichier de réponse est faible.

2. Créez des répertoires qui serviront de points de montage pour les volumes logiques.

   - Pour les données et la base de données du Serveur d'administration :

     ```
     mkdir -p /mnt/KlFocDataShare_klfoc
     ```

   - Pour le fichier de réponse :

     ```
     mkdir -p /mnt/KlFocStateShare_klfoc
     ```

Nous vous recommandons d'utiliser les répertoires `/mnt/KlFocDataShare_klfoc` et `/mnt/KlFocStateShare_klfoc` pour des raisons de cohérence, mais vous pouvez définir des noms personnalisés si nécessaire.

Le système de fichiers des nœuds du cluster est prêt. Ensuite, il faut configurer un système de fichiers en cluster répliqué.

Configuration d'un système de fichiers en cluster répliqué

Installation et configuration de DRBD

DRBD est un logiciel tiers utilisé pour la réplication des données (plus particulièrement pour les volumes de données et les points de montage créés à l'étape précédente).

Une fois que vous avez préparé le système de fichiers des nœuds du cluster, vous devez installer les utilitaires DRBD et configurer les ressources DRBD pour la réplication des données entre les nœuds du cluster. Effectuez la procédure ci-dessous sur les deux nœuds du cluster.

Pour installer et configurer DRBD sur les nœuds du cluster, procédez comme suit :

1. Installez les utilitaires DRBD :

   ```
   apt update
   apt install -y drbd-utils
   ```

   Nous vous recommandons d'utiliser la version 9.2.6 ou une version ultérieure de DRBD, car elle intègre un système de chiffrement du trafic.

   Le trafic DRBD peut également être chiffré à l'aide de votre propre solution VPN.

2. Créez des fichiers de configuration de ressources DRBD pour chaque volume logique créé lors de la préparation du système de fichiers (`klfocdata` et `klfocstate`).

   Tous les fichiers de configuration doivent être placés dans `/etc/drbd.d/`.

   - Ressource `klfocdata` (données et base de données du Serveur d'administration)

     Utilisez la réplication asynchrone (protocole A) pour la ressource klfocdata. Configurez tous les autres paramètres en fonction de votre environnement.

     Exemple de fichier de configuration :

     ```
     resource klfocdata {
         protocol A;
         net {
             after-sb-0pri    discard-least-changes;
             after-sb-1pri    call-pri-lost-after-sb;
             after-sb-2pri    call-pri-lost-after-sb;
         }
         syncer {
             rate 110M;
         }
         # Hostname of the active node
         on db1 {
             device    /dev/drbd0;
             disk      /dev/<volume group name>/klfocdata;
             address   <disk IP address>;
             meta-disk internal;
         }
         # Hostname of the passive node
         on db2 {
             device    /dev/drbd0;
             disk      /dev/<volume group name>/klfocdata;
             address   <disk IP address>;
             meta-disk internal;
     ```

```
    }
}
```

- Ressource `klfocstate` (le fichier de réponse)

  Utilisez la réplication synchrone (protocole C) pour créer la ressource klfocstate. Configurez tous les autres paramètres en fonction de votre environnement.

  Exemple de fichier de configuration :

```
resource klfocstate {
    protocol C;
    net {
        after-sb-0pri    discard-least-changes;
        after-sb-1pri    call-pri-lost-after-sb;
        after-sb-2pri    call-pri-lost-after-sb;
    }
    syncer {
        rate 110M;
    }
    # Hostname of the active node
    on db1 {
        device    /dev/drbd2;
        disk      /dev/<volume group name>/klfocstate;
        address   <disk IP address>;
        meta-disk internal;
    }
    # Hostname of the passive node
    on db2 {
        device    /dev/drbd2;
        disk      /dev/<volume group name>/klfocstate;
        address   <disk IP address>;
        meta-disk internal;
    }
}
```

3. Initialisez les métadonnées DRBD pour les deux ressources :

```
drbdadm create-md klfocdata
drbdadm create-md klfocstate
```

4. Démarrez toutes les ressources configurées avec DRBD :

```
drbdadm up all
```

DRBD est installé et configuré sur les deux nœuds du cluster.

Créez un système de fichiers répliqué sur le nœud actif du cluster

Une fois que vous avez installé et configuré DRBD sur les deux nœuds du cluster, créez un système de fichiers répliqué sur le nœud actif du cluster. Effectuez la procédure ci-dessous sur le nœud actif du cluster.

Pour créer un système de fichiers répliqué sur le nœud actif du cluster, procédez comme suit :

1. Mettez les deux ressources DRBD en rôle principal :

```
drbdadm primary --force klfocdata
drbdadm primary --force klfocstate
```

2. Formatez les appareils DRBD afin de préparer les volumes répliqués en vue de leur utilisation sur les nœuds du cluster :

```
mkfs.ext4 /dev/drbd0
mkfs.ext4 /dev/drbd2
```

3. Configurez les paramètres du système de fichiers :

```
tune2fs -m 0 /dev/drbd0
tune2fs -m 0 /dev/drbd2
```

4. Montez les appareils DRBD dans les répertoires créés précédemment :

```
mount -o noatime /dev/drbd0 /mnt/KlFocDataShare_klfoc
mount -o noatime /dev/drbd2 /mnt/KlFocStateShare_klfoc
```

   Si le service multipathd est installé, il doit être configuré pour ignorer les appareils `/dev/drbd*` sur les deux nœuds du cluster.

5. Vérifiez l'état de la réplication :

```
drbdadm status
```

   La sortie de la configuration correcte du système de fichiers :

```
klfocdata role:Secondary
disk:UpToDate open:no
db2 role:Primary tls:yes
peer-disk:UpToDate

klfocstate role:Secondary
disk:UpToDate open:no
db2 role:Primary tls:yes
peer-disk:UpToDate
```

Un système de fichiers répliqué est configuré sur le nœud actif du cluster. Vous devez ensuite installer et configurer Corosync et Pacemaker sur les nœuds du cluster.

Installation et configuration de Corosync et Pacemaker sur les nœuds du cluster

Corosync et Pacemaker assurent la communication au sein du cluster et la gestion des ressources pour garantir la haute disponibilité. Ils garantissent que les services sont automatiquement transférés vers un nœud opérationnel en cas de panne, minimisant ainsi les temps d'arrêt.

Pour installer et configurer Corosync et Pacemaker sur les nœuds du cluster, procédez comme suit :

1. Sur les deux nœuds du cluster, installez les paquets requis :

```
sudo apt install pacemaker -y
sudo apt install crmsh -y
sudo apt install resource-agent-extra -y
```

2. Configurez Corosync et Pacemaker sur les deux nœuds du cluster en suivant les instructions de la documentation officielle. Pour cela, il faut notamment activer le démarrage automatique, générer et distribuer la clé d'authentification, et configurer les autorisations d'accès au fichier authkey.

   Pour vous assurer que les paramètres sont corrects, exécutez la commande suivante sur l'un des nœuds du cluster :

```
crm status
```

   Le résultat attendu devrait afficher l'état du cluster et dresser la liste de tous les nœuds actifs, confirmant ainsi que Corosync fonctionne correctement et que les nœuds communiquent entre eux.

3. Sur les deux nœuds du cluster, configurez les paramètres de base du cluster Pacemaker :

```
crm configure property stonith-enabled="false"
crm configure property symmetric-cluster="false"
crm configure rsc_defaults resource-stickiness="110"
crm configure rsc_defaults migration-threshold=3
crm configure property no-quorum-policy=ignore
```

4. Sur les deux nœuds du cluster, désactivez le lancement des scripts administrés par Corosync :

```
systemctl disable drbd.service
```

5. Sur l'un des nœuds du cluster, créez les ressources basées sur DRBD dans Pacemaker.

   - Ressource DRBD pour klfocdata

     a. Créez une ressource de cluster pour le volume DRBD `klfocdata`, afin que le cluster puisse gérer son état et surveiller automatiquement son intégrité :

```
crm configure primitive drbd_klfocdata ocf:linbit:drbd params drbd_resource="klfocdata" \
op monitor interval="60s" op start interval="0" timeout="240s" op stop interval="0" \
timeout="240s" op monitor role=Master interval="10s" op monitor role=Slave interval="30s"
```

     b. Créer une ressource `ms_drbd_klfocdata` gérée par le cluster à partir de la ressource `drbd_klfocdata` créée :

```
crm configure ms ms_drbd_klfocdata drbd_klfocdata meta master-max="1" master-node-max="1" \
clone-max="2" clone-node-max="1" notify="true"
```

c. Créez un point de montage pour le volume DRBD `fs_klfocdata` en précisant l'appareil, le répertoire de destination, le type de système de fichiers et les options de montage :

```
crm configure primitive fs_klfocdata ocf:heartbeat:Filesystem params device="/dev/drbd0" \
directory="/mnt/KlFocDataShare_klfoc" fstype="ext4" options="data=journal"
```

- Ressource DRBD pour klfocstate

a. Créez une ressource de cluster pour le volume DRBD `klfocstate`, afin que le cluster puisse gérer son état et surveiller automatiquement son intégrité :

```
crm configure primitive drbd_klfocstate ocf:linbit:drbd params drbd_resource="klfocstate" \
op monitor interval="60s" op start interval="0" timeout="240s" op stop interval="0" \
timeout="240s" op monitor role=Master interval="10s" op monitor role=Slave interval="30s"
```

b. Créer une ressource ms_drbd_klfocstate gérée par le cluster à partir de la ressource `drbd_klfocstate` créée :

```
crm configure ms ms_drbd_klfocstate drbd_klfocstate meta master-max="1" master-node-max="1" \
clone-max="2" clone-node-max="1" notify="true"
```

c. Créez un point de montage pour le volume DRBD `fs_klfocstate` en précisant l'appareil, le répertoire de destination, le type de système de fichiers et les options de montage :

```
crm configure primitive fs_klfocstate ocf:heartbeat:Filesystem params device="/dev/drbd2" \
directory="/mnt/KlFocStateShare_klfoc" fstype="ext4" options="noatime"
```

6. Définissez l'ordre de montage des ressources dont les DRBD sont à l'état Primary. Nommez cette ressource `cluster_resources` :

```
crm configure colocation cluster_resources inf: fs_klfocdata ms_drbd_klfocdata:Master ms_drbd_klfocstate:Master
```

7. Configurez le groupe de ressources et de services `group_klfoc` :

```
crm configure group group_klfoc fs_klfocdata fs_klfocstate
```

8. Configurez le groupe de ressources `group_klfoc` pour qu'il démarre après les ressources DRBD correspondantes. Attribuez le nom `all_after_drbd` à cette règle :

```
crm configure order all_after_drbd inf: ms_drbd_klfocdata:promote group_klfoc:start
```

9. Définissez la préférence de démarrage des ressources principales et secondaires : une priorité de 100 pour `node1` et de 50 pour `node2` :

```
crm configure location loc_klfocdata_one ms_drbd_klfocdata 100: db1 # hostname of the first cluster node
crm configure location loc_klfocdata_two ms_drbd_klfocdata 50: db2 # hostname of the second cluster node
crm configure location loc_klfocstate_one ms_drbd_klfocstate 100: db1 # hostname of the first cluster node
crm configure location loc_klfocstate_two ms_drbd_klfocstate 50: db2 # hostname of the second cluster node
crm configure location loc_group_one group_klfoc 100: db1 # hostname of the first cluster node
crm configure location loc_group_two group_klfoc 50: db2 # hostname of the second cluster node
```

10. Sur les deux nœuds du cluster, désactivez le lancement automatique du service DRBD :

```
systemctl disable drbd.service
```

Corosync et Pacemaker sont installés et configurés sur les nœuds du cluster. Ensuite, il faut installer le SGBD et créer la base de données du Serveur d'administration ainsi que la base de données IAM.

Installation et configuration du SGBD PostgreSQL

Une fois que vous avez installé et configuré Corosync et Pacemaker sur les nœuds du cluster, vous devez installer le SGBD sur les deux nœuds du cluster.

Pour installer et configurer le SGBD, procédez comme suit :

1. Sur les deux nœuds du cluster, installez PostgreSQL 17 x64 ou une version ultérieure.

   Pour en savoir plus sur l'installation de PostgreSQL, consultez sa documentation.

2. Assurez-vous que les nœuds du cluster sur lesquels le SGBD est installé ne contiennent pas de comptes utilisateurs SGBD portant les noms suivants :

   - client
   - iam
   - ksc
   - locker
   - pat
   - scope
   - voltron

3. Sur les deux nœuds du cluster, arrêtez le SGBD, puis désactivez le lancement automatique du service SGBD :

```
sudo systemctl stop postgresql
sudo systemctl disable postgresql
```

4. Sur le nœud actif du cluster, copiez le répertoire DBMS dans le répertoire `/mnt/KlFocDataShare_klfoc/dbms` :

```
rsync -av /var/lib/postgresql/17/main/ /mnt/KlFocDataShare_klfoc/dbms
mv /var/lib/postgresql/17/main /var/lib/postgresql/17/main.bk
```

5. Sur le nœud actif du cluster, copiez les fichiers de configuration de PostgreSQL dans le répertoire `/mnt/KlFocDataShare_klfoc/dbms` :

```
sudo cp /etc/postgresql/17/main/pg_hba.conf /mnt/KlFocDataShare_klfoc/dbms
sudo cp /etc/postgresql/17/main/pg_ident.conf /mnt/KlFocDataShare_klfoc/dbms
```

6. Sur les deux nœuds du cluster, ouvrez le fichier de configuration `/etc/postgresql/17/main/postgresql.conf`, puis définissez le répertoire `/mnt/KlFocDataShare_klfoc/dbms` en tant que répertoire des données de la base de données.

   Spécifiez également les chemins d'accès aux fichiers de configuration (`/mnt/KlFocDataShare_klfoc/dbms/pg_hba.conf` et `/mnt/KlFocDataShare_klfoc/dbms/pg_ident.conf`) et supprimez le paramètre `include_dir` :

```
data_directory = '/mnt/KlFocDataShare_klfoc/dbms'
hba_file = '/mnt/KlFocDataShare_klfoc/dbms/pg_hba.conf'
ident_file = '/mnt/KlFocDataShare_klfoc/dbms/pg_ident.conf'
listen_addresses = '*'
```

7. Dans le fichier de configuration `/etc/postgresql/17/main/postgresql.conf`, adaptez la configuration du SGBD à la configuration requise par Kaspersky Security Center Linux.

8. Créez et configurez des comptes pour travailler avec PostgreSQL.

9. Créez la ressource de service PostgreSQL :

```
crm configure primitive klfocsvc_dbms ocf:heartbeat:pgsql \
params pgctl="/usr/lib/postgresql/17/bin/pg_ctl" \
psql="/usr/bin/psql" \
pgdata="/mnt/KlFocDataShare_klfoc/dbms" \
config="/etc/postgresql/17/main/postgresql.conf" \
socketdir="/var/run/postgresql" \
op start timeout=60s \
op stop timeout=60s \
op monitor interval=30s timeout=60s
```

10. Ajoutez la ressource PostgreSQL au groupe de clusters `group_klfoc` :

```
crm configure edit group_klfoc
```

11. Ajoutez le nom de la ressource PostgreSQL `klfocsvc_dbms` à la fin de la liste, par exemple :

```
group group_klfoc {
...
klfocsvc_dbms
}
```

12. Sur le nœud actif du cluster, sur le serveur SGBD, créez une base de données pour IAM. Le nom de la base de données doit être différent de celui de la base de données que vous avez installée pour fonctionner avec Kaspersky Security Center Linux. Le Serveur d'administration ne supprime pas automatiquement la base de données IAM lors de la désinstallation ou du déplacement du serveur vers un autre appareil. Vous devez supprimer la base de données manuellement :

```
sudo -i -u postgres psql -U postgres -c "CREATE DATABASE <iam_db_name>;"
```

Le SGBD est installé et configuré. La base de données du Serveur d'administration et la base de données IAM sont créées. Ensuite, il faut installer Kaspersky Security Center Linux sur les nœuds du cluster.

Installation de Kaspersky Security Center Linux sur les nœuds d'un cluster de basculement géo-distribué

Kaspersky Security Center Linux est installé sur les nœuds du cluster de basculement géo-distribué à l'aide d'un fichier de réponse en mode silencieux, c'est-à-dire sans intervention de l'utilisateur. Le fichier de réponses contient un ensemble personnalisé de paramètres d'installation : les variables et leurs valeurs respectives.

Prérequis :

- Effectuez toutes les étapes préparatoires :
  - Préparation d'un système de fichiers pour les nœuds d'un cluster
  - Configuration d'un système de fichiers en cluster répliqué
  - Installation et configuration de Corosync et Pacemaker sur les nœuds du cluster
  - Installation et configuration du SGBD PostgreSQL
- Assurez-vous que les nœuds du cluster fonctionnent sous Ubuntu Server 24.04 LTS (Noble Numbat) x64.
- Téléchargez le fichier d'installation `ksc64_[version_number]_amd64.deb` à partir du site de Kaspersky.

Installation sur le nœud actif

Pour installer Kaspersky Security Center Linux sur le nœud actif 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. Créez un groupe `kladmins` et des comptes non privilégiés `ksc` et `ksciam`, qui doivent être membres 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
   adduser ksciam
   gpasswd -a ksciam kladmins
   usermod -g kladmins ksciam
   ```

3. Dans le répertoire `/mnt/KlFocDataShare_klfoc/`, créez le répertoire des fichiers Kaspersky Security Center Linux :

   ```
   mkdir /mnt/KlFocDataShare_klfoc/ksc/
   ```

4. Créez le fichier de réponses (au format TXT) et ajoutez-y une liste de variables au format VARIABLE_NAME=variable_value. Ajoutez chaque variable sur une ligne distincte.

   Dans la liste des paramètres utilisés pour l'installation de Kaspersky Security Center Linux en mode silencieux, indiquez les paramètres suivants, nécessaires au déploiement d'un cluster géo-distribué :

   - `KLFOC_UNATT_EXT_RESOURCE_MANAGEMENT=2`

     Définissez la valeur `2` pour déployer le cluster géo-distribué.

- `KLSRV_UNATT_SERVERADDRESS=<DNS balancer address>` et `KLSRV_UNATT_IAM_ADDRESS=<DNS balancer address>`

  L'équilibreur de charge DNS avec contrôle d'intégrité doit déjà être déployé. Les valeurs de ces paramètres doivent être identiques et correspondre au nom de domaine complet de l'équilibreur de charge DNS.

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. Lancez l'installation de Kaspersky Security Center Linux en mode silencieux à l'aide des commandes suivantes :

   - Dans l'environnement racine :

```
apt-get install /<path>/ksc64_[номер_версии]_amd64.deb -y
```

   - Dans l'environnement utilisateur :

```
sudo -E apt-get install /<path>/ksc64_[номер_версии]_amd64.deb -y
```

7. Désactivez le lancement automatique du service klfocsvc_klfoc.service :

```
systemctl disable klfocsvc_klfoc.service
```

8. Une fois que Kaspersky Security Center Linux est installé, arrêtez le nœud actif du cluster.

9. Déplacez toutes les ressources du cluster vers le nœud passif.

   Vous pouvez utiliser la commande `crm node standby` (et la réactiver avec `crm node online`).

Installation sur le nœud passif

Pour installer Kaspersky Security Center Linux sur le nœud passif :

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

```
sudo apt-get install /<path>/ksc64_<version_number>_amd64.deb
```

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

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

3. 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 :

   - Saisissez `y` si vous comprenez et acceptez les termes du CLUF. Saisissez `n` si vous n'acceptez pas les conditions du CLUF. Pour utiliser Kaspersky Security Center Linux, vous devez accepter les conditions du Contrat de licence utilisateur final.

   - Saisissez `y` si vous comprenez et acceptez les conditions de la Politique de confidentialité et si 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.

4. Sélectionnez le nœud de cluster passif comme mode d'installation du Serveur d'administration.

5. Lorsque vous y êtes invité, saisissez le chemin d'accès local au point de montage du partage d'état : `/mnt/KlFocStateShare_klfoc`.

6. Désactivez le lancement automatique du service klfocsvc_klfoc.service :

```
systemctl disable klfocsvc_klfoc.service
```

7. Créez la ressource de service `klfocsvc_klfoc` :

```
crm configure primitive klfocsvc_klfoc systemd:klfocsvc_klfoc \
op start timeout="900s" interval="0" \
op stop timeout="900s" interval="0" \
op monitor interval="30s" timeout="90s"
```

8. Ajoutez la ressource `klfocsvc_klfoc` au groupe `group_klfoc` :

```
crm configure edit group_klfoc
```

9. Ajoutez `klfocsvc_klfoc` à la fin de la ligne du groupe, par exemple :

```
group group_klfoc {
...
klfocsvc_klfoc
}
```

10. Vérifiez que toutes les ressources sont à l'état " démarré " sur le nœud actif.

```
crm status
```

Configuration du chiffrement entre les nœuds du cluster

Pour configurer le chiffrement entre les nœuds du cluster, procédez comme suit :

Si vous avez installé la version 9.2.6 ou une version ultérieure de DRBD lors de la configuration d'un système de fichiers en cluster répliqué, configurez le chiffrement entre les nœuds du cluster conformément à la documentation officielle de DRBD.

Vous pouvez également chiffrer le trafic entre les nœuds du cluster en utilisant votre propre solution VPN.

Le cluster de basculement Kaspersky Security Center Linux géo-distribué est installé. Ensuite, il faut installer Kaspersky Security Center Web Console sur les deux nœuds du cluster.

Cluster géo-distribué fonctionnant sous SberLinux avec le SGBD Platform V Pangolin

En suivant ce scénario, vous pouvez préparer votre infrastructure et déployer un cluster de basculement Kaspersky Security Center Linux géo-distribué.

Prérequis

- Déployez un équilibreur de charge DNS haute disponibilité avec contrôle d'intégrité.
- Assurez-vous que les nœuds actifs et passifs du cluster sont deux appareils dont les configurations matérielles et logicielles sont identiques.
  - Configuration matérielle :
    - Processeur : 16 noyaux, 2 500 MHz
    - RAM : 32 Go
    - Espace disque : 500 Go avec 300 IOPS ou plus
    - Contrôleur d'interface réseau : 1 Gbit/s
  - Configuration logicielle :
    - Système d'exploitation : Platform V SberLinux OS Server (SLO) 9.5.1 64 bits
    - DBMS : Platform V Pangolin 6.5.1 64 bits

Étapes

Le cluster de basculement Kaspersky Security Center Linux déployé dans un seul centre de données ne peut pas être mis à niveau vers un cluster de basculement géo-distribué.

Le déploiement du cluster de basculement Kaspersky Security Center Linux géo-distribué se déroule par étapes :

1. **Préparation d'un système de fichiers pour les nœuds d'un cluster de basculement**

   Préparez le système de fichiers sur les deux nœuds du cluster. La préparation consiste à créer des volumes logiques LVM et à configurer des répertoires comme points de montage.

2. **Configuration d'un système de fichiers en cluster répliqué**

   Installez les utilitaires DRBD et configurez les ressources DRBD pour la réplication des données entre les nœuds du cluster de basculement. Ensuite, créez un système de fichiers répliqué sur le nœud actif du cluster.

3. **Installation et configuration de Corosync et Pacemaker sur les nœuds du cluster de basculement**

   Installez Corosync et Pacemaker afin d'assurer la communication au sein du cluster et la gestion des ressources pour garantir la haute disponibilité.

4. **Installation et configuration du SGBD Platform V Pangolin**

   Installez et configurer Platform V Pangolin sur les nœuds du cluster.

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

   Installez Kaspersky Security Center Linux sur les nœuds du cluster, puis configurez le chiffrement entre ces nœuds.

6. **Installation de Kaspersky Security Center Web Console sur les nœuds du cluster de basculement**

   Installez Kaspersky Security Center Web Console sur les deux nœuds du cluster de basculement afin d'assurer une haute disponibilité.

Préparation d'un système de fichiers pour les nœuds d'un cluster

Dans un premier temps, pour préparer le déploiement du cluster de basculement Kaspersky Security Center Linux géo-distribué, vous devez configurer le système de fichiers sur les deux nœuds du cluster. La préparation consiste à créer des volumes logiques LVM et à configurer des répertoires comme points de montage. Effectuez la procédure ci-dessous sur les deux nœuds du cluster.

Pour préparer un système de fichiers sur les nœuds du cluster, procédez comme suit :

1. Créez un volume logique LVM pour les données et la base de données du Serveur d'administration :

   ```
   lvcreate -L <volume size> -n klfocdata <volume group name>
   ```

   Créez un volume logique LVM distinct pour stocker le fichier de réponse :

   ```
   lvcreate -L <volume size> -n klfocstate <volume group name>
   ```

où :

- `volume group name` est le nom du groupe de volumes utilisé par LVM.
- `klfocdata` et `klfocstate` sont des noms de volumes logiques. Ces volumes logiques sont créés au sein du groupe de volumes

  Nous vous recommandons d'utiliser ces noms de volume pour des raisons de cohérence, mais vous pouvez définir des noms personnalisés si nécessaire.
- `volume size` la taille du volume. Nous vous recommandons de réserver au moins 500 Go pour les données et la base de données du Serveur d'administration. Le volume nécessaire au stockage du fichier de réponse est faible.

2. Créez des répertoires qui serviront de points de montage pour les volumes logiques.

   - Pour les données et la base de données du Serveur d'administration :

     ```
     mkdir -p /mnt/KlFocDataShare_klfoc
     ```

   - Pour le fichier de réponse :

     ```
     mkdir -p /mnt/KlFocStateShare_klfoc
     ```

   Nous vous recommandons d'utiliser les répertoires `/mnt/KlFocDataShare_klfoc` et `/mnt/KlFocStateShare_klfoc` pour des raisons de cohérence, mais vous pouvez définir des noms personnalisés si nécessaire.

Le système de fichiers des nœuds du cluster est prêt. Ensuite, il faut configurer un système de fichiers en cluster répliqué.

Configuration d'un système de fichiers en cluster répliqué

Installation et configuration de DRBD

DRBD est un logiciel tiers utilisé pour la réplication des données (plus particulièrement pour les volumes de données et les points de montage créés à l'étape précédente).

Une fois que vous avez préparé le système de fichiers des nœuds du cluster, vous devez installer les utilitaires DRBD et configurer les ressources DRBD pour la réplication des données entre les nœuds du cluster. Effectuez la procédure ci-dessous sur les deux nœuds du cluster.

Pour installer et configurer DRBD sur les nœuds du cluster, procédez comme suit :

1. Installez les utilitaires DRBD comme suit :

   a. Activez les stockages EPEL et ELRepo sur les deux nœuds :

   ```
   dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
   dnf install https://www.elrepo.org/elrepo-release-9.el9.elrepo.noarch.rpm
   ```

b. Générez toutes les versions disponibles du paquet kmod-drbd9x et filtrez la liste des paquets compilés pour la plateforme el9_6 (par exemple, si vous utilisez Plateform V SberLinux OS Server (SLO) 9.6) :

```
dnf search --showduplicates kmod-drbd9x | grep el9_6
```

c. Installez la dernière version disponible figurant dans la liste sur les deux nœuds. Exemple pour Platform V SberLinux OS Server (SLO) 9.6 :

```
dnf install kmod-drbd9x-9.2.14-1.el9_6.elrepo.x86_64
dnf install drbd drbd-utils drbd-udev drbd-pacemaker drbd-selinux
modprobe drbd
```

Si une nouvelle version est disponible à l'avenir, remplacez la chaîne de version en conséquence.

Nous vous recommandons d'utiliser la version 9.2.6 ou une version ultérieure de DRBD, car elle intègre un système de chiffrement du trafic.

Le trafic DRBD peut également être chiffré à l'aide de votre propre solution VPN.

2. Créez des fichiers de configuration de ressources DRBD pour chaque volume logique créé lors de la préparation du système de fichiers (`klfocdata` et `klfocstate`).

   Tous les fichiers de configuration doivent être placés dans `/etc/drbd.d/`.

   - Ressource `klfocdata` (données et base de données du Serveur d'administration)

     Utilisez la réplication asynchrone (protocole A) pour la ressource klfocdata. Configurez tous les autres paramètres en fonction de votre environnement.

     Exemple de fichier de configuration :

```
resource klfocdata {
    protocol A;
    net {
        after-sb-0pri    discard-least-changes;
        after-sb-1pri    call-pri-lost-after-sb;
        after-sb-2pri    call-pri-lost-after-sb;
    }
    syncer {
        rate 110M;
    }
    # Hostname of the active node
    on db1 {
        device    /dev/drbd0;
        disk      /dev/<volume group name>/klfocdata;
        address   <disk IP address>;
        meta-disk internal;
    }
    # Hostname of the passive node
    on db2 {
        device    /dev/drbd0;
        disk      /dev/<volume group name>/klfocdata;
        address   <disk IP address>;
        meta-disk internal;
    }
}
```

   - Ressource `klfocstate` (le fichier de réponse)

     Utilisez la réplication synchrone (protocole C) pour créer la ressource klfocstate. Configurez tous les autres paramètres en fonction de votre environnement.

Exemple de fichier de configuration :

```
resource klfocstate {
    protocol C;
    net {
        after-sb-0pri    discard-least-changes;
        after-sb-1pri    call-pri-lost-after-sb;
        after-sb-2pri    call-pri-lost-after-sb;
    }
    syncer {
        rate 110M;
    }
    # Hostname of the active node
    on db1 {
        device    /dev/drbd2;
        disk      /dev/<volume group name>/klfocstate;
        address   <disk IP address>;
        meta-disk internal;
    }
    # Hostname of the passive node
    on db2 {
        device    /dev/drbd2;
        disk      /dev/<volume group name>/klfocstate;
        address   <disk IP address>;
        meta-disk internal;
    }
}
```

3. Initialisez les métadonnées DRBD pour les deux ressources :

```
drbdadm create-md klfocdata
drbdadm create-md klfocstate
```

4. Démarrez toutes les ressources configurées avec DRBD :

```
drbdadm up all
```

DRBD est installé et configuré sur les deux nœuds du cluster.

Créez un système de fichiers répliqué sur le nœud actif du cluster

Une fois que vous avez installé et configuré DRBD sur les deux nœuds du cluster, créez un système de fichiers répliqué sur le nœud actif du cluster. Effectuez la procédure ci-dessous sur le nœud actif du cluster.

Pour créer un système de fichiers répliqué sur le nœud actif du cluster, procédez comme suit :

1. Mettez les deux ressources DRBD en rôle principal :

```
drbdadm primary --force klfocdata
drbdadm primary --force klfocstate
```

2. Formatez les appareils DRBD afin de préparer les volumes répliqués en vue de leur utilisation sur les nœuds du cluster :

```
mkfs.ext4 /dev/drbd0
mkfs.ext4 /dev/drbd2
```

3. Configurez les paramètres du système de fichiers :

```
tune2fs -m 0 /dev/drbd0
tune2fs -m 0 /dev/drbd2
```

4. Montez les appareils DRBD dans les répertoires créés précédemment :

```
mount -o noatime /dev/drbd0 /mnt/KlFocDataShare_klfoc
mount -o noatime /dev/drbd2 /mnt/KlFocStateShare_klfoc
```

   Si le service multipathd est installé, il doit être configuré pour ignorer les appareils `/dev/drbd*` sur les deux nœuds du cluster.

5. Vérifiez l'état de la réplication :

```
drbdadm status
```

   La sortie de la configuration correcte du système de fichiers :

```
klfocdata role:Secondary
disk:UpToDate open:no
db2 role:Primary tls:yes
peer-disk:UpToDate

klfocstate role:Secondary
disk:UpToDate open:no
db2 role:Primary tls:yes
peer-disk:UpToDate
```

Un système de fichiers répliqué est configuré sur le nœud actif du cluster. Vous devez ensuite installer et configurer Corosync et Pacemaker sur les nœuds du cluster.

Installation et configuration de Corosync et Pacemaker sur les nœuds du cluster

Corosync et Pacemaker assurent la communication au sein du cluster et la gestion des ressources pour garantir la haute disponibilité. Ils garantissent que les services sont automatiquement transférés vers un nœud opérationnel en cas de panne, minimisant ainsi les temps d'arrêt.

Pour installer et configurer Corosync et Pacemaker sur les nœuds du cluster, procédez comme suit :

1. Sur les deux nœuds du cluster, installez les paquets requis :

```
dnf install pcs
dnf install drbd-pacemaker
```

2. Configurez Corosync et Pacemaker sur les deux nœuds du cluster en suivant les instructions de la documentation officielle. Pour cela, il faut notamment activer le démarrage automatique, générer et distribuer la clé d'authentification, et configurer les autorisations d'accès au fichier authkey.

   Pour vous assurer que les paramètres sont corrects, exécutez la commande suivante sur l'un des nœuds du cluster :

   ```
   pcs status
   ```

   Le résultat attendu devrait afficher l'état du cluster et dresser la liste de tous les nœuds actifs, confirmant ainsi que Corosync fonctionne correctement et que les nœuds communiquent entre eux.

3. Sur les deux nœuds du cluster, configurez les paramètres de base du cluster Pacemaker :

   ```
   pcs property set stonith-enabled=false
   pcs property set symmetric-cluster=false
   pcs resource defaults resource-stickiness=110
   pcs resource defaults migration-threshold=3
   pcs property set no-quorum-policy=ignore
   ```

4. Sur les deux nœuds du cluster, désactivez le lancement des scripts administrés par Corosync :

   ```
   systemctl disable drbd.service
   ```

5. Sur l'un des nœuds du cluster, créez les ressources basées sur DRBD dans Pacemaker.

   - Ressource DRBD pour klfocdata

     a. Créez une ressource de cluster pour le volume DRBD `klfocdata`, afin que le cluster puisse gérer son état et surveiller automatiquement son intégrité :

     ```
     pcs resource create drbd_klfocdata ocf:linbit:drbd \
     drbd_resource="klfocdata" \
     op monitor interval=60s \
     op start interval=0 timeout=240s \
     op stop interval=0 timeout=240s \
     op monitor role=Master interval=10s \
     op monitor role=Slave interval=30s \
     ```

     b. Créer une ressource `ms_drbd_klfocdata` gérée par le cluster à partir de la ressource `drbd_klfocdata` créée :

     ```
     pcs resource clone drbd_klfocdata promotable=true
     master-max=1
     clone-max=2
     clone-node-max=1 notify=true
     ```

     c. Créez un point de montage pour le volume DRBD `fs_klfocdata` en précisant l'appareil, le répertoire de destination, le type de système de fichiers et les options de montage :

     ```
     pcs resource create fs_klfocdata ocf:heartbeat:Filesystem \
     device="/dev/drbd0" \
     directory="/mnt/KlFocDataShare_klfoc" \
     fstype="ext4" \
     options="data=journal"
     ```

- Ressource DRBD pour klfocstate

  a. Créez une ressource de cluster pour le volume DRBD `klfocstate`, afin que le cluster puisse gérer son état et surveiller automatiquement son intégrité :

  ```
  pcs resource create drbd_klfocstate ocf:linbit:drbd \
  drbd_resource=klfocstate \
  op monitor interval=60s \
  op start interval=0 timeout=240s \
  op stop interval=0 timeout=240s \
  op monitor role=Promoted interval=10s \
  op monitor role=Unpromoted interval=30s \
  ```

  b. Créer une ressource ms_drbd_klfocstate gérée par le cluster à partir de la ressource `drbd_klfocstate` créée :

  ```
  pcs resource clone drbd_klfocstate promotable=true \
  master-max=1 \
  clone-max=2 \
  clone-node-max=1 \
  notify=true
  ```

  c. Créez un point de montage pour le volume DRBD `fs_klfocstate` en précisant l'appareil, le répertoire de destination, le type de système de fichiers et les options de montage :

  ```
  pcs resource create fs_klfocstate ocf:heartbeat:Filesystem \
  device="/dev/drbd2" \
  directory="/mnt/KlFocStateShare_klfoc" \
  fstype="ext4" \
  options="noatime"
  ```

6. Sur les deux nœuds du cluster, désactivez le lancement automatique du service DRBD :

   ```
   systemctl disable drbd.service
   ```

   Corosync et Pacemaker sont installés et configurés sur les nœuds du cluster. Ensuite, il faut installer le SGBD et créer la base de données du Serveur d'administration ainsi que la base de données IAM.

Installation et configuration du SGBD Platform V Pangolin

Une fois que vous avez installé et configuré Corosync et Pacemaker sur les nœuds du cluster, vous devez installer le SGBD sur les deux nœuds du cluster.

Pour installer et configurer le SGBD, procédez comme suit :

1. Sur les deux nœuds du cluster, installez Platform V Pangolin 6.5.1 x64 ou une version ultérieure.

   Pour en savoir plus sur l'installation de Platform V Pangolin, consultez sa documentation.

2. Assurez-vous que les nœuds du cluster sur lesquels le SGBD est installé ne contiennent pas de comptes utilisateurs SGBD portant les noms suivants :

   - client
   - iam
   - ksc

- locker
- pat
- scope
- voltron

3. Sur le nœud actif du cluster, copiez le répertoire DBMS dans le répertoire `/mnt/KlFocDataShare_klfoc/dbms` :

```
sudo rsync -av  /pgdata/06/data/ /mnt/KlFocDataShare_klfoc/dbms
sudo mv /pgdata/06/data/ /pgdata/06/data.bk/
```

4. Sur les deux nœuds du cluster, ouvrez le fichier de configuration `/mnt/KlFocDataShare_klfoc/dbms/postgresql.conf`, puis définissez le répertoire `/mnt/KlFocDataShare_klfoc/dbms` en tant que répertoire des données de la base de données.

   Spécifiez également les chemins d'accès aux fichiers de configuration (`/mnt/KlFocDataShare_klfoc/dbms/pg_hba.conf` et `/mnt/KlFocDataShare_klfoc/dbms/pg_ident.conf`) et supprimez le paramètre `include_dir` :

```
data_directory = '/mnt/KlFocDataShare_klfoc/dbms'
hba_file = '/mnt/KlFocDataShare_klfoc/dbms/pg_hba.conf'
ident_file = '/mnt/KlFocDataShare_klfoc/dbms/pg_ident.conf'
listen_addresses = '*'
```

5. Dans le fichier de configuration `/mnt/KlFocDataShare_klfoc/dbms/postgresql.conf`, adaptez la configuration du SGBD aux exigences de Kaspersky Security Center Linux.

6. Créez et configurez des comptes pour utiliser PostgreSQL.

7. Créez la ressource du service SGBD :

```
pcs resource create klfocsvc_dbms pgsql \
pgctl="/usr/pangolin-6.5/bin/pg_ctl"  psql="/usr/bin/psql" pgdata="/mnt/KlFocDataShare_klfoc/dbms"
config="/mnt/KlFocDataShare_klfoc/dbms/postgresql.conf" socketdir="/tmp" \
op start timeout=60s interval=0s \
op stop timeout=60s interval=0s \
op monitor interval=30s timeout=60s \
op promote timeout=120s interval=0s \
op demote timeout=120s interval=0s \
meta target-role=Started
```

8. Sur les deux nœuds du cluster, désactivez le lancement automatique du service SGBD :

```
sudo systemctl disable pangolin.service
```

9. Ajoutez la ressource SGBD `klfocsvc_dbms` au groupe de clusters `group_klfoc` :

```
pcs resource group add group_klfoc klfocsvc_dbms
```

10. Ajoutez le nom de la ressource SGBD `klfocsvc_dbms` à la fin de la liste, par exemple :

```
group group_klfoc {
...
klfocsvc_dbms
}
```

11. Sur le nœud actif du cluster, sur le serveur SGBD, créez une base de données pour IAM. Le nom de la base de données doit être différent de celui de la base de données que vous avez installée pour fonctionner avec Kaspersky Security Center Linux. Le Serveur d'administration ne supprime pas automatiquement la base de données IAM lors de la désinstallation ou du déplacement du serveur vers un autre appareil. Vous devez supprimer la base de données manuellement :

```
sudo -i -u postgres psql -U postgres -c "CREATE DATABASE <iam_db_name>;"
```

Le SGBD est installé et configuré. La base de données du Serveur d'administration et la base de données IAM sont créées. Ensuite, il faut installer Kaspersky Security Center Linux sur les nœuds du cluster.

Installation de Kaspersky Security Center Linux sur les nœuds d'un cluster de basculement géo-distribué

Kaspersky Security Center Linux est installé sur les nœuds du cluster de basculement géo-distribué à l'aide d'un fichier de réponse en mode silencieux, c'est-à-dire sans intervention de l'utilisateur. Le fichier de réponses contient un ensemble personnalisé de paramètres d'installation : les variables et leurs valeurs respectives.

Prérequis :

- Effectuez toutes les étapes préparatoires :
  - Préparation d'un système de fichiers pour les nœuds d'un cluster
  - Configuration d'un système de fichiers en cluster répliqué
  - Installation et configuration de Corosync et Pacemaker sur les nœuds du cluster
  - Installation et configuration du SGBD Platform V Pangolin
- Assurez-vous que les nœuds du cluster exécutent Platform V SberLinux OS Server (SLO) 9.5.1 x64.
- Téléchargez le fichier d'installation `ksc64_[version_number]_amd64.deb` à partir du site de Kaspersky.

Installation sur le nœud actif

Pour installer Kaspersky Security Center Linux sur le nœud actif 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. Créez un groupe `kladmins` et des comptes non privilégiés `ksc` et `ksciam`, qui doivent être membres 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
adduser ksciam
gpasswd -a ksciam kladmins
usermod -g kladmins ksciam
```

3. Dans le répertoire `/mnt/KlFocDataShare_klfoc/`, créez le répertoire des fichiers Kaspersky Security Center Linux :

```
mkdir /mnt/KlFocDataShare_klfoc/ksc/
```

4. Créez le fichier de réponses (au format TXT) et ajoutez-y une liste de variables au format VARIABLE_NAME=variable_value. Ajoutez chaque variable sur une ligne distincte.

   Dans la liste des paramètres utilisés pour l'installation de Kaspersky Security Center Linux en mode silencieux, indiquez les paramètres suivants, nécessaires au déploiement d'un cluster géo-distribué :

   - `KLFOC_UNATT_EXT_RESOURCE_MANAGEMENT=2`

     Définissez la valeur `2` pour déployer le cluster géo-distribué.

   - `KLSRV_UNATT_SERVERADDRESS=<DNS balancer address>` et `KLSRV_UNATT_IAM_ADDRESS=<DNS balancer address>`

     L'équilibreur de charge DNS avec contrôle d'intégrité doit déjà être déployé. Les valeurs de ces paramètres doivent être identiques et correspondre au nom de domaine complet de l'équilibreur de charge DNS.

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. Lancez l'installation de Kaspersky Security Center Linux en mode silencieux à l'aide des commandes suivantes :

   - Dans l'environnement racine :

```
apt-get install /<path>/ksc64_[version_number]_amd64.deb -y
```

- Dans l'environnement utilisateur :

```
sudo -E apt-get install /<path>/ksc64_[version_number]_amd64.deb -y
```

7. Désactivez le lancement automatique du service klfocsvc_klfoc.service :

```
systemctl disable klfocsvc_klfoc.service
```

8. Une fois que Kaspersky Security Center Linux est installé, arrêtez le nœud actif du cluster.

9. Déplacez toutes les ressources du cluster vers le nœud passif.

   Vous pouvez utiliser la commande `pcs node standby` (et la réactiver avec `pcs node online`).

Installation sur le nœud passif

Pour installer Kaspersky Security Center Linux sur le nœud passif :

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

```
sudo apt-get install /<path>/ksc64_<version_number>_amd64.deb
```

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

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

3. 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 :

   - Saisissez `y` si vous comprenez et acceptez les termes du CLUF. Saisissez `n` si vous n'acceptez pas les conditions du CLUF. Pour utiliser Kaspersky Security Center Linux, vous devez accepter les conditions du Contrat de licence utilisateur final.

   - Saisissez `y` si vous comprenez et acceptez les conditions de la Politique de confidentialité et si 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.

4. Sélectionnez le nœud de cluster passif comme mode d'installation du Serveur d'administration.

5. Lorsque vous y êtes invité, saisissez le chemin d'accès local au point de montage du partage d'état : `/mnt/KlFocStateShare_klfoc`.

6. Désactivez le lancement automatique du service klfocsvc_klfoc.service :

```
systemctl disable klfocsvc_klfoc.service
```

7. Créez la ressource de service `klfocsvc_klfoc` :

```
crm configure primitive klfocsvc_klfoc systemd:klfocsvc_klfoc \
op start timeout="900s" interval="0" \
op stop timeout="900s" interval="0" \
op monitor interval="30s" timeout="90s"
```

8. Ajoutez la ressource `klfocsvc_klfoc` au groupe `group_klfoc` :

```
pcs resource group add group_klfoc klfocsvc_klfoc
```

9. Ajoutez `klfocsvc_klfoc` à la fin de la ligne du groupe, par exemple :

```
group group_klfoc {
...
klfocsvc_klfoc
}
```

10. Vérifiez que toutes les ressources sont à l'état " démarré " sur le nœud actif.

```
pcs status
```

Configuration du chiffrement entre les nœuds du cluster

Pour configurer le chiffrement entre les nœuds du cluster, procédez comme suit :

Si vous avez installé la version 9.2.6 ou une version ultérieure de DRBD lors de la configuration d'un système de fichiers en cluster répliqué, configurez le chiffrement entre les nœuds du cluster conformément à la documentation officielle de DRBD.

Vous pouvez également chiffrer le trafic entre les nœuds du cluster en utilisant votre propre solution VPN.

Le cluster de basculement Kaspersky Security Center Linux géo-distribué est installé. Ensuite, il faut installer Kaspersky Security Center Web Console sur les deux nœuds du cluster.

Installation de Kaspersky Security Center Web Console sur des nœuds de cluster de basculement géo-distribués

Pour un déploiement de cluster de basculement Kaspersky Security Center Linux géo-distribué, il est nécessaire que la haute disponibilité de Kaspersky Security Center Web Console soit prise en charge. Pour ce faire, Kaspersky Security Center Web Console doit être installé sur les deux nœuds du cluster.

Installation de Kaspersky Security Center Web Console :

1. Sur les deux nœuds, créez un utilisateur pour pouvoir utiliser 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 kscadmin -p <password>
   ```

   où le mot de passe doit contenir au moins 8 caractères.

2. Sur les deux nœuds, 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. Sur les deux nœuds, créez un fichier de réponse qui contient les paramètres pour connecter Kaspersky Security Center Web Console au Serveur d'administration : `/etc/ksc-web-console-setup.json`.

   Exemple de fichier de réponse contenant l'ensemble minimal de paramètres

   L'ensemble des paramètres du fichier de réponse dépend de la version du Serveur d'administration auquel Kaspersky Security Center Web Console se connecte :

   - Serveur d'administration 16 ou versions ultérieures

     Exemple de fichier de réponse avec l'ensemble minimal de paramètres pour se connecter au Serveur d'administration version 16 ou version ultérieure :

     ```
     {
         "address": "ksc-web-console.example.com",
         "port": 8080,
         "trusted":  {
             "Administration Server v16": {
                 "iamHost": "ksc16.example.com",
                 "iamOAuthPort": 4444,
                 "iamProxyPort": 9050,
                 "iamCertPath": "/var/opt/kaspersky/klnagent_srv/iam/main_certificate.pem",
                 "iamPATPath": "/var/opt/kaspersky/klnagent_srv/iam/initial_token.txt",
                 "kscPort": 13299,
                 "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
             }
         },
         "certDomain":"ksc-web-console.example.com",
         "acceptEula": true
     }
     ```

   - Serveur d'administration 15.4 ou versions ultérieures

     Exemple de fichier de réponse avec l'ensemble minimal de paramètres pour se connecter au Serveur d'administration version 15.4 ou version antérieure :

     ```
     {
         "address": "ksc-web-console.example.com",
         "port": 8080,
         "trusted":  {
              "Administration Server v15.4": {
                  "kscHost": "ksc.example.com",
                  "kscPort": 13299,
                  "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
              }
         },
         "certDomain":"ksc-web-console.example.com",
         "acceptEula": true
     }
     ```

Vous pouvez installer Kaspersky Security Center Web Console soit sur le même appareil que le Serveur d'administration, soit sur un autre appareil. Si Kaspersky Security Center Web Console est installé sur un autre appareil, l'adresse de Kaspersky Security Center Web Console (définie par `address`) et l'adresse du Serveur d'administration (définie par `iamHost` ou `kscHost`) diffèrent. Si Kaspersky Security Center Web Console est installé sur le même appareil qui héberge le Serveur d'administration, ces paramètres ont les mêmes valeurs.

La valeur `iamHost` doit correspondre à l'adresse IAM spécifiée lors de l'installation du Serveur d'administration. Pour obtenir l'adresse IAM indiquée, exécutez la commande suivante sur l'appareil sur lequel le Serveur d'administration est installé :

```
grep "iam_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml
```

Pour en savoir plus, consultez l'article : Paramètres d'installation de Kaspersky Security Center Web Console.

Vous pouvez ajouter plusieurs Serveurs d'administration de différentes versions à la liste des serveurs approuvés. Dans ce cas, les Serveurs peuvent utiliser différentes méthodes d'authentification.

Nous vous recommandons d'indiquer les numéros de port supérieurs à 1024. Si vous voulez que Kaspersky Security Center Web Console fonctionne sur les ports inférieurs à 1024, après l'installation, vous devez vous assurer que vous avez l'utilitaire setcap, puis exécutez la commande suivante :

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

Si vous ne disposez pas de l'utilitaire setcap, vous pouvez l'installer. **Cliquez sur ce lien pour voir les commandes**.

Pour les systèmes d'exploitation Debian et Ubuntu, exécutez l'une des commandes suivantes :

- `sudo apt-get install libcap2-bin`
- `sudo apt install libcap2-bin`

Pour SUSE Linux Enterprise Server et Red Hat Enterprise Linux, exécutez la commande suivante :

- `sudo zypper install libcap-progs`

4. Sur les deux nœuds, exécutez le fichier de configuration sous un compte disposant des privilèges root.

```
sudo apt-get install 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. Sur l'un des nœuds du cluster, créez une ressource Pacemaker pour le service KSCWebConsole afin que ce dernier soit géré par Pacemaker :

```
crm configure primitive ksc_webconsole systemd:KSCWebConsole \
op monitor interval=30s timeout=60s \
op start timeout=120s \
op stop timeout=120s \
meta target-role=Stopped
```

6. Sur les deux nœuds, arrêtez le service KSCWebConsole et désactivez son lancement automatique :

```
sudo systemctl stop KSCWebConsole
sudo systemctl disable KSCWebConsole
```

7. Sur l'un des nœuds du cluster, ajoutez la ressource `ksc_webconsole` au groupe `group_klfoc` :

```
crm configure edit group_klfoc
```

8. Ajoutez `ksc_webconsole` à la fin de la ligne de groupe, après `klfocsvc_dbms`, par exemple :

```
group group_klfoc {
...
klfocsvc_dbms
ksc_webconsole
}
```

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

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.

N'apportez aucune modification manuelle à la base de données du Serveur d'administration ni à la base de données IAM, qu'il s'agisse de modifier des valeurs, de supprimer ou d'ajouter des schémas, des tables ou des index. Toute modification apportée aux bases de données qui n'est pas effectuée par le Serveur d'administration lui-même perturbe le bon fonctionnement de ce dernier, soit immédiatement, soit ultérieurement, par exemple après avoir mis à niveau le système vers une version plus récente, lors de la restauration à partir d'une copie de sauvegarde, etc. La modification des bases de données n'est autorisée que si vous avez reçu des instructions explicites du Support technique de Kaspersky.

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 la section Configuration du compte SGBD pour l'utilisation avec MySQL et MariaDB.

Pour en savoir plus sur le déplacement des données d'un tablespace partagé vers un tablespace fichier par table, consultez la section Déplacement des données depuis un tablespace partagé vers un tablespace fichier par table dans les SGBD MySQL et MariaDB.

Configuration des privilèges pour la récupération des données du Serveur d'administration

Les droits que vous avez accordés au compte SGBD interne suffisent pour restaurer les données du Serveur d'administration à partir de la sauvegarde.

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.

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.

Lors de l'utilisation d'un cluster Postgres à haute disponibilité (version 14 ou version ultérieure) comme base de données, l'utilisateur de la base de données doit avoir le privilège `pg_read_all_stats`. Vous pouvez accorder ce privilège à l'aide de la commande suivante :

```
GRANT pg_read_all_stats TO "%1";
```

où `%1` est le nom de l'utilisateur de la base de données.

Le nom d'utilisateur est indiqué lors du programme d'installation du Serveur d'administration dans le paramètre `KLSRV_UNATT_DBMS_LOGIN`.

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.

N'apportez aucune modification manuelle à la base de données du Serveur d'administration ni à la base de données IAM, qu'il s'agisse de modifier des valeurs, de supprimer ou d'ajouter des schémas, des tables ou des index. Toute modification apportée aux bases de données qui n'est pas effectuée par le Serveur d'administration lui-même perturbe le bon fonctionnement de ce dernier, soit immédiatement, soit ultérieurement, par exemple après avoir mis à niveau le système vers une version plus récente, lors de la restauration à partir d'une copie de sauvegarde, etc. La modification des bases de données n'est autorisée que si vous avez reçu des instructions explicites du Support technique de Kaspersky.

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 kscdbadmin et spécifiez le mot de passe pour kscdbadmin
   */
   CREATE USER 'kscdbadmin' IDENTIFIED BY '<mot de passe>';
   ```

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 kscdbadmin */
   GRANT USAGE ON *.* TO 'kscdbadmin';
   GRANT ALL ON kav.* TO 'kscdbadmin';
   GRANT SELECT, SHOW VIEW ON mysql.* TO 'kscdbadmin';
   GRANT SELECT, SHOW VIEW ON sys.* TO 'kscdbadmin';
   GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'kscdbadmin';
   GRANT PROCESS ON *.* TO 'kscdbadmin';
   GRANT SUPER ON *.* TO 'kscdbadmin';
   ```

   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 'kscdbadmin'`.

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

   ```
   SHOW grants for 'kscdbadmin';
   ```

5. Créez un compte SGBD pour IAM. Exécutez la commande suivante :

   ```
   /* Créez un utilisateur nommé iamdbadmin et spécifiez le mot de passe pour iamdbadmin
   */
   CREATE USER 'iamdbadmin' 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 'iamdbadmin'@'%' IDENTIFIED WITH mysql_native_password BY '<mot de passe>';
  ```

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

  ```
  ALTER USER 'iamdbadmin'@'%' IDENTIFIED WITH mysql_native_password BY '<mot de passe>';
  ```

6. 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 iamdbadmin */
   GRANT USAGE ON *.* TO 'iamdbadmin';
   GRANT ALL ON iamdb.* TO 'iamdbadmin';
   GRANT SELECT, SHOW VIEW ON mysql.* TO 'iamdbadmin';
   GRANT SELECT, SHOW VIEW ON sys.* TO 'iamdbadmin';
   GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'iamdbadmin';
   GRANT PROCESS ON *.* TO 'iamdbadmin';
   GRANT SUPER ON *.* TO 'iamdbadmin';
   ```

   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 'iamdbadmin'`.

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

   ```
   SHOW grants for 'iamdbadmin';
   ```

8. Pour créer manuellement une base de données du Serveur d'administration, exécutez la commande suivante (dans cette commande, le nom de la base de données du Serveur d'administration est *kav*) :

   ```
   CREATE DATABASE kav
   ```

   Utilisez le même nom de base de données que vous avez indiqué dans le script qui crée le compte SGBD.

9. Pour créer manuellement une base de données IAM, exécutez le script suivant (dans cette commande, le nom de la base de données IAM est *iam*) :

   ```
   CREATE DATABASE iam
   ```

Le Serveur d'administration ne supprime pas automatiquement la base de données IAM lors de la désinstallation ou du déplacement du serveur vers un autre appareil. Vous devez supprimer la base de données manuellement.

10. 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.
3. Configurez le serveur PostgreSQL ou Postgres Pro pour qu'il fonctionne avec Kaspersky Security Center Linux.

N'apportez aucune modification manuelle à la base de données du Serveur d'administration ni à la base de données IAM, qu'il s'agisse de modifier des valeurs, de supprimer ou d'ajouter des schémas, des tables ou des index. Toute modification apportée aux bases de données qui n'est pas effectuée par le Serveur d'administration lui-même perturbe le bon fonctionnement de ce dernier, soit immédiatement, soit ultérieurement, par exemple après avoir mis à niveau le système vers une version plus récente, lors de la restauration à partir d'une copie de sauvegarde, etc. La modification des bases de données n'est autorisée que si vous avez reçu des instructions explicites du Support technique de Kaspersky.

Configurer les comptes SGBD pour installer le Serveur d'administration

Pour configurer les comptes SGBD pour l'installation du Serveur d'administration :

1. Exécutez un environnement pour l'utilisation avec Postgres.
2. Connectez-vous sous l'utilisateur *Postgres* dans la base de données *Postgres*.
3. Créez un nouveau rôle Postgres (dans cet exemple, le rôle est *kscdbadmin*) :

```
CREATE USER "kscdbadmin" WITH PASSWORD '<password>';
```

4. Créez une base de données pour le Serveur d'administration (dans cet exemple, son nom est `kav`) :

```
CREATE DATABASE "kav" ENCODING 'UTF8' OWNER "kscdbadmin";
```

Nous vous recommandons de définir le rôle Postgres créé à l'étape 3 de cette instruction comme propriétaire de la base de données (dans cet exemple, le rôle est *kscdbadmin*).

Définir un autre utilisateur comme propriétaire de la base de données

Si vous devez définir un autre rôle Postgres, connectez-vous à la base de données du Serveur d'administration sous ce rôle de propriétaire (ou de superutilisateur) et exécutez les commandes suivantes :

```
GRANT ALL PRIVILEGES ON DATABASE "kav" TO "kscdbadmin";
GRANT USAGE ON SCHEMA public TO "kscdbadmin";
GRANT CREATE ON SCHEMA public TO "kscdbadmin";
GRANT ALL PRIVILEGES ON ALL TABLES IN SCHEMA "public" TO "kscdbadmin";
GRANT ALL PRIVILEGES ON ALL SEQUENCES IN SCHEMA "public" TO "kscdbadmin";
```

Assurez-vous que le rôle du propriétaire de la base de données dispose des privilèges CONNECT et TEMPORARY.

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 "kscdbadmin" TEMPLATE template0;`
au lieu de :
`CREATE DATABASE "kav" ENCODING 'UTF8' OWNER "kscdbadmin";`

5. Créez un rôle Postgres pour IAM (dans cet exemple, le rôle Postgres est `iamdbadmin`) :

```
CREATE USER "iamdbadmin" WITH PASSWORD '<password>';
```

6. Créez une base de données IAM (dans cet exemple, le nom de la base de données IAM est `iam`) :

```
CREATE DATABASE "iam" ENCODING 'UTF8' OWNER "iamdbadmin";
```

Nous vous recommandons de définir le rôle Postgres créé à l'étape 5 de cette instruction comme propriétaire de la base de données (dans cet exemple, le rôle est *iamdbadmin*).

Définir un autre utilisateur comme propriétaire de la base de données IAM

Si vous devez définir un autre rôle Postgres, connectez-vous à la base de données IAM sous ce rôle (ou sous le rôle de superutilisateur) et exécutez les commandes suivantes :

```
GRANT ALL PRIVILEGES ON DATABASE "iam" TO "iamdbadmin";
GRANT USAGE ON SCHEMA public TO "iamdbadmin";
GRANT CREATE ON SCHEMA public TO "iamdbadmin";
GRANT ALL PRIVILEGES ON ALL TABLES IN SCHEMA "public" TO "iamdbadmin";
GRANT ALL PRIVILEGES ON ALL SEQUENCES IN SCHEMA "public" TO "iamdbadmin";
```

Assurez-vous que le rôle du propriétaire de la base de données dispose des privilèges CONNECT et TEMPORARY.

> 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 "iam" ENCODING 'UTF8' OWNER "iamdbadmin" TEMPLATE template0;`
> au lieu de :
> `CREATE DATABASE "iam" ENCODING 'UTF8' OWNER "iamdbadmin";`

Le Serveur d'administration ne supprime pas automatiquement la base de données IAM lors de la désinstallation ou du déplacement du serveur vers un autre appareil. Vous devez supprimer la base de données manuellement.

7. 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.

Déplacement de données d'un tablespace partagé vers un tablespace fichier par table dans les SGBD MySQL ou MariaDB

Pour les SGBD MySQL et MariaDB, vous pouvez stocker les données comme suit :

- En tant que tablespace partagé, lorsque les données de toutes les bases de données utilisateur sont stockées dans un fichier unique (généralement, dans le fichier `ibdata1`).
- En tant que tablespace fichier par table, lorsqu'un espace de données distinct est créé pour chaque table en tant que fichier distinct.

L'utilisation d'un tablespace partagé augmente le risque de fragmentation du tablespace. L'opération `SHRINK` étant impossible, un fichier du tablespace partagé peut occuper environ 90 % de l'espace disque. Cela affecte négativement les performances du sous-système de disque. Il est donc utile d'opter pour un tablespace fichier par table.

Cet article explique comment déplacer des données d'un tablespace partagé vers un tablespace fichier par table. Si les SGBD MySQL ou MariaDB sont également utilisés par d'autres applications, vous devez déplacer les bases de données de ces applications dans le tablespace fichier par table.

> Il est recommandé de n'effectuer cette procédure que si vous utilisez les SGBD MySQL ou MariaDB pour le Serveur d'administration.
> Le déplacement des données d'un tablespace partagé vers un tablespace fichier par table peut augmenter la charge du sous-système de disque.

Prérequis

Avant de commencer, assurez-vous que :

- Vous avez créé une copie de sauvegarde des données du Serveur d'administration en exécutant une tâche de sauvegarde des données ou l'utilitaire klbackup.
- Vous avez créé une copie de sauvegarde des autres applications dont les bases de données sont gérées par le SGBD MySQL ou MariaDB (le cas échéant).
- Sur l'appareil sur lequel le SGBD est installé, il y a de l'espace libre sur la partition avec la base de données.

L'espace disque requis représente 150 % de la taille totale actuelle des bases (taille actuelle du fichier `ibdata1`).

Processus

Pour déplacer des données d'un tablespace partagé vers un tablespace fichier par table, procédez comme suit :

1. Arrêtez le service du Serveur d'administration de Kaspersky Security Center et les autres applications utilisant l'instance du SGBD pour lequel vous souhaitez exécuter cette procédure.
2. En fonction de la version du SGBD, connectez-vous à votre SGBD en tant que superutilisateur, puis, dans n'importe quelle application pratique, exécutez le script `fix_tablespace.sql`.

   Vous pouvez consulter les scripts `fix_tablespace.sql` en cliquant sur ces liens :

   Consultez le script pour MySQL 5.7 et MariaDB 10.1 ou toute version ultérieure

```
DROP PROCEDURE IF EXISTS upgd_alter_all_tables_for_all_databases_to_innodb;
DELIMITER //
CREATE PROCEDURE `upgd_alter_all_tables_for_all_databases_to_innodb` ()
BEGIN
    DECLARE __st_FETCH_STATUS INT;
    DECLARE `schemaName` VARCHAR(192);
    DECLARE `tableName` VARCHAR(192);
    DECLARE `curIX` CURSOR FOR
    SELECT `TABLE_SCHEMA` , `TABLE_NAME`
    FROM information_schema.TABLES
    WHERE `TABLE_SCHEMA` NOT IN ('mysql', 'performance_schema', 'sys') AND TABLE_TYPE = 'BASE TABLE';
    DECLARE CONTINUE HANDLER FOR SQLSTATE '02000' SET __st_FETCH_STATUS = 1;
    OPEN `curIX`;
    SET `__st_FETCH_STATUS` = 0; FETCH `curIX` INTO `schemaName`, `tableName`;
    while1 : WHILE (0 = 0 AND __st_FETCH_STATUS = 0 ) DO
        SET @`strSQL` = CONCAT( 'ALTER TABLE `' , `schemaName`, '`.`',`tableName`, '` ENGINE=''InnoDB'';'
);
        PREPARE stmt1 FROM @`strSQL`;
        EXECUTE stmt1;
        DEALLOCATE PREPARE stmt1;
        SET `__st_FETCH_STATUS` = 0; FETCH `curIX` INTO `schemaName`, `tableName`;
    END WHILE;
    CLOSE `curIX`;
END
//
DELIMITER ;
SET GLOBAL innodb_file_per_table = 1;
CALL upgd_alter_all_tables_for_all_databases_to_innodb();
DROP PROCEDURE IF EXISTS upgd_alter_all_tables_for_all_databases_to_innodb;
```

Consultez le script pour MySQL 8.0+

```
DROP PROCEDURE IF EXISTS upgd_alter_all_tables_for_all_databases_to_innodb;
DELIMITER //
CREATE PROCEDURE `upgd_alter_all_tables_for_all_databases_to_innodb` ()
BEGIN
    DECLARE __st_FETCH_STATUS INT;
    DECLARE `schemaName` VARCHAR(192);
    DECLARE `tableName` VARCHAR(192);
    DECLARE `curIX` CURSOR FOR
    SELECT `TABLE_SCHEMA` , `TABLE_NAME`
    FROM information_schema.TABLES
    WHERE `TABLE_SCHEMA` NOT IN ('mysql', 'performance_schema', 'sys') AND TABLE_TYPE = 'BASE TABLE';
    DECLARE CONTINUE HANDLER FOR SQLSTATE '02000' SET __st_FETCH_STATUS = 1;
    OPEN `curIX`;
    SET `__st_FETCH_STATUS` = 0; FETCH `curIX` INTO `schemaName`, `tableName`;
    while1 : WHILE (0 = 0 AND __st_FETCH_STATUS = 0 ) DO
        SET @`strSQL` = CONCAT( 'ALTER TABLE `' , `schemaName`, '`.`',`tableName`, '` ENGINE=''InnoDB'';'
);
        PREPARE stmt1 FROM @`strSQL`;
        EXECUTE stmt1;
        DEALLOCATE PREPARE stmt1;
        SET @`strSQL` = CONCAT( 'ALTER TABLE `' , `schemaName`, '`.`',`tableName`, '` TABLESPACE =
innodb_file_per_table;' );
        PREPARE stmt2 FROM @`strSQL`;
        EXECUTE stmt2;
        DEALLOCATE PREPARE stmt2;
        SET `__st_FETCH_STATUS` = 0; FETCH `curIX` INTO `schemaName`, `tableName`;
    END WHILE;
    CLOSE `curIX`;
END
//
DELIMITER ;
SET GLOBAL innodb_file_per_table = 1;
CALL upgd_alter_all_tables_for_all_databases_to_innodb();
DROP PROCEDURE IF EXISTS upgd_alter_all_tables_for_all_databases_to_innodb;
```

Vous ne devez pas arrêter l'exécution du script.
Si aucune erreur de SGBD ne s'est produite, mais que vous avez interrompu l'exécution du script, soit exécutez à nouveau le script, soit arrêtez d'exécuter les étapes de cette procédure, redémarrez le service SGBD et restaurez les données du Serveur d'administration à partir de la sauvegarde.

3. Dans la section `[mysqld]` du fichier my.cnf, définissez le paramètre `innodb_file_per_table` sur `1`.

4. Redémarrez le service MySQL ou MariaDB.

5. Relancez le service du Serveur d'administration de Kaspersky Security Center.

Les données sont déplacées d'un tablespace partagé vers un tablespace fichier par table.

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 mobile
- Certificat du Serveur Web
- Certificat de Kaspersky Security Center Web Console
- Certificat du Gestionnaire des identités et des accès

Par défaut, Kaspersky Security Center utilise des certificats autosignés (c'est-à-dire des certificats délivrés par Kaspersky Security Center lui-même). Si nécessaire, vous pouvez remplacer les certificats autosignés par des certificats utilisateur conformément aux normes de sécurité de votre organisation. Lors de l'utilisation d'un certificat personnalisé, le fichier de certificat doit inclure la chaîne complète des clés publiques, y compris tous les certificats intermédiaires jusqu'à l'autorité de certification (AC) racine. 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.
- CR—certificat commun de réserve pour les ports 13000 et 13291.
- M—certificat mobile pour le port 13292.
- MR—certificat mobile de réserve pour le port 13292.
- MCA—autorité de certification mobile pour les certificats utilisateur générés automatiquement.

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 lorsque Kaspersky Security Center Web Console s'y connecte.
- 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 crée 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. À cet effet, le certificat commun de réserve devient 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.

Une fois que le certificat du Serveur d'administration a été remplacé par un certificat de réserve ou personnalisé, indiquez le nouveau certificat dans le fichier de réponse, puis réinstallez Kaspersky Security Center Web Console à l'aide de ce fichier. Sinon, Kaspersky Security Center Web Console ne pourra pas se connecter au Serveur d'administration.

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.

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.

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 90 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.

De plus, l'authentification du Serveur d'administration sur les appareils mobiles qui fonctionnent sous le système d'exploitation iOS requiert un certificat du serveur MDM iOS. Pour en savoir plus, consultez la section Configuration d'un certificat de serveur MDM iOS.

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, ainsi que pour les paquets d'installation de Kaspersky Security for Mobile. Pour cela, le Serveur Web peut utiliser différents certificats.

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

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

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

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

Certificat de Kaspersky Security Center Web Console

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 Kaspersky Security Center Web Console 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.

Certificat du Gestionnaire des identités et des accès

Un certificat du Gestionnaire des identités et des accès (certificat IAM) est requis dans les cas suivants :

- Authentification du Serveur d'administration lorsqu'un utilisateur s'y connecte via le protocole OAuth.
- Authentification du Serveur d'administration lorsque Kaspersky Security Center Web Console s'y connecte.

Le certificat IAM est créé automatiquement lors de la première exécution du Serveur d'administration. Le certificat est stocké sur l'appareil du Serveur d'administration dans le répertoire suivant : /var/opt/kaspersky/klnagent_srv/iam/main_certificate.pem (pour le cluster de basculement Kaspersky Security Center : <dossier de données partagé>/iam/main_certificate.pem). Lorsque vous créez le fichier de réponse pour l'installation de Kaspersky Security Center Web Console, vous devez indiquer le chemin d'accès au certificat IAM à l'aide du paramètre `iamCertPath`.

Le certificat IAM est valable 365 jours. Kaspersky Security Center crée automatiquement un certificat IAM de réserve 48 heures avant l'expiration du certificat actuel. Le certificat de réserve est ensuite utilisé pour remplacer facilement le certificat IAM expiré.

La durée de validité maximale de tout certificat IAM ne doit pas dépasser 397 jours.

Si nécessaire, vous pouvez attribuer un certificat IAM personnalisé. 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.

> Une fois que le certificat IAM a été remplacé par un certificat de réserve ou personnalisé, indiquez le nouveau certificat dans le fichier de réponse, puis réinstallez Kaspersky Security Center Web Console à l'aide de ce fichier. Sinon, Kaspersky Security Center Web Console ne pourra pas se connecter au Serveur d'administration.

Lorsque vous vous connectez à Kaspersky Security Center Web Console, le navigateur est redirigé vers la page de connexion au Serveur d'administration (https://<`adresse du Serveur d'administration`>:4444) pour l'authentification. Le trafic entre le navigateur et le Serveur d'administration est chiffré à l'aide du protocole TLS et du certificat IAM.

Il se peut que le navigateur vous informe que la connexion au Serveur d'administration n'est pas privée et que le certificat IAM est incorrect. Cet avertissement apparaît car le certificat IAM est auto-signé et généré automatiquement par Kaspersky Security Center. Pour supprimer cet avertissement, vous pouvez effectuer une des actions suivantes :

- Remplacez le certificat IAM 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 IAM 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 clé • Signature CRL Utilisation de clés étendues (facultatif) : authentification du serveur, authentification du client. Le certificat doit inclure un nom alternatif du sujet (SAN) valide qui contient l'adresse de bouclage du Serveur d'administration : • Pour IPv4 : 127.0.0.1 • Pour IPv6 : 0:0:0:0:0:0:0:1	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 imposées aux certificats de serveur ainsi qu'aux exigences de base actuelles du Forum CA/Browser.	—
Certificat de Kaspersky Security Center Web Console	Utilisation de clés étendues (EKU) : authentification du serveur. 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. La valeur doit correspondre à l'adresse IAM spécifiée lors de l'installation du Serveur d'administration. Pour obtenir l'adresse IAM indiquée, exécutez la commande suivante sur l'appareil sur lequel le Serveur d'administration est installé : `grep "iam_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml` Le certificat répond aux exigences réelles des navigateurs imposées aux certificats de serveur ainsi qu'aux exigences de base actuelles du Forum CA/Browser.	Les certificats chiffrés ne sont pas pris en charge par Kaspersky Security Center Web Console.
Certificat du Gestionnaire des identités et des accès (certificat IAM)	Utilisation de clés étendues : authentification du serveur. Le conteneur PEM à partir duquel le certificat est indiqué inclut la chaîne entière de clés publiques. Le certificat répond aux exigences réelles des navigateurs imposées aux certificats de serveur ainsi qu'aux exigences de base actuelles du Forum CA/Browser.	Les certificats chiffrés ne sont pas pris en charge par Kaspersky Security Center Web Console.

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. Ouvrez le fichier de réponse que vous avez créé lors de l'installation de Kaspersky Security Center Web Console.

   Si vous le souhaitez, vous pouvez créer un nouveau fichier de réponse.

2. Dans le fichier, spécifiez les chemins d'accès suivants :

   - vers le fichier de certificat personnalisé de Kaspersky Security Center Web Console à l'aide du paramètre `certPath` ;
   - vers la clé privée associée au certificat personnalisé de Kaspersky Security Center Web Console à l'aide du paramètre `keyPath`.

     Vous devez spécifier les deux chemins. Sinon, le navigateur Internet continue de vous informer que votre connexion n'est pas privée.

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 <nom du fichier.pfx> -clcerts -nokeys | sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > server.crt
   ```

   ```
   openssl pkcs12 -in <nom du fichier.pfx> -nocerts -nodes | sed -ne '/-BEGIN PRIVATE KEY-/,/-END PRIVATE KEY-/p' > key.pem
   ```

2. Assurez-vous que le fichier de certificat et la clé privée sont générés dans le même répertoire où le fichier .pfx est stocké.

3. Kaspersky Security Center Web Console ne prend pas en charge les certificats protégés par une phrase secrète. Par conséquent, exécutez la commande suivante dans un utilitaire multiplateforme basé sur OpenSSL pour supprimer une phrase secrète du fichier .pem :

   ```
   openssl rsa -in key.pem -out key-without-passphrase.pem
   ```

   N'utilisez pas le même nom pour les fichiers .pem d'entrée et de sortie.

   Par conséquent, le nouveau fichier .pem n'est pas chiffré. Vous n'avez pas besoin d'entrer une phrase secrète pour l'utiliser.

Les fichiers .crt et .pem sont prêts à l'emploi, vous pouvez donc les spécifier dans le programme d'installation de Kaspersky Security Center Web Console.

Scénario : Spécifier le certificat personnalisé du Serveur d'administration

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

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

Prérequis

Les conditions suivantes doivent être remplies :

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

  Dans le tableau suivant, prenez note de l'exigence « CA: true ». Cela signifie que le nouveau certificat doit être émis par une autorité de certification (CA) de confiance. Le nouveau certificat portant la mention " CA: true " doit inclure toute la chaîne de confiance et une clé privée, qui doit être stockée dans un fichier avec l'extension pfx ou p12.

Conditions requises pour les certificats du Serveur d'administration

Type de certificat	Conditions
Certificat commun, certificat de réserve commun ("C", "CR")	Longueur de clé minimale : 2 048. Contraintes de base : • Contrainte de longueur de chemin : aucune La valeur Contrainte de longueur de chemin peut varier d'un nombre entier de "Aucune", mais ne peut pas être inférieure à 1. Utilisation des clés : • Signature numérique • Signature du certificat • Chiffrement de clé • Signature CRL Utilisation de clés étendues (EKU) : authentification du serveur, authentification du client. L'EKU est facultative, mais si votre certificat la contient, les données d'authentification du serveur et du client doivent être spécifiées dans l'EKU. Le certificat doit inclure un nom alternatif du sujet (SAN) valide qui contient l'adresse de bouclage du Serveur d'administration : • Pour IPv4 : 127.0.0.1 • Pour IPv6 : 0:0:0:0:0:0:0:1

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

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

Étapes

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

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

   Utiliser la ligne de commande utilitaire klsetsrvcert dans ce but.

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

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

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

   Après avoir remplacé le certificat, indiquez-le dans le fichier de réponses, puis mettez à jour Kaspersky Security Center Web Console à l'aide de ce fichier. Sinon, Kaspersky Security Center Web Console ne pourra pas se connecter au Serveur d'administration.

Résultats

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

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

Pour éviter de perdre le contrôle des appareils, consultez le scénario : spécification du certificat personnalisé du Serveur d'administration avant de continuer.

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

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

```
/opt/kaspersky/ksc64/sbin/klsetsrvcert [-t <certificate type> {-i <path to new certificate> [-p <password>] [-o
<validation parameters>] | -g <dns name>}][-f <replacement time>][-r <root certificates>][-l <log file path>]
```

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

Valeurs des paramètres de l'utilitaire klsetsrvcert

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

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

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

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

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

1. Pour installer le nouveau certificat,

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

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

   ```
   klsetsrvcert -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.

Questions et réponses

Quelles sont les étapes supplémentaires à suivre après le remplacement du certificat commun du Serveur d'administration ?

1. Assurez-vous que les **conditions requises pour les certificats personnalisés sont remplies**.

   Si vous utilisez un certificat personnalisé au lieu du certificat auto-signé, avant de mettre à niveau Kaspersky Security Center Linux vers une version plus récente, vous devez vous assurer que le certificat inclut le nom alternatif du sujet (SAN). Si ce n'est pas le cas, il est important de remplacer le certificat avant de mettre à niveau Kaspersky Security Center Linux. Sinon, vous ne pourrez pas vous connecter à Web Console après la mise à niveau.

   Pour vous assurer que le certificat inclut un SAN, procédez comme suit :

   1. Sur l'appareil sur lequel le Serveur d'administration est installé, exécutez la commande suivante :

      - Pour un appareil fonctionnant sous Linux :

        ```
        sudo openssl x509 -in
        /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -noout -ext
        subjectAltName
        ```

      - Pour un appareil fonctionnant sous Windows :

        ```
        certutil -dump %ProgramData%\KasperskyLab\adminkit\1093\cert\klserver.cer
        ```

2. Assurez-vous que le nom alternatif du sujet (SAN) figure dans la sortie de la commande et qu'il contient l'adresse de l'appareil du Serveur d'administration.

3. Si le nom alternatif du sujet est absent, utilisez l'utilitaire klsetsrvcert pour remplacer votre certificat utilisateur par un certificat conforme aux exigences.

2. Assurez-vous que le fichier de configuration du serveur IAM contient l'adresse actuelle du Serveur d'administration. Sinon, ajoutez l'adresse au fichier de configuration.

3. Réinstallez Web Console pour éviter l'erreur suivante :

   Le Serveur d'administration utilise un certificat non approuvé. Veuillez reconfigurer l'application en indiquant un certificat valide, ou contactez l'administrateur principal.

Connexion des Agents d'administration 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 [-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 : `<chemin>\klmover.exe [-address <adresse du serveur>] [-pn <numéro de port>] [-ps <numéro de port SSL>] [-nossl] [-cert <chemin d'accès au fichier de certificat>]`
- Pour macOS :

  ```
  /Library/Application Support/Kaspersky Lab/klnagent/Binaries/klmover [-address <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 < adresse du serveur >`	Adresse du Serveur d'administration pour la connexion. Vous pouvez spécifier une adresse IP ou un nom DNS.
`-pn < numéro de port >`	Numéro de port à utiliser pour une connexion non sécurisée au Serveur d'administration. Le numéro de port par défaut est 14000.
`-ps < numéro de port SSL >`	Numéro de port SSL à utiliser pour une connexion sécurisée au Serveur d'administration sous protocole SSL. Le numéro de port par défaut est 13000.
`-nossl`	Utilise une connexion non sécurisée au Serveur d'administration. Si aucune clé n'est utilisée, la connexion de l'Agent d'administration au Serveur d'administration est établie à l'aide du protocole sécurisé SSL.
`-cert < chemin d'accès au fichier de certificat >`	Utilise le fichier de certificat spécifié pour l'authentification, afin d'accéder au Serveur d'administration.
`-nauninstpwd < mot de passe >`	Utilisez ce paramètre pour spécifier le mot de passe de désinstallation de l'Agent d'administration. Paramètre facultatif.

Réémettre le certificat du Serveur Web

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

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

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

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

1. générez votre certificat personnalisé et préparez-le pour l'utiliser dans Kaspersky Security Center Linux. Vérifiez si votre certificat personnalisé répond aux exigences de Kaspersky Security Center Linux. S'il y a lieu, modifiez le certificat.

2. Dans le menu principal, cliquez sur le nom du Serveur d'administration.

   La fenêtre des propriétés du Serveur d'administration s'ouvre.

3. Sous l'onglet **Général**, sélectionnez la section **Serveur Internet**.

4. Dans la sous-section **Par le protocole HTTP**, sélectionnez l'option **Charger le certificat depuis le fichier** et cliquez sur le bouton **Changer le certificat**.

5. Dans la fenêtre qui s'ouvre, sélectionnez dans le champ **Format du certificat** le type de votre certificat :

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

   - Si vous avez sélectionné **Certificat X.509**, cliquez sur le bouton **Parcourir** à côté du champ **Clé privée** et spécifiez la clé privée sur votre disque dur. Si la clé privée est protégée par mot de passe, saisissez le mot de passe dans le champ **Mot de passe**.

6. Cliquez sur le bouton **Enregistrer**, puis cliquez sur le bouton **OK**.

   La fenêtre se ferme.

7. Si nécessaire, dans le champ **Port HTTPS du serveur Internet**, modifiez le numéro du port HTTPS du Serveur Internet et cliquez sur le bouton **Enregistrer**.

Le certificat du serveur Web est réémis.

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

1. Dans le menu principal, cliquez sur le nom du Serveur d'administration.

   La fenêtre des propriétés du Serveur d'administration s'ouvre.

2. Sous l'onglet **Général**, sélectionnez la section **Certificats**.

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

   a. Sélectionnez l'option **Le certificat a été émis via le Serveur d'administration** et cliquez sur le bouton **Parcourir**.

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

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

a. Vérifiez si votre certificat personnalisé répond aux exigences de Kaspersky Security Center Linux. S'il y a lieu, modifiez le certificat.

b. Sélectionnez l'option **Autre certificat**, cliquez sur le bouton **Gérer le certificat**, puis, dans la fenêtre qui s'ouvre, cliquez sur le bouton **Parcourir**.

c. Dans la fenêtre qui s'ouvre, sélectionnez dans le champ **Format du certificat** le type de votre certificat :

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

   - Si vous avez sélectionné **Certificat X.509**, cliquez sur le bouton **Parcourir** à côté du champ **Clé privée** et spécifiez la clé privée sur votre disque dur. Si la clé privée est protégée par mot de passe, saisissez le mot de passe dans le champ **Mot de passe**.

d. Cliquez sur le bouton **Enregistrer**, puis cliquez sur le bouton **OK**.

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

Remplacer le certificat IAM par défaut par un certificat personnalisé

Pour modifier le certificat IAM par défaut :

1. générez votre certificat personnalisé et préparez-le pour l'utiliser dans Kaspersky Security Center Linux. Vérifiez si votre certificat personnalisé répond aux exigences de Kaspersky Security Center Linux.

2. Assurez-vous que le groupe kladmins a accès aux fichiers du certificat IAM.

3. Localisez le fichier de configuration IAM : `/var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml`

   Dans ce fichier, ajoutez les chemins d'accès aux fichiers de certificats IAM à la section `server_iam` :

   - `certificates.main.cert` : chemin d'accès au certificat principal.

   - `certificates.main.key` : chemin d'accès à la clé privée du certificat principal. La clé privée ne doit pas être protégée par un mot de passe.

4. Localisez le fichier de configuration de Web Console : `/etc/ksc-web-console-setup.json`

   Dans ce fichier, définissez la valeur du champ `iamCertPath` sur le chemin d'accès à la clé publique du certificat principal.

5. Redémarrez le service kliam à l'aide de la commande suivante :

   ```
   sudo service kliam_srv restart
   ```

6. Réinstallez Web Console.

   Une fois réinstallée, la Web Console utilise le certificat IAM personnalisé.

Pour modifier le certificat IAM de réserve, procédez comme suit :

1. Localisez le fichier de configuration IAM : `/var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml`

   Dans ce fichier, indiquez les chemins vers les fichiers de certificat IAM :

   - `server_iam.certificates.reserve.cert` : chemin d'accès au certificat principal.
   - `server_iam.certificates.reserve.key` : chemin d'accès à la clé privée du certificat principal. La clé privée ne doit pas être protégée par un mot de passe.

2. Redémarrez le service kliam à l'aide de la commande suivante :

   ```
   sudo systemctl restart kliam_srv.service
   ```

   Une fois que le fichier de certificat principal expire, le certificat IAM de réserve est utilisé à la place.

Ajout de l'adresse du Serveur d'administration à la configuration du serveur IAM

Après avoir modifié le certificat du Serveur d'administration commun (" C ") lors d'une mise à niveau, d'un déplacement ou d'une migration, vous devez indiquer l'adresse du Serveur d'administration dans le fichier de configuration du serveur IAM afin de garantir une validation adéquate du certificat entre le serveur IAM et le Serveur d'administration.

Pour ajouter l'adresse du Serveur d'administration à la configuration du serveur IAM, procédez comme suit :

1. Récupérez la valeur du nom alternatif du sujet (SAN) à partir du certificat du Serveur d'administration commun (" C ") en exécutant la commande suivante :

   ```
   sudo openssl x509 -in /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -noout -ext subjectAltName
   ```

2. En fonction du résultat de la commande, exécutez l'une des actions suivantes :

   - Si le résultat indique que la valeur est manquante, vérifiez les **exigences relatives au certificat personnalisé**.

     Si vous utilisez un certificat personnalisé au lieu du certificat auto-signé, avant de mettre à niveau Kaspersky Security Center Linux vers une version plus récente, vous devez vous assurer que le certificat inclut le nom alternatif du sujet (SAN). Si ce n'est pas le cas, il est important de remplacer le certificat avant de mettre à niveau Kaspersky Security Center Linux. Sinon, vous ne pourrez pas vous connecter à Web Console après la mise à niveau.

     Pour vous assurer que le certificat inclut un SAN, procédez comme suit :

     1. Sur l'appareil sur lequel le Serveur d'administration est installé, exécutez la commande suivante :

        - Pour un appareil fonctionnant sous Linux :

          ```
          sudo openssl x509 -in
          /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -noout -ext
          subjectAltName
          ```

- Pour un appareil fonctionnant sous Windows :

  ```
  certutil -dump %ProgramData%\KasperskyLab\adminkit\1093\cert\klserver.cer
  ```

2. Assurez-vous que le nom alternatif du sujet (SAN) figure dans la sortie de la commande et qu'il contient l'adresse de l'appareil du Serveur d'administration.

3. Si le nom alternatif du sujet est absent, utilisez l'utilitaire klsetsrvcert pour remplacer votre certificat utilisateur par un certificat conforme aux exigences.

S'il ne répond pas aux exigences, remplacez le certificat commun du Serveur d'administration sur l'ancien Serveur d'administration à l'aide de l'utilitaire klsetsrvcert. Ensuite, répétez la procédure de mise à niveau, de déplacement ou de migration.

- Si la valeur contient des noms DNS ou des adresses de bouclage (127.0.0.1 et/ou 0:0:0:0:0:0:0:1), utilisez l'un d'entre eux dans le fichier de configuration. Il est conseillé d'utiliser l'adresse 127.0.0.1.

3. Ajoutez l'une des valeurs d'adresse SAN du certificat commun du Serveur d'administration au bloc `server_iam` du fichier de configuration du serveur IAM au format suivant : `ksc_address: "<SAN_address>"`.

   Vous pouvez modifier le fichier de configuration du serveur IAM à l'aide d'un éditeur de texte, par exemple vi. La commande suivante ouvre le fichier dans l'éditeur de texte vi :

   ```
   vi /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml
   ```

   Exemple du bloc server_iam dans le fichier de configuration du serveur IAM :

   ```
   server_iam:
       iam_address: "ksc.example.com"
       server_display_name: "ksc.example.com"
       ksc_address: "oldksc.example.internal"
       ksc_ca: "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
   ```

   Veillez à utiliser le même espacement que dans l'exemple.

4. Assurez-vous que le nom de réseau indiqué dans le paramètre `ksc_address` se résout en adresse de bouclage (127.0.0.1 ou 0:0:0:0:0:0:0:1) du Serveur d'administration. Pour ce faire, vous pouvez utiliser l'utilitaire Ping sur le Serveur d'administration.

   Si l'adresse autorisée est différente ou si l'adresse ne peut pas être résolue, ajoutez une ligne au fichier hosts sur le Serveur d'administration.

5. Redémarrez le service du serveur IAM pour appliquer les modifications de configuration en exécutant la commande suivante :

   ```
   sudo systemctl restart kliam_srv.service
   ```

L'adresse du Serveur d'administration est ajoutée au fichier de configuration du serveur IAM à partir du certificat commun du Serveur d'administration.

Elimination des défaillances

La présence sur le réseau de plusieurs Serveurs d'administration portant le même nom de réseau, ainsi que des problèmes de configuration du serveur IAM, peuvent entraîner des erreurs lors de la connexion à Web Console. Le tableau ci-dessous présente les erreurs possibles et leurs solutions.

Erreur	Description	Solution
Votre demande ne peut pas être traitée pour le moment. Veuillez patienter, puis réessayer.	Outre le processus d'initialisation des données après la mise à niveau ou la restauration de Kaspersky Security Center Linux, cette erreur peut se produire si la connexion au Serveur d'administration via l'adresse réseau indiquée échoue.	Vérifiez que l'adresse indiquée correspond bien à l'adresse IP du Serveur d'administration actuel.
Le Serveur d'administration utilise un certificat non approuvé. Veuillez reconfigurer l'application en indiquant un certificat valide, ou contactez l'administrateur principal.	Cette erreur peut se produire si la valeur d'adresse indiquée dans le fichier de configuration du serveur IAM ne correspond pas à celle figurant dans l'attribut Nom alternatif du sujet (SAN) du certificat commun du Serveur d'administration.	Suivez les instructions ci-dessus.
Le nom d'utilisateur ou le mot de passe est incorrect.	Outre dans le cas d'identifiants incorrects, cette erreur peut se produire si un autre Serveur d'administration portant le même nom existe sur le réseau.	Vérifiez que l'adresse indiquée correspond bien à l'adresse IP du Serveur d'administration actuel.

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). JavaScript doit être activé dans votre navigateur.

Vous pouvez vous connecter à Kaspersky Security Center Web Console à l'aide des méthodes suivantes :

- En utilisant l'authentification de domaine (authentification unique)

  Ce mode est utilisé pour sécuriser l'authentification des instances de Kaspersky Security Center Web Console connectées aux versions 16 et ultérieures du Serveur d'administration. Si vous souhaitez utiliser l'authentification du domaine, vous devez spécifier des paramètres supplémentaires d'interaction avec le Gestionnaire des identités et des accès (IAM) lors de l'installation de Kaspersky Security Center Web Console.

- En indiquant le nom et le mot de passe de l'utilisateur du domaine

  Avant de vous connecter avec un compte d'utilisateur de domaine, sondez le contrôleur de domaine pour obtenir la liste des utilisateurs du domaine. Ensuite, il faut indiquer le nom d'utilisateur et le mot de passe du domaine pour se connecter au Serveur d'administration. Cette méthode est prise en charge pour l'authentification uniquement via Microsoft Active Directory.

- En indiquant le nom et le mot de passe de l'utilisateur interne

Le compte utilisateur sous lequel vous voulez vous connecter à Kaspersky Security Center Web Console doit avoir un rôle attribué. Avant de vous connecter, assurez-vous qu'un rôle a été attribué au domaine ou au compte utilisateur interne. Dans le cas contraire, une erreur de connexion se produira.

Se connecter en utilisant l'authentification de domaine (authentification unique)

Pour vous connecter à Kaspersky Security Center Web Console à l'aide de l'authentification de domaine :

1. Dans votre navigateur, accédez à l'adresse https://`<Adresse de Kaspersky Security Center Web Console>`:`<Numéro de port>`.

   La page de sélection du Serveur d'administration s'affiche.

2. Si vous avez ajouté plusieurs serveurs de confiance, dans la liste des Serveurs d'administration, sélectionnez le Serveur d'administration auquel vous souhaitez vous connecter.

   Si vous n'avez ajouté qu'un seul Serveur d'administration, la liste des Serveurs d'administration n'est pas affiché.

   Le navigateur est redirigé vers https://`<adresse du Serveur d'administration>`:4444.

3. Configurez l'authentification de domaine Kerberos.

4. Exécutez une des actions suivantes :

   - Cliquez sur le bouton **Utiliser l'authentification du domaine**.

   - Si un ou plusieurs Serveurs d'administration virtuels sont créés sur le Serveur et que vous souhaitez vous connecter à un Serveur virtuel, en utilisant l'authentification de domaine :

     a. Cliquez sur **Afficher les options du Serveur virtuel**.

     b. Saisissez le nom du Serveur d'administration virtuel que vous avez indiqué lors de la création du Serveur virtuel.

     c. Cliquez sur le bouton **Utiliser l'authentification du domaine**.

5. Spécifiez un code de sécurité à usage unique généré à l'aide de l'application d'authentification de l'appareil mobile.

   Lors de la première connexion, configurez l'authentification en deux étapes pour votre compte. Si vous n'avez pas accès à la configuration de l'authentification à deux facteurs, contactez un utilisateur disposant du droit Modifier les ACL des objets dans la zone fonctionnelle **Fonctions générales** : **Autorisations d'utilisateur** et de l'authentification à deux facteurs configurée pour ajouter votre compte à la liste d'autorisation pour l'authentification à deux facteurs.

Après la connexion, la page d'accueil de Kaspersky Security Center Web Console s'affiche. Elle contient la langue et le thème que vous avez utilisés la dernière fois. Vous pouvez naviguer dans Kaspersky Security Center Web Console et l'utiliser avec Kaspersky Security Center Linux.

Connexion à l'aide du nom d'utilisateur et du mot de passe du domaine ou de l'utilisateur interne

Pour se connecter à Kaspersky Security Center Web Console en spécifiant le nom d'utilisateur et le mot de passe, procédez comme suit :

1. Dans votre navigateur, accédez à l'adresse https://`<Adresse de Kaspersky Security Center Web Console>`:`<Numéro de port>`.

   La page de sélection du Serveur d'administration s'affiche.

2. Si vous avez ajouté plusieurs serveurs de confiance, dans la liste des Serveurs d'administration, sélectionnez le Serveur d'administration auquel vous souhaitez vous connecter.

   Si vous n'avez ajouté qu'un seul Serveur d'administration, la liste des Serveurs d'administration n'est pas affiché.

   Le navigateur est redirigé vers https://`<adresse du Serveur d'administration>`:4444.

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 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**.

5. Spécifiez un code de sécurité à usage unique généré à l'aide de l'application d'authentification de l'appareil mobile.

   Lors de la première connexion, configurez l'authentification en deux étapes pour votre compte. Si vous n'avez pas accès à la configuration de l'authentification à deux facteurs, contactez un utilisateur disposant du droit Modifier les ACL des objets dans la zone fonctionnelle **Fonctions générales** : **Autorisations d'utilisateur** et de l'authentification à deux facteurs configurée pour ajouter votre compte à la liste d'autorisation pour l'authentification à deux facteurs.

6. Si la modification forcée du mot de passe est activée pour votre compte ou si votre mot de passe a expiré, la fenêtre de modification du mot de passe s'affiche. Définissez un nouveau mot de passe pour vous connecter à Kaspersky Security Center Web Console.

Après la connexion, la page d'accueil de Kaspersky Security Center Web Console s'affiche. Elle contient la langue et le thème que vous avez utilisés 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 volet supérieur, accédez au menu de votre compte en cliquant sur le nom de votre compte, puis sélectionnez **Se déconnecter**.

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

Interface de Kaspersky Security Center Web Console

L'administration de Kaspersky Security Center Linux s'opère via l'interface de Kaspersky Security Center Web Console.

La fenêtre de Kaspersky Security Center Web Console contient les éléments suivants :

- Menu principal dans la partie gauche de la fenêtre
- Volet supérieur dans la partie supérieure de la fenêtre
- Zone de travail dans la partie droite de la fenêtre

Menu principal

Le menu principal contient les sections suivantes :

- **Serveur d'administration**. Affiche le nom du Serveur d'administration auquel vous êtes actuellement connecté. Pour ouvrir les propriétés du Serveur d'administration, cliquez sur le nom du Serveur d'administration.
- **Navigation dans la console**. Affiche la carte du menu principal. La plupart des sections affichées peuvent être ajoutées à des favoris ou définies comme page d'accueil. Par défaut, les **Navigation dans la console** sont définis comme page d'accueil. Vous pouvez modifier ces paramètres.
- **Surveillance**. Fournit une vue d'ensemble de votre infrastructure, des états de la protection et des statistiques.
- **Gestion des ressources**. Contient les outils pour les ressources, ainsi que les tâches et les stratégies d'application de Kaspersky.
- **Utilisateurs et rôles**. Permet d'administrer les utilisateurs et les rôles, de configurer les privilèges des utilisateurs en attribuant des rôles aux utilisateurs et d'associer des profils de stratégie à des rôles.
- **Opérations**. Contient diverses opérations, y compris les licences des applications, l'affichage et la gestion des disques chiffrés et des événements de chiffrement, ainsi que l'administration des applications tierces. Cela vous permet également d'accéder aux stockages d'applications.
- **Découverte et déploiement**. Permet de sonder le réseau à la recherche d'appareils clients et de distribuer les appareils aux groupes d'administration manuellement ou automatiquement. Cette section contient également l'assistant de démarrage rapide de l'application et l'assistant de déploiement de la protection.
- **Place de marché**. Contient des informations sur l'ensemble des solutions d'entreprise de Kaspersky et vous permet de sélectionner celles dont vous avez besoin, puis de procéder à l'achat de ces solutions sur le site de Kaspersky.
- **Paramètres**. Permet de sauvegarder l'état actuel d'un plug-in Web pour pouvoir restaurer l'état enregistré ultérieurement. Contient vos paramètres personnels liés à l'apparence de l'interface, tels que la langue de l'interface ou le thème.

Si nécessaire, vous pouvez réduire le menu principal à des icônes en cliquant sur le chevron (<<) en bas de l'écran.

Volet supérieur

Le volet supérieur est toujours affiché dans toutes les sections de la console et ne peut pas être masqué.

La partie gauche du volet présente le nom et le logo de l'application. Si vous cliquez sur le nom ou le logo de l'application, la page d'accueil de Kaspersky Security Center Web Console s'ouvre.

Dans la partie droite du volet, les paramètres suivants s'affichent :

- Icône de notification (🔔). Si vous cliquez sur l'icône, un panneau avec des notifications s'ouvre.
- Le menu de votre compte. Contient un lien vers l'aide de Kaspersky Security Center Linux. Il vous permet également de vous déconnecter de Kaspersky Security Center Linux, de modifier le mot de passe de votre propre compte et d'afficher la version de Kaspersky Security Center Web Console ainsi que la liste des plug-ins Internet d'administration installés.

Zone de travail

La zone de travail affiche les informations que vous choisissez d'afficher dans les sections de la fenêtre de l'interface de Kaspersky Security Center Web Console. Il contient également des éléments de contrôle qui permettent de configurer l'affichage des informations.

> Nous vous recommandons d'utiliser un seul onglet de navigateur pour travailler avec Kaspersky Security Center Web Console.

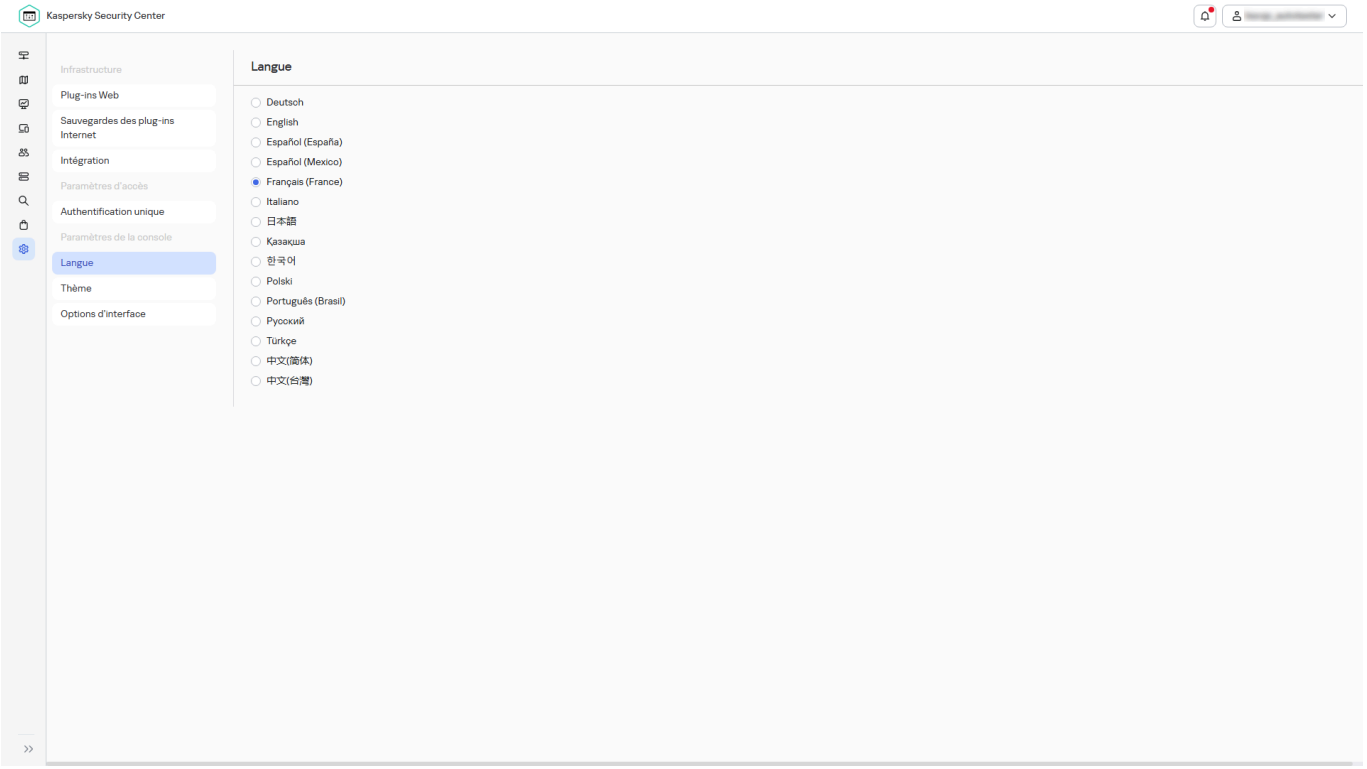
Modification de la langue de l'interface de Kaspersky Security Center Web Console

Vous pouvez sélectionner la langue de l'interface de Kaspersky Security Center Web Console.

Pour modifier la langue d'interface, procédez comme suit :

1. Dans le menu principal, accédez à **Configuration** → **Langue**.

2. Sélectionnez une des langues de localisation prises en charge.



Modification de la langue de l'interface de Kaspersky Security Center Web Console

Modification de la page d'accueil de Kaspersky Security Center Web Console

La page d'accueil s'affiche après votre connexion à Kaspersky Security Center Web Console.

Par défaut, la section **Navigation dans la console** est définie comme page d'accueil. Si nécessaire, vous pouvez modifier la page d'accueil.

Pour modifier la page d'accueil :

1. Dans la section **Navigation dans la console**, passez le curseur de la souris sur l'élément que vous souhaitez définir comme page d'accueil.

2. Une fois que l'icône d'accueil (⌂) s'affiche, cliquez sur celle-ci.

   La page d'accueil est modifiée. Un message correspondant s'affiche à l'écran. L'élément sélectionné comme page d'accueil est marqué par l'icône d'accueil (⌂).

Les sections **Place de marché** et **Configuration** ne peuvent pas être définies comme page d'accueil.

Ajout et suppression de signets

À partir de la section **Signets** dans le menu principal, vous pouvez ajouter des sections de Kaspersky Security Center Web Console à vos signets et y accéder rapidement.

Si vous n'avez ajouté aucune section aux signets, la section **Signets** ne s'affiche pas dans le menu principal.

Vous ne pouvez ajouter aux signets que les sections qui affichent des pages. Par exemple, si vous accédez à **Gestion des ressources** → **Ressources (Appareils)**, une page avec le tableau des appareils s'ouvre, ce qui signifie que vous pouvez ajouter cette section aux signets. Si une fenêtre ou aucun élément ne s'affiche après que vous avez sélectionné la section dans le menu principal, vous ne pouvez pas ajouter une telle section aux signets.

Pour ajouter une section aux signets :

1. Dans le menu principal, placez le curseur de la souris sur la section que vous souhaitez épingler.
2. Une fois que l'icône de signet ( ) s'affiche, cliquez sur celle-ci.

   La section s'affiche dans la section **Signets**.

Pour supprimer une section des signets :

1. Dans le menu principal, accédez à la section **Signets**.
2. Passez le curseur de la souris sur la section que vous souhaitez supprimer, puis cliquez sur l'icône de signet ( ).

   La section est retirée des signets.

Vous pouvez également ajouter et supprimer des sections des signets dans la section **Navigation dans la console** en passant le survolant à l'aide du curseur de la souris et en cliquant sur l'icône des signets ( ). L'élément sélectionné sera marqué par l'icône des signets ( ) et affiché dans la section **Signets** dans le menu principal. Si vous souhaitez supprimer l'élément des signets, cliquez sur l'icône des signets ( ).

La section **Signets** s'affiche uniquement dans le menu principal. Elle ne s'affiche jamais sur la page **Navigation dans la console**.

Suppression de Kaspersky Security Center Web Console

Vous devrez peut-être désinstaller Kaspersky Security Center Web Console Server (également appelé Kaspersky Security Center Web Console) dans les cas suivants :

- Restauration des données à partir d'une sauvegarde à l'aide d'un autre certificat commun.
- Réémission du certificat commun du Serveur d'administration.

- Remplacement du certificat de Web Console par un certificat personnalisé.
- Kaspersky Security Center Web Console n'est plus utilisé sur cet appareil.

Pour supprimer Kaspersky Security Center Web Console, procédez comme suit :

1. En fonction de votre distribution Linux, exécutez l'une des commandes suivantes :
   - `sudo dnf remove ksc-web-console`
   - `sudo apt remove ksc-web-console`
2. Vérifiez le résultat en exécutant la commande suivante :

   ```
   sudo systemctl status KSC*
   ```

   Kaspersky Security Center Web Console ne doit pas apparaître dans le résultat de la commande.

Si vous souhaitez restaurer Kaspersky Security Center Web Console, installez-le sur l'appareil comme indiqué dans l'article : Installation de Kaspersky Security Center Web Console.

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 **Ressources (Appareils)** 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.

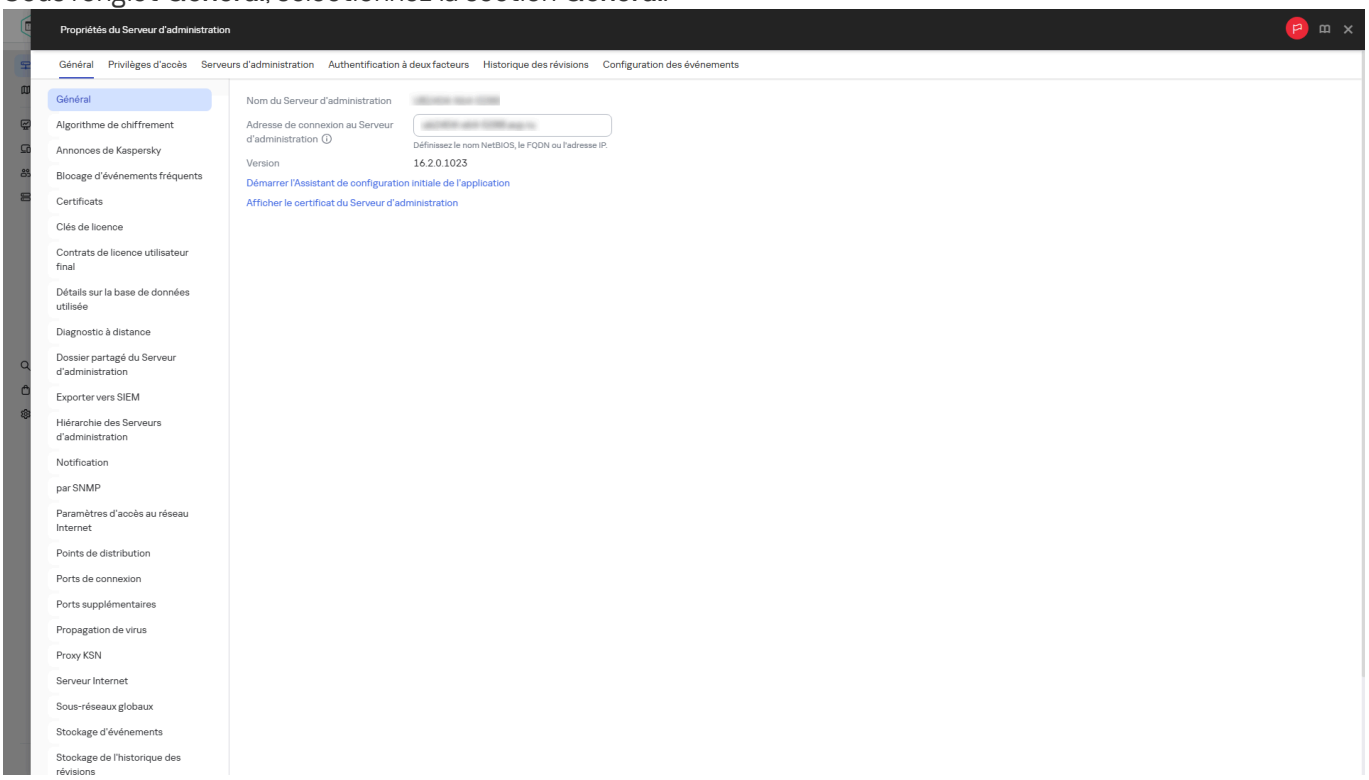
L'application vous invite automatiquement à lancer l'Assistant de configuration initiale de l'application après l'installation du Serveur d'administration, lors de la première connexion au Serveur d'administration. Vous pouvez aussi lancer l'Assistant de configuration initiale de l'application manuellement à tout moment.

Pour lancer manuellement l'Assistant de configuration initiale de l'application, procédez comme suit :

1. Dans le menu principal, cliquez sur le nom du Serveur d'administration.

   La fenêtre des propriétés du Serveur d'administration s'ouvre.

2. Sous l'onglet **Général**, sélectionnez la section **Général**.



Fenêtre des propriétés du Serveur d'administration

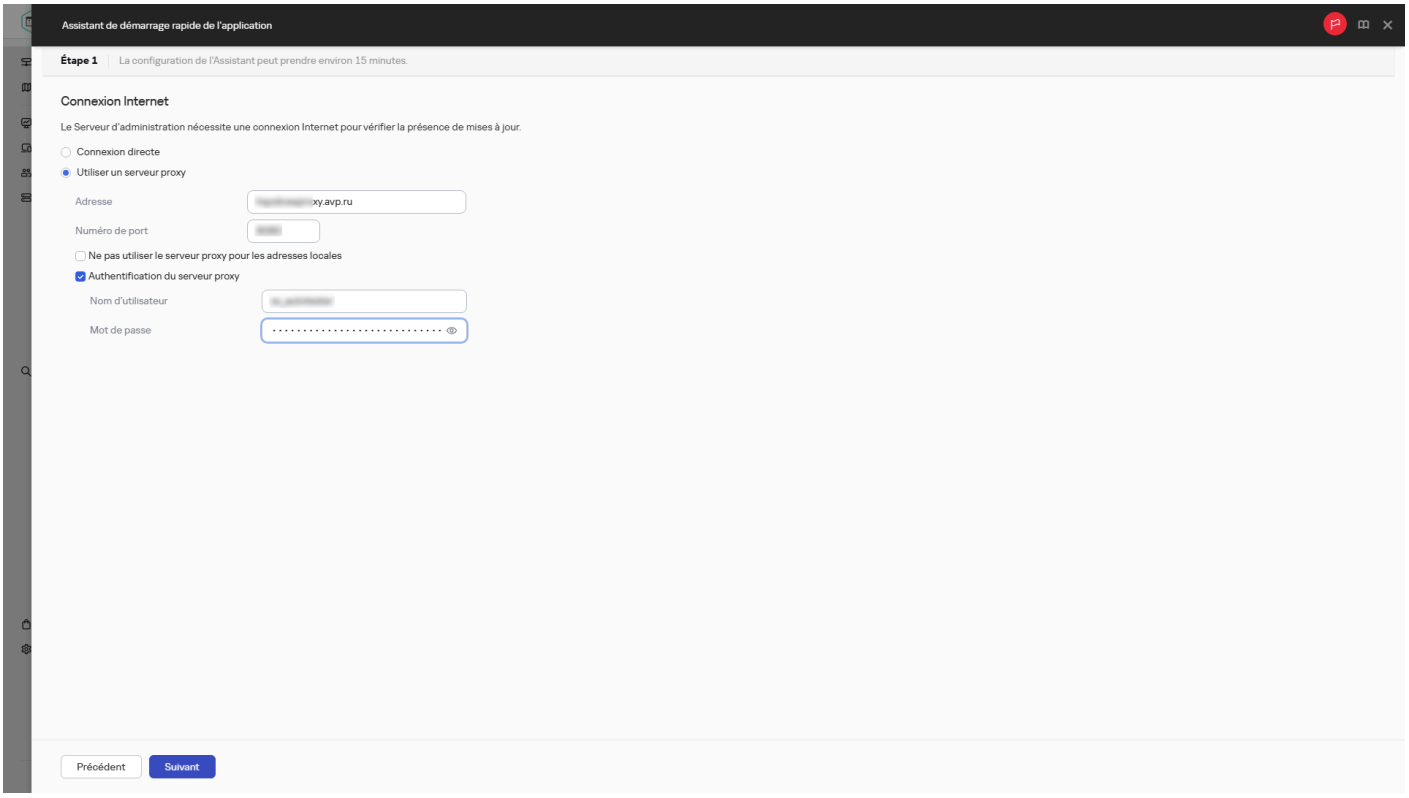
3. Cliquez sur **Démarrer l'Assistant de configuration initiale de l'application**.

L'Assistant propose de réaliser la configuration initiale du Serveur d'administration. Suivez les étapes 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 :



Paramètres de connexion à Internet

- **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**

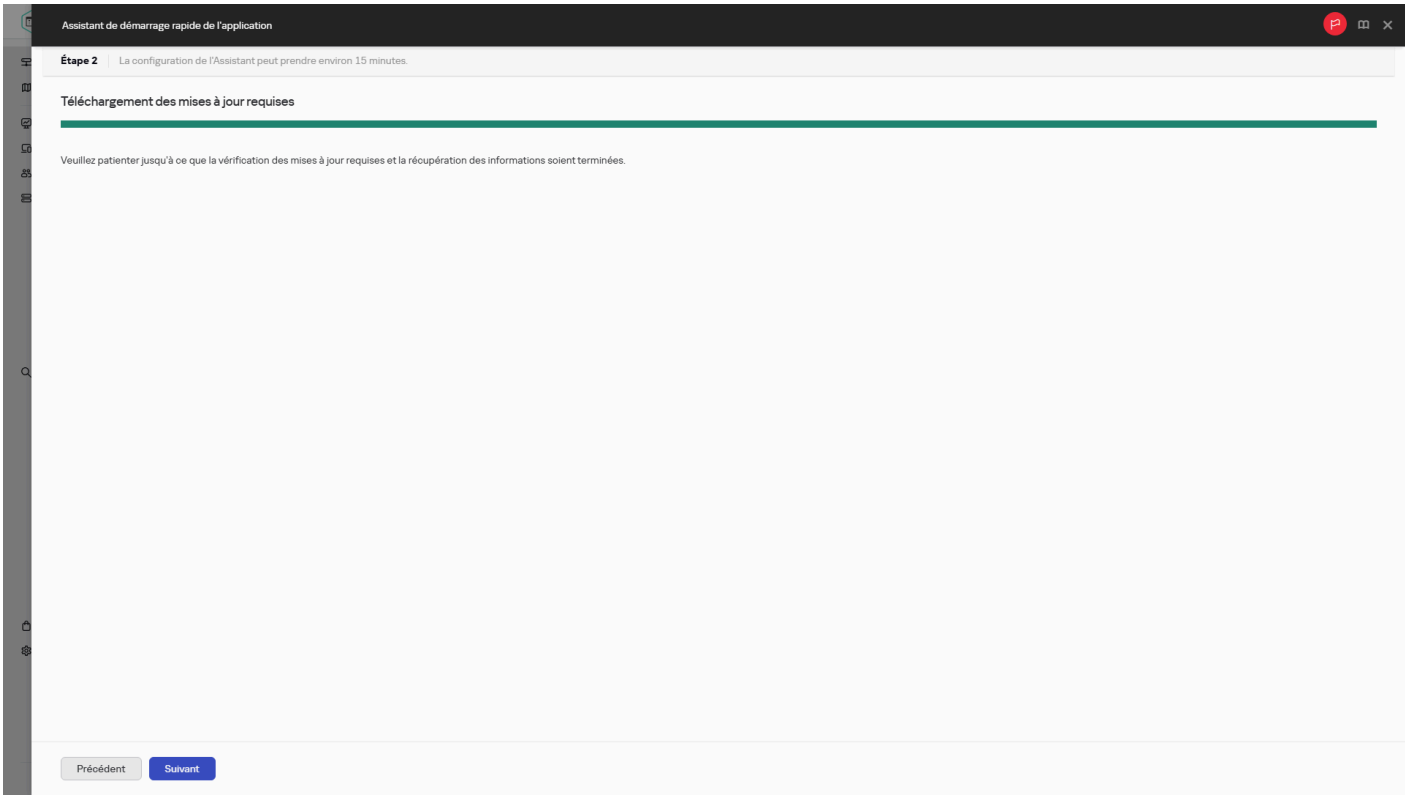
  Mot de passe défini par l'utilisateur sous le compte duquel la connexion au serveur proxy est établie (ce champ est disponible si la case **Authentification du serveur proxy** est cochée).

  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

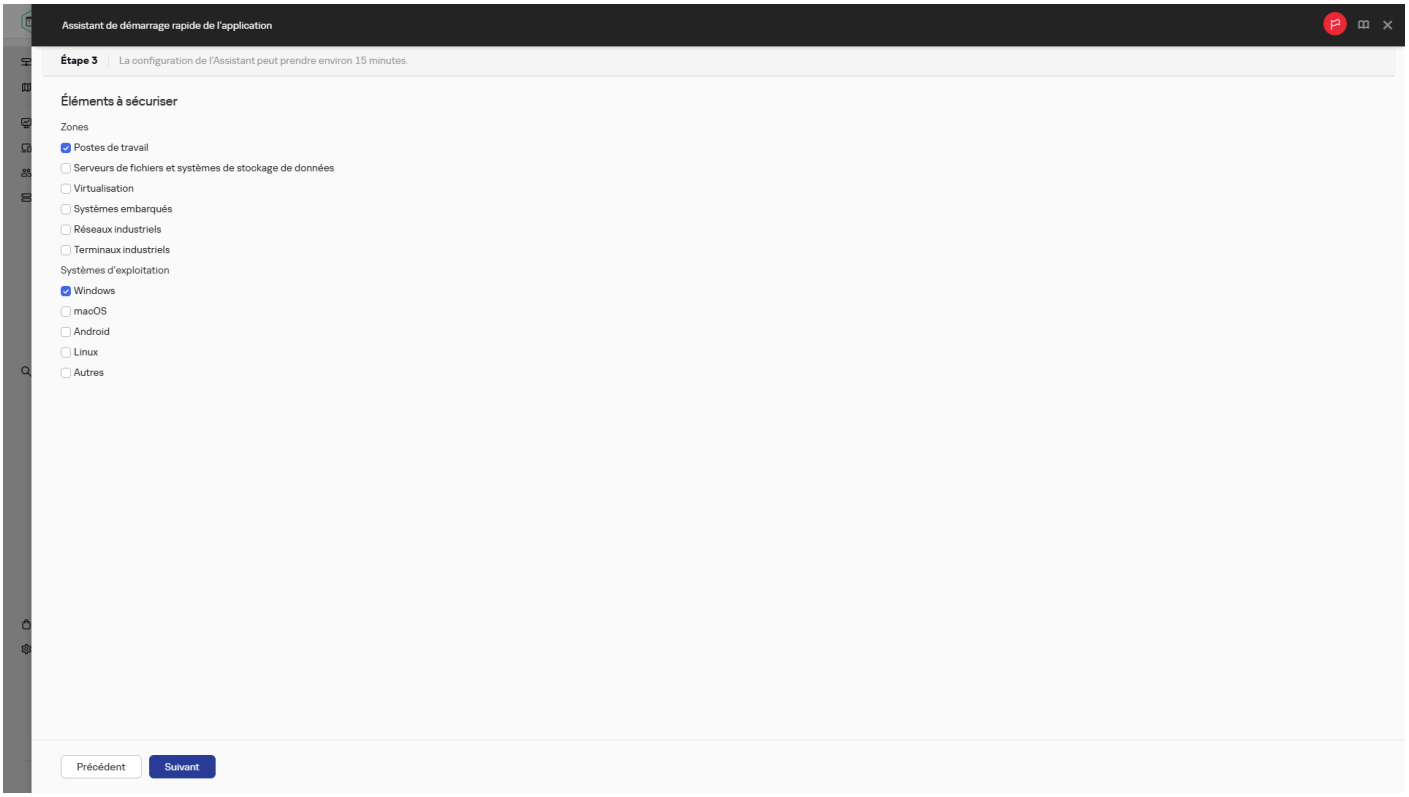
Les mises à jour requises sont automatiquement téléchargées des serveurs Kaspersky.



Téléchargement des mises à jour requises

Étape 3. Sélection des actifs à sécuriser

Sélectionnez les zones de protection et les systèmes d'exploitation utilisés sur votre réseau. Lorsque vous sélectionnez ces options, vous spécifiez les filtres pour les plug-ins d'administration des applications et les paquets de distribution sur les serveurs Kaspersky que vous pouvez télécharger pour les installer sur les appareils clients de votre réseau.



Sélection des actifs à sécuriser

Sélectionnez les options :

- **Zone**

  Vous pouvez sélectionner les zones de protection suivantes :

  - **Postes de travail**
  - **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.

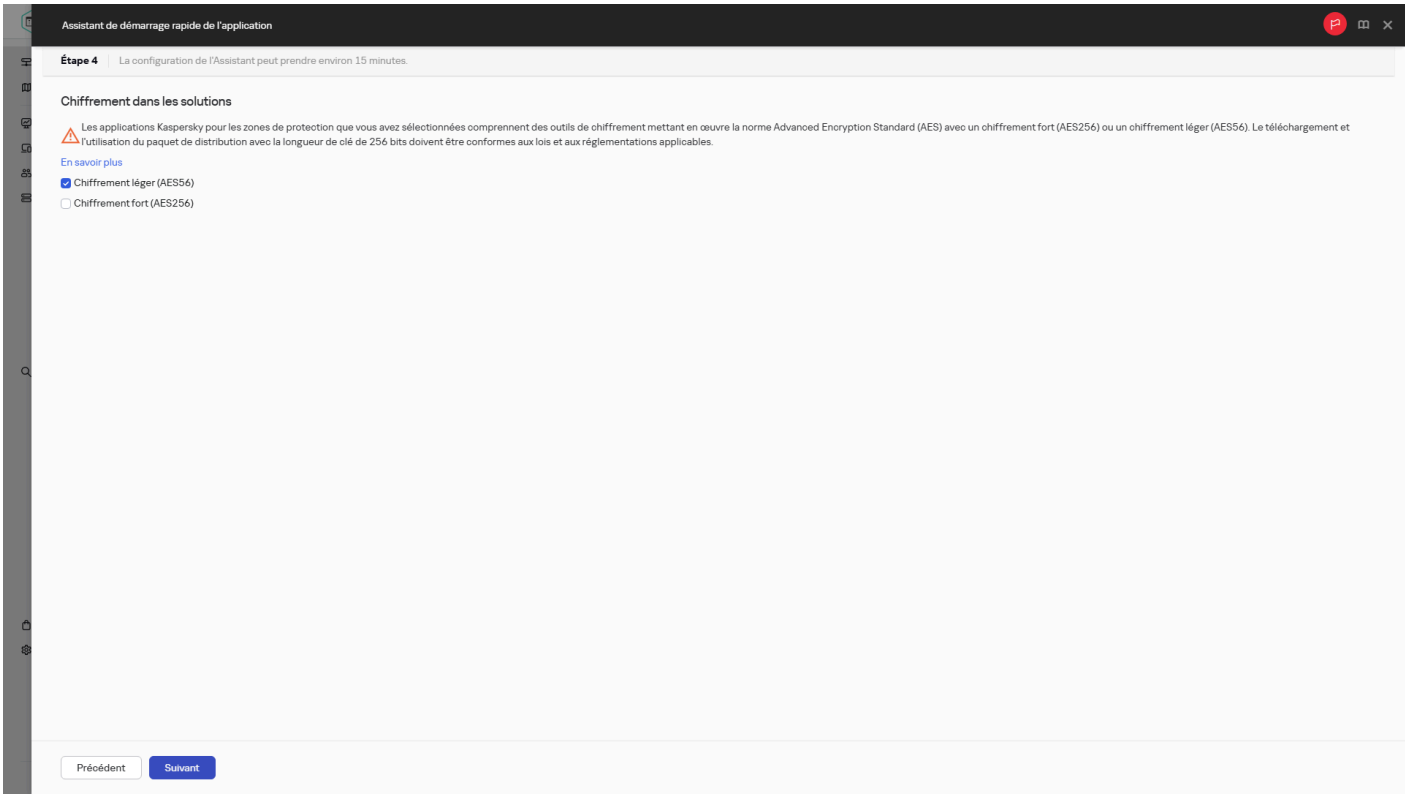
Vous pouvez sélectionner les paquets de l'application Kaspersky dans la liste des paquets disponibles ultérieurement, indépendamment de l'Assistant de configuration initiale de l'application. Pour simplifier la recherche des paquets requis, vous pouvez filtrer la liste des packages disponibles selon 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.



Sélection du chiffrement dans les solutions

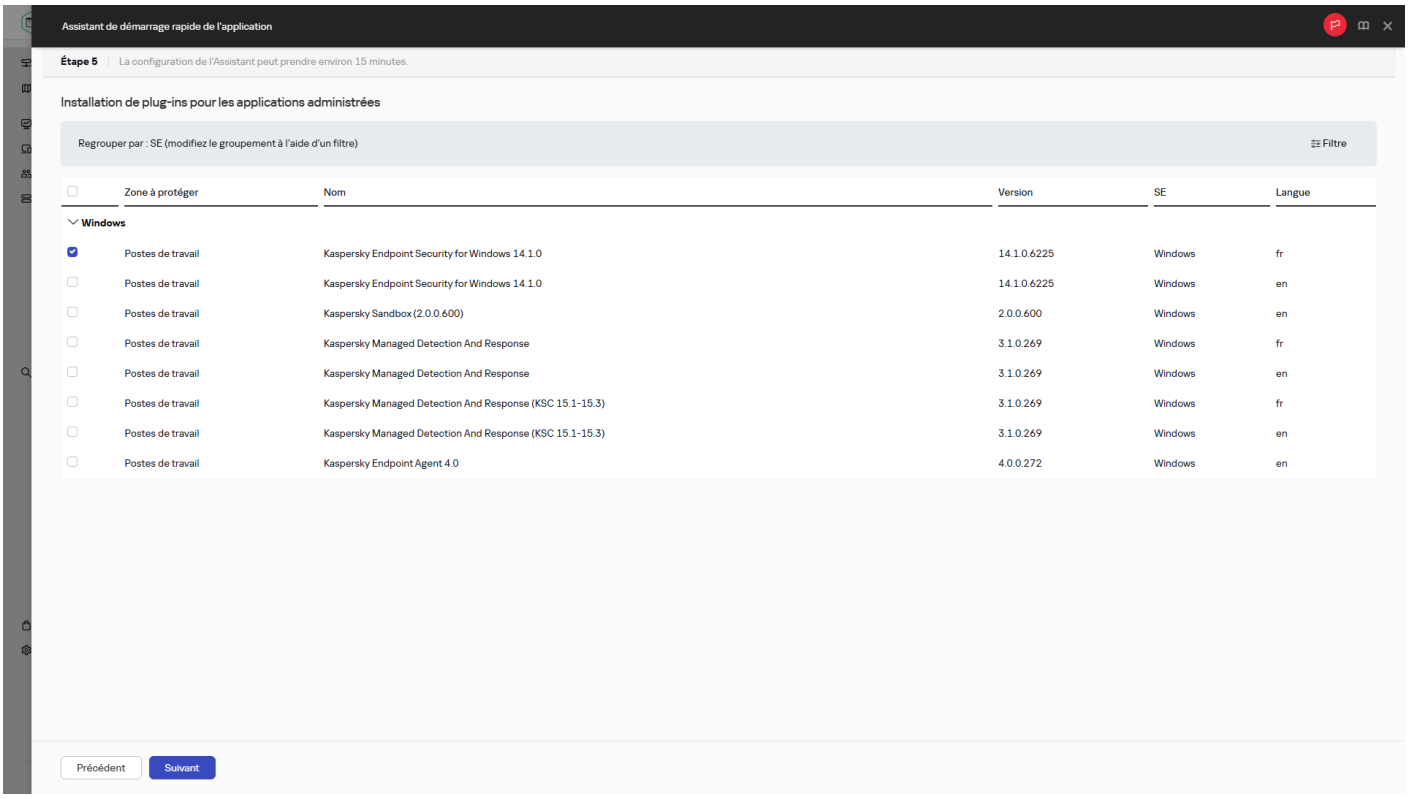
Dans la fenêtre **Chiffrement dans les solutions**, sélectionnez l'un des types de chiffrement suivants :

- Chiffrement léger. Ce type de chiffrement utilise une longueur de clé de 56 bits.
- Chiffrement fort. Ce type de chiffrement utilise une longueur de clé de 256 bits.

Vous pouvez sélectionner le paquet de distribution de Kaspersky Endpoint Security for Windows avec le type de chiffrement requis ultérieurement, indépendamment de l'Assistant de configuration initiale de l'application.

Étape 5. Configuration de l'installation de plug-ins pour les applications administrées

Sélectionnez les plug-ins pour les applications administrées à installer. Une liste des plug-ins situés sur les serveurs de Kaspersky s'affiche. La liste est filtrée selon les options sélectionnées à l'étape précédente de l'Assistant. Par défaut, une liste complète comprend des plug-ins dans toutes les langues. Pour afficher uniquement le plug-in dans une langue en particulier, utilisez le filtre.



Installation de plug-ins pour les applications administrées

La liste des plug-ins comprend les colonnes suivantes :

- **Zone à protéger**

  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.

- **SE**

  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.

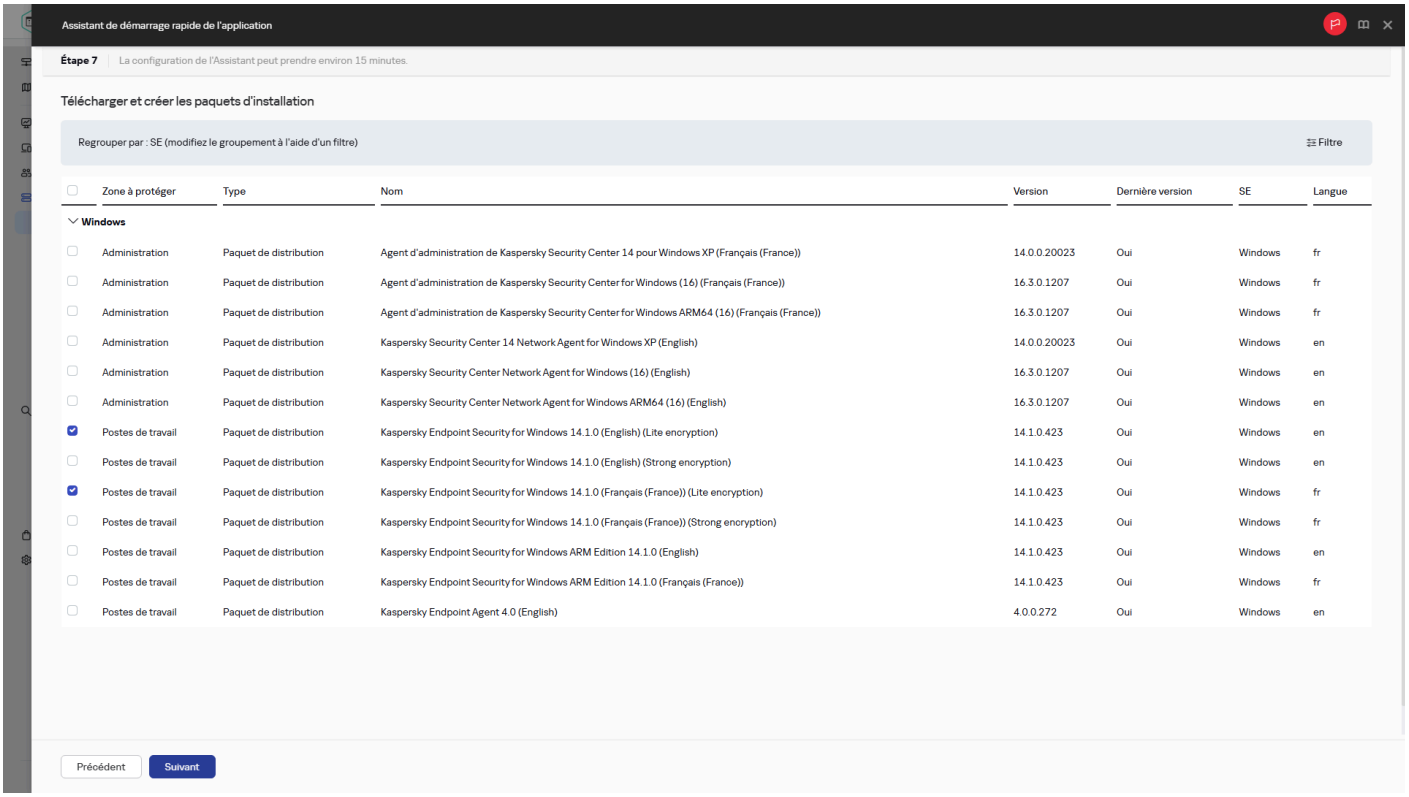
Lorsque tous les plug-ins sélectionnés sont installés, l'Assistant de configuration initiale de l'application vous amène automatiquement à l'étape suivante.

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.



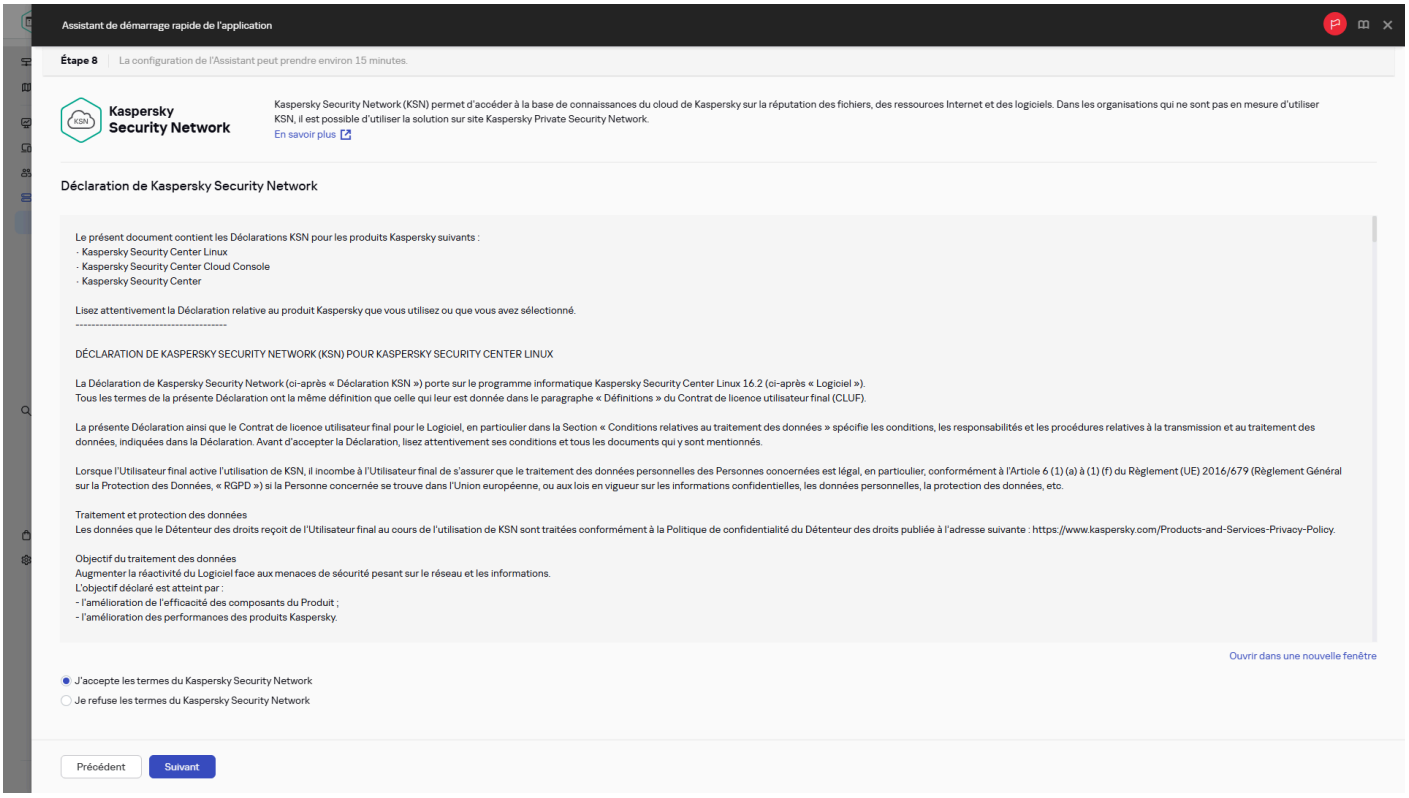
Téléchargement des paquets de distribution et création des paquets d'installation

Pour terminer le téléchargement de certains paquets de distribution, vous devez accepter le CLUF. Lorsque vous cliquez sur le bouton **Accepter**, le texte du CLUF s'affiche. Pour passer à l'étape suivante de l'Assistant, vous devez accepter les termes et conditions du CLUF et les termes et conditions de la politique de confidentialité de Kaspersky. Si vous n'acceptez pas les termes et conditions, le téléchargement du paquet est annulé.

Une fois que vous avez accepté les termes et conditions du CLUF et les termes et conditions de la politique de confidentialité de Kaspersky, le téléchargement des paquets de distribution se poursuit. Par la suite, vous pouvez utiliser les paquets d'installation pour déployer des applications Kaspersky sur les appareils clients.

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.



Configuration 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**

  Un *code d'activation* est une suite unique de vingt caractères composés de lettres latines et de chiffres. 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 d'un code d'activation, vous avez besoin d'un accès Internet afin de 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** 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.

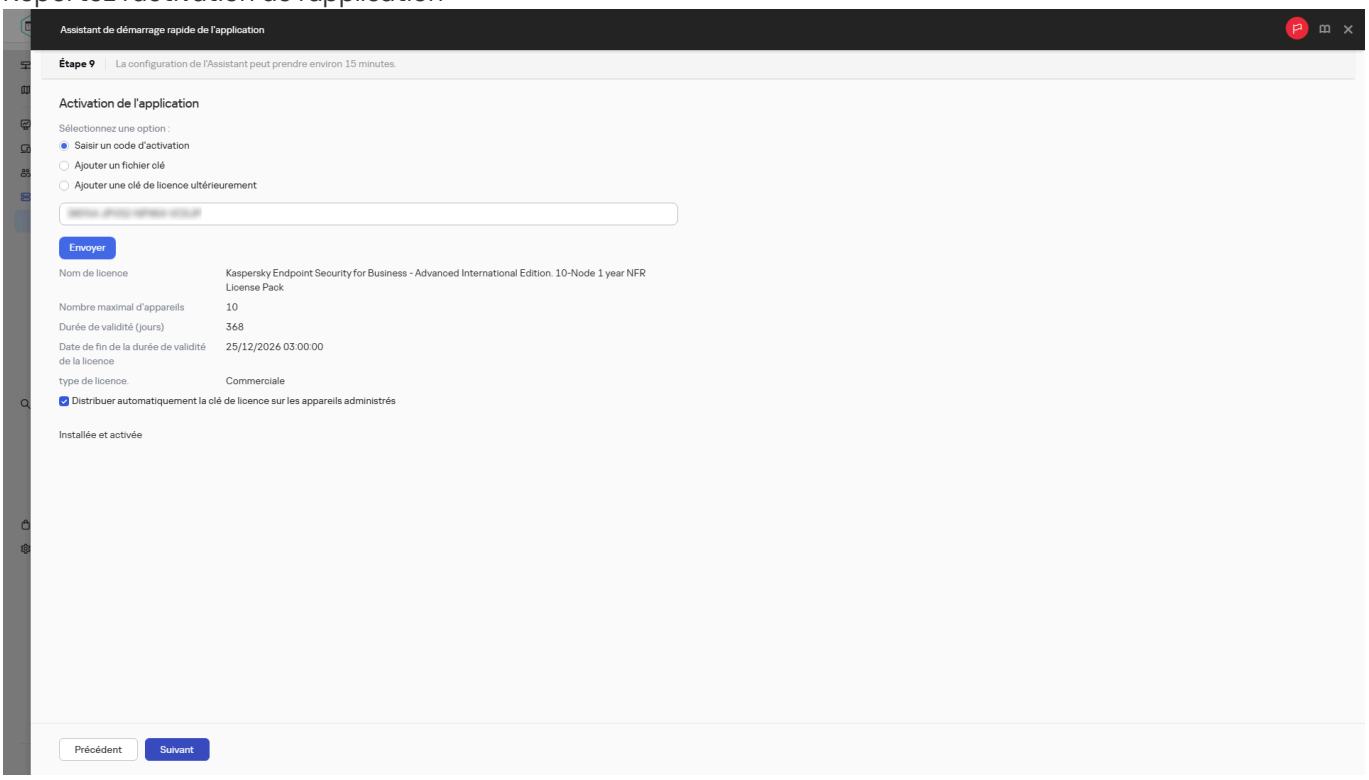
  L'activation de l'application à l'aide d'un fichier clé ne requiert pas de connexion aux serveurs d'activation de Kaspersky.

  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** du menu principal.

- Reportez l'activation de l'application



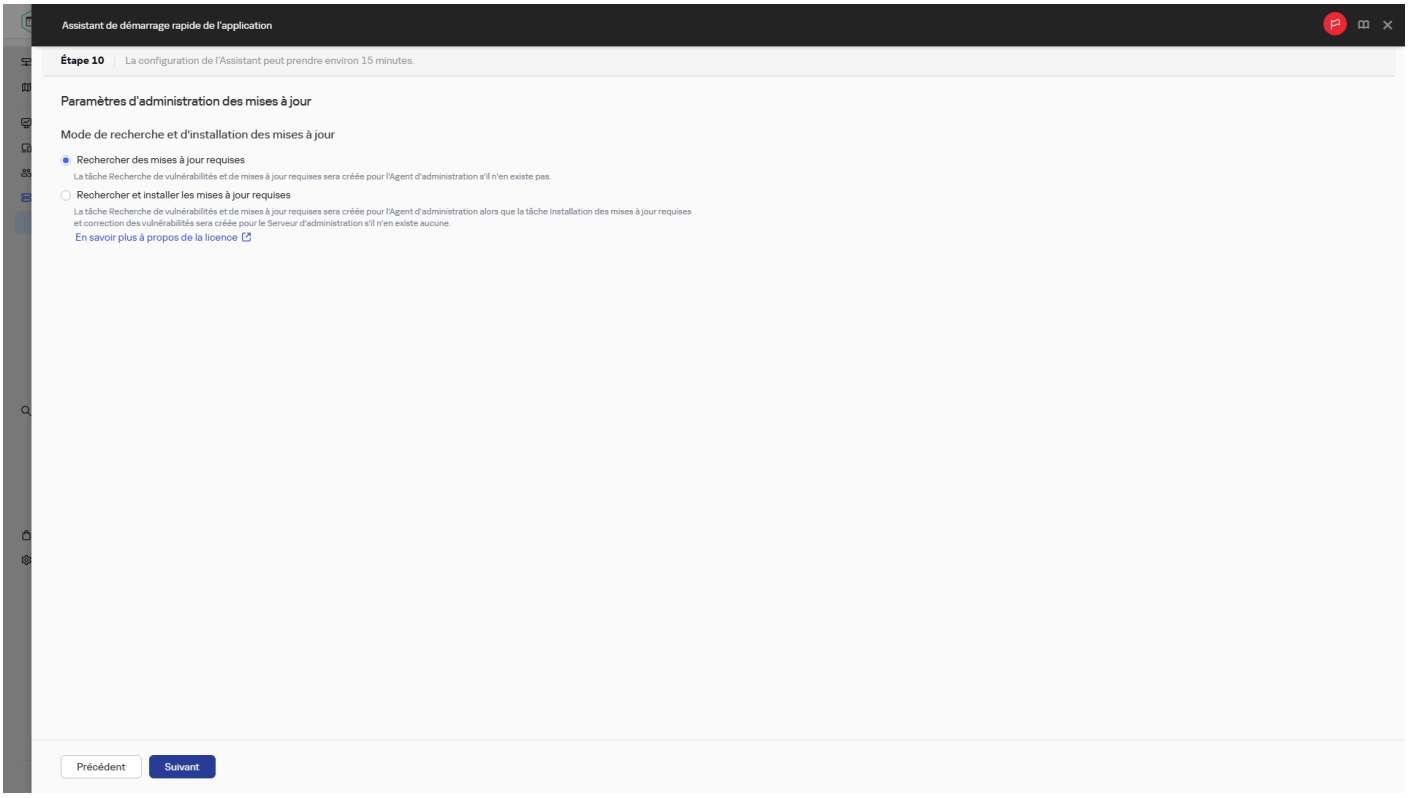
Sélection de la méthode d'activation de l'application

Si vous avez choisi l'activation reportée de l'application, vous pouvez ajouter une clé de licence plus tard à tout moment en sélectionnant **Opérations** → **Licence**.

Lors de l'utilisation de Kaspersky Security Center, déployé depuis une image AMI payante ou pour un SKU facturé mensuellement en fonction de l'utilisation, il est impossible d'ajouter un fichier clé ou de saisir un code.

Étape 9. Spécification des paramètres de gestion des mises à jour tierces

L'étape **Paramètres d'administration des mises à jour** de l'Assistant de configuration initiale de l'application ne s'affiche pas si vous ne disposez pas de licence pour le fonctionnement de Gestion des vulnérabilités et des correctifs et si la tâche *Recherche de vulnérabilités et de mises à jour requises* existe déjà.



Paramètres de gestion des mises à jour tierces

Pour les mises à jour logicielles tierces, sélectionnez l'une des options suivantes :

- **Rechercher des mises à jour requises**

  La tâche *Recherche de vulnérabilités et de mises à jour requises* est créée automatiquement, si vous n'en avez pas.

  Par défaut, cette option est sélectionnée.

- **Rechercher et installer les mises à jour requises**

  Les tâches *Recherche de vulnérabilités et de mises à jour requises* et *Installation des mises à jour requises et correction des vulnérabilités* sont créées automatiquement, si vous n'en avez pas.

  Cette option est accessible uniquement en présence d'une licence pour le fonctionnement de Gestion des vulnérabilités et des correctifs.

Pour les mises à jour Windows Update, sélectionnez **Utiliser des sources de mise à jour définies dans la stratégie de domaine.**

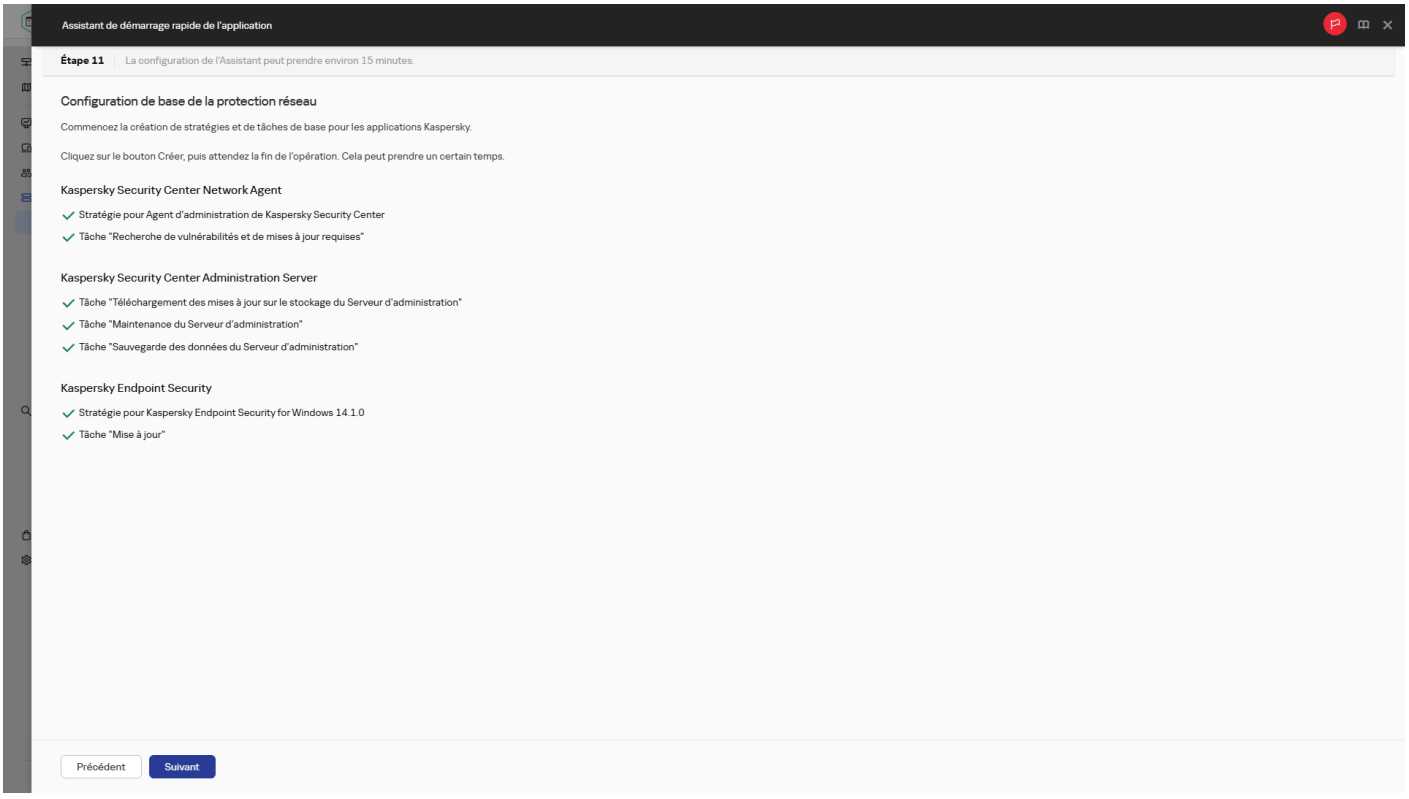
Les appareils clients téléchargent les mises à jour de Windows Update en fonction des paramètres de stratégie de votre domaine. La stratégie d'Agent d'administration est créée automatiquement si vous n'en avez pas.

Vous pouvez créer les tâches *Recherche de vulnérabilités et de mises à jour requises* et *Installation des mises à jour requises et correction des vulnérabilités* séparément de l'assistant de démarrage rapide.

Étape 10. Création de la configuration de base de la protection d'un réseau

Vous pouvez consulter une liste de stratégies et de tâches créées.

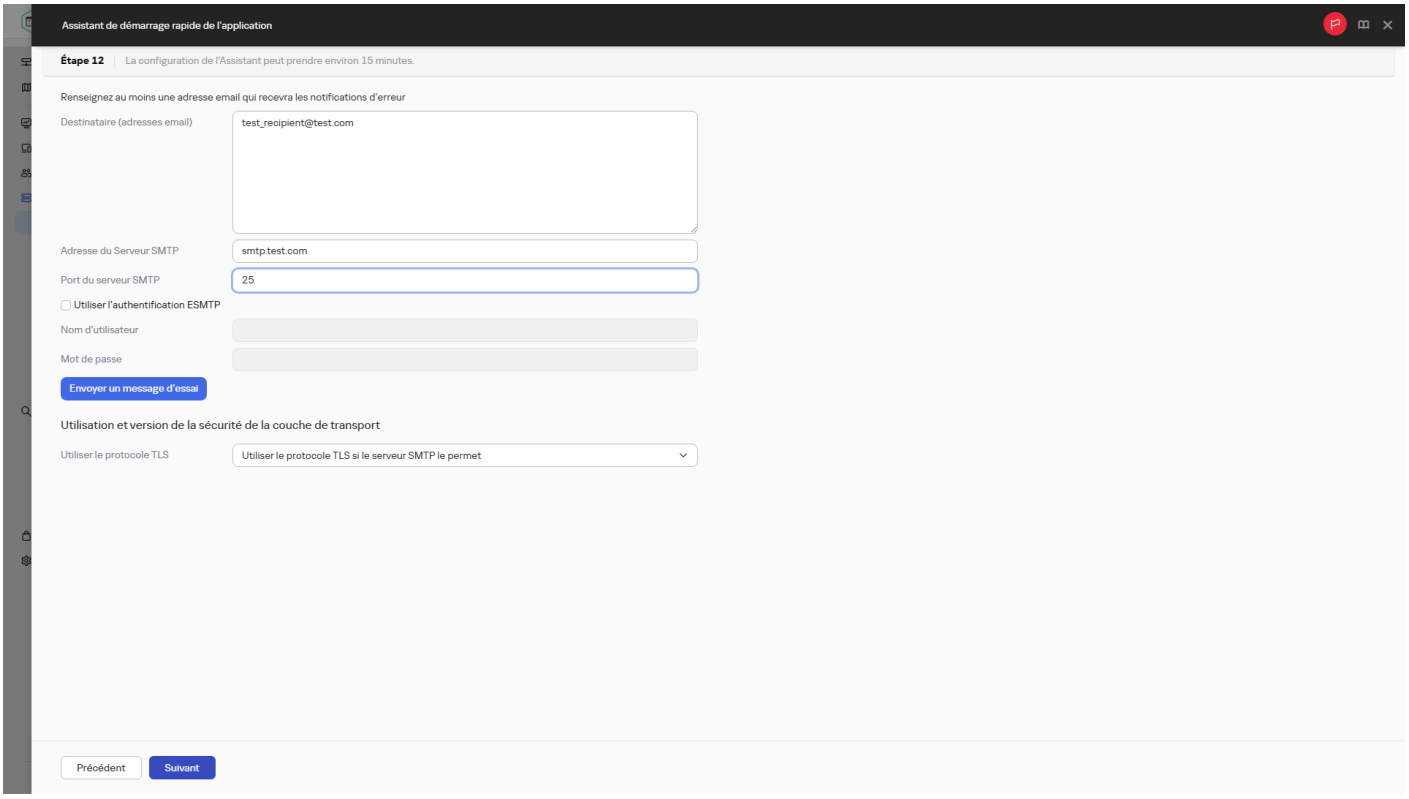
Avant de passer à l'étape suivante de l'Assistant, attendez la fin de la création des stratégies et des tâches.



Création de la configuration de base de la protection d'un réseau

Étape 11. Configuration des notifications par email

Configurez l'envoi des notifications sur les événements enregistrés lors du travail avec les applications de Kaspersky sur les appareils clients. Ces paramètres seront utilisés comme paramètres par défaut pour les stratégies d'applications.



Configuration des notifications par email

Pour configurer la diffusion des notifications relatives aux événements qui surviennent dans les applications de Kaspersky, utilisez les paramètres suivants :

- **Destinataire (adresses email)**

  Les adresses email des utilisateurs auxquels l'application va envoyer les notifications. Vous pouvez spécifier une ou plusieurs adresses. 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.

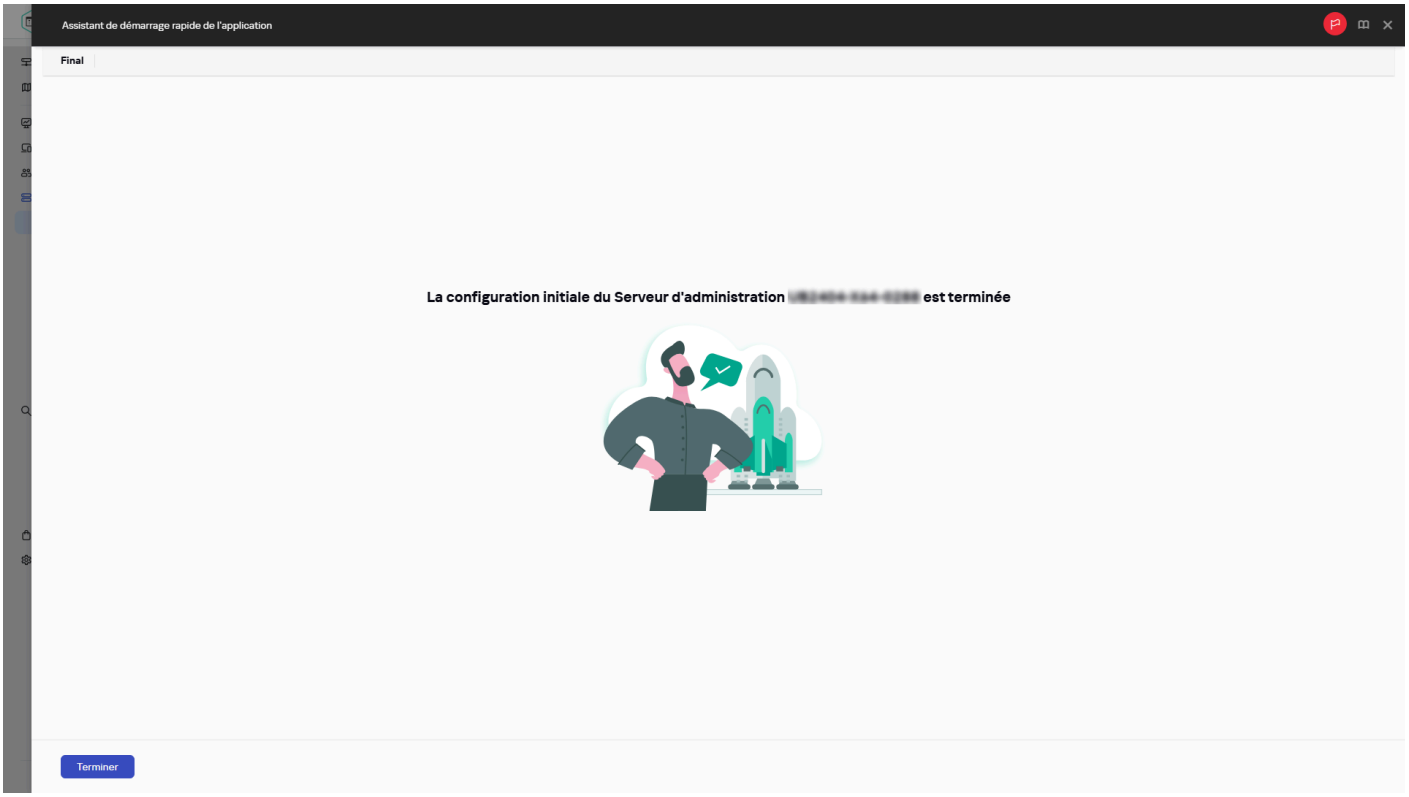
- **Utiliser l'authentification ESMTP**

  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 12. Fin de l'Assistant de configuration initiale de l'application

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



Dernière étape de l'Assistant de configuration initiale de l'application

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

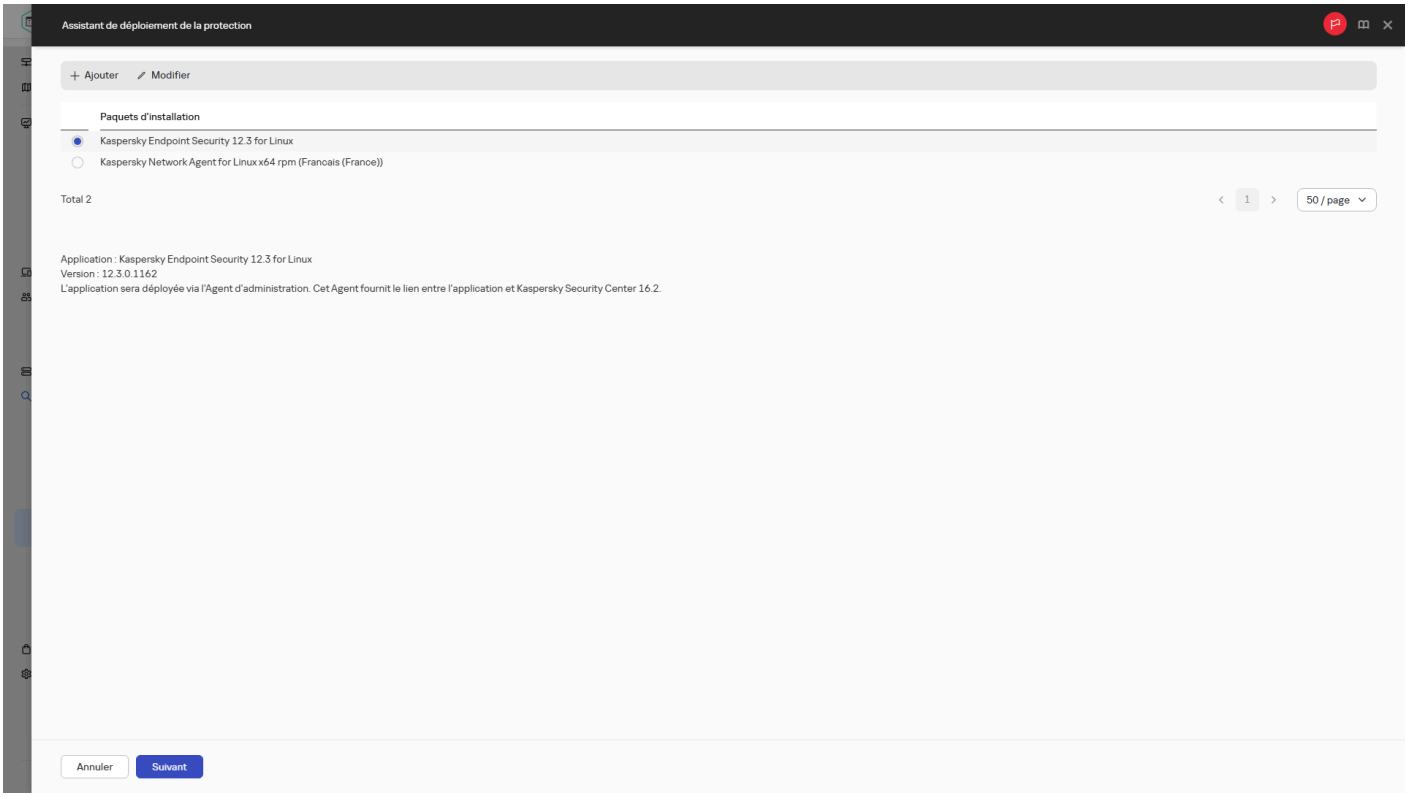
Dans le menu principal, accédez à **Découverte et déploiement** → **Déploiement et attribution** → **Assistant de déploiement de la protection**.

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.



Sélection du paquet d'installation

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 :

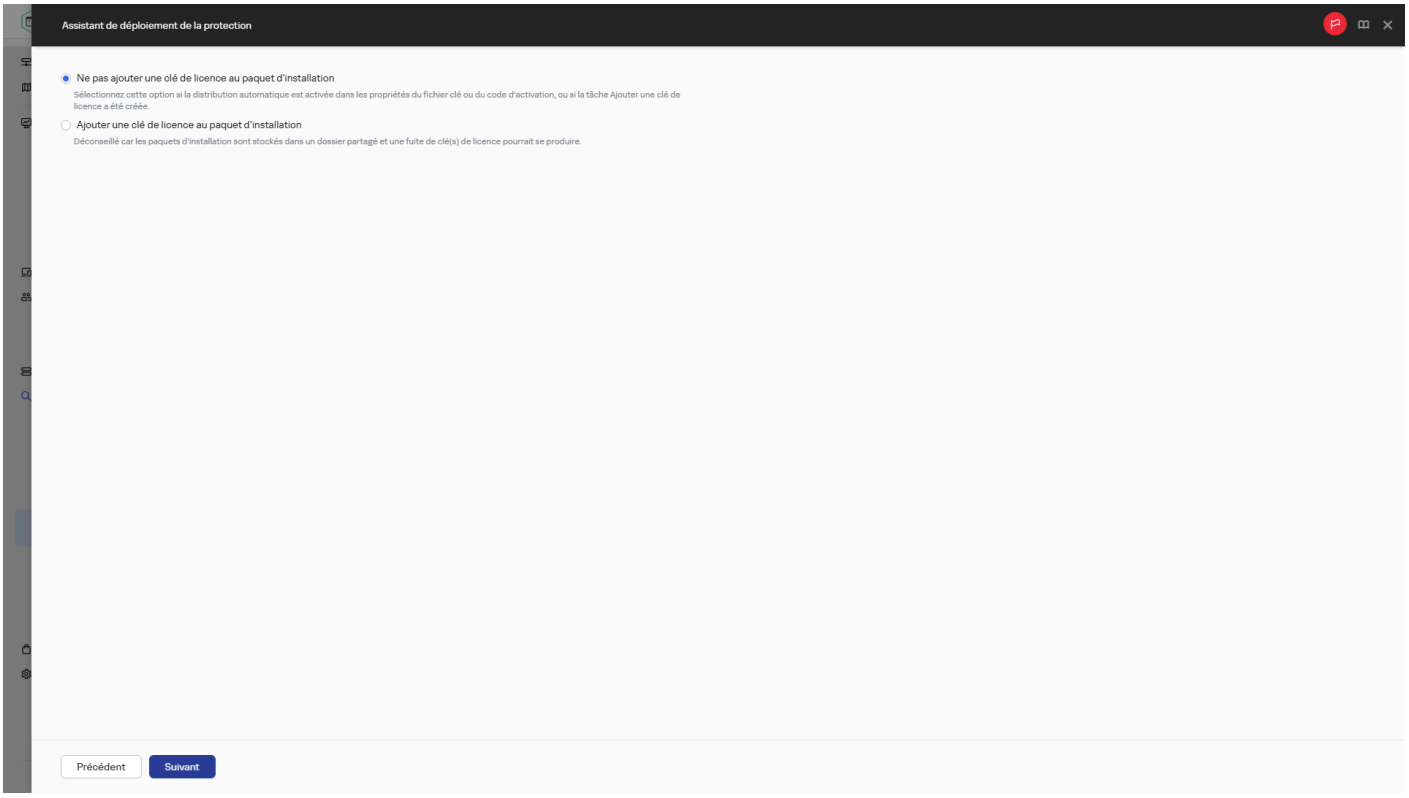
  - Si la diffusion automatique est activée dans les propriétés de la clé.
  - Si la tâche **Ajout de la clé** est créée.

- **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.

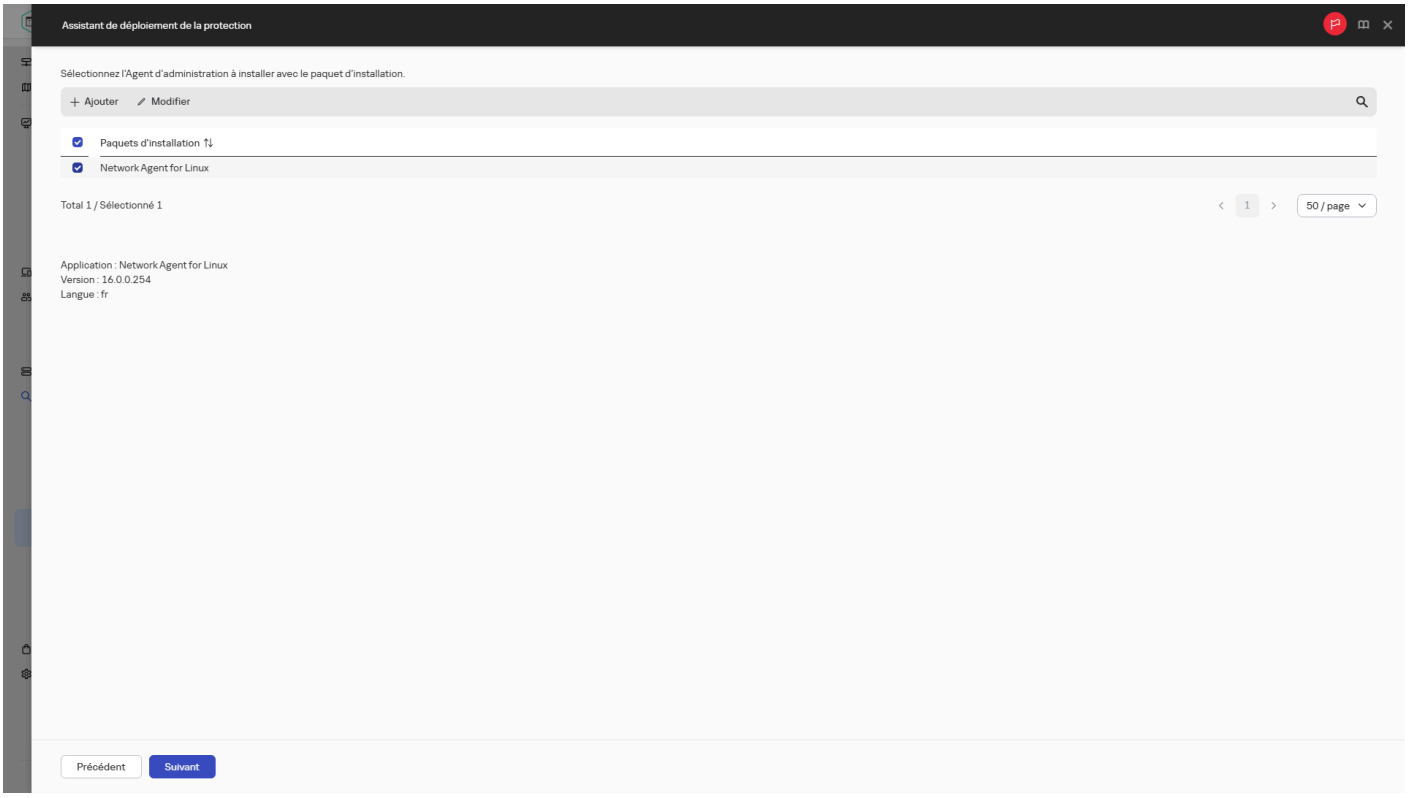


Sélection d'une méthode pour la distribution du fichier clé ou du code d'activation

Étape 4. Sélection de la version de l'Agent d'administration

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.

Sélectionnez la dernière version de l'agent d'administration.



Sélection de la version de l'Agent d'administration

Étape 5. Sélection des appareils

Composez une liste d'appareils sur lesquels l'application va être installée :

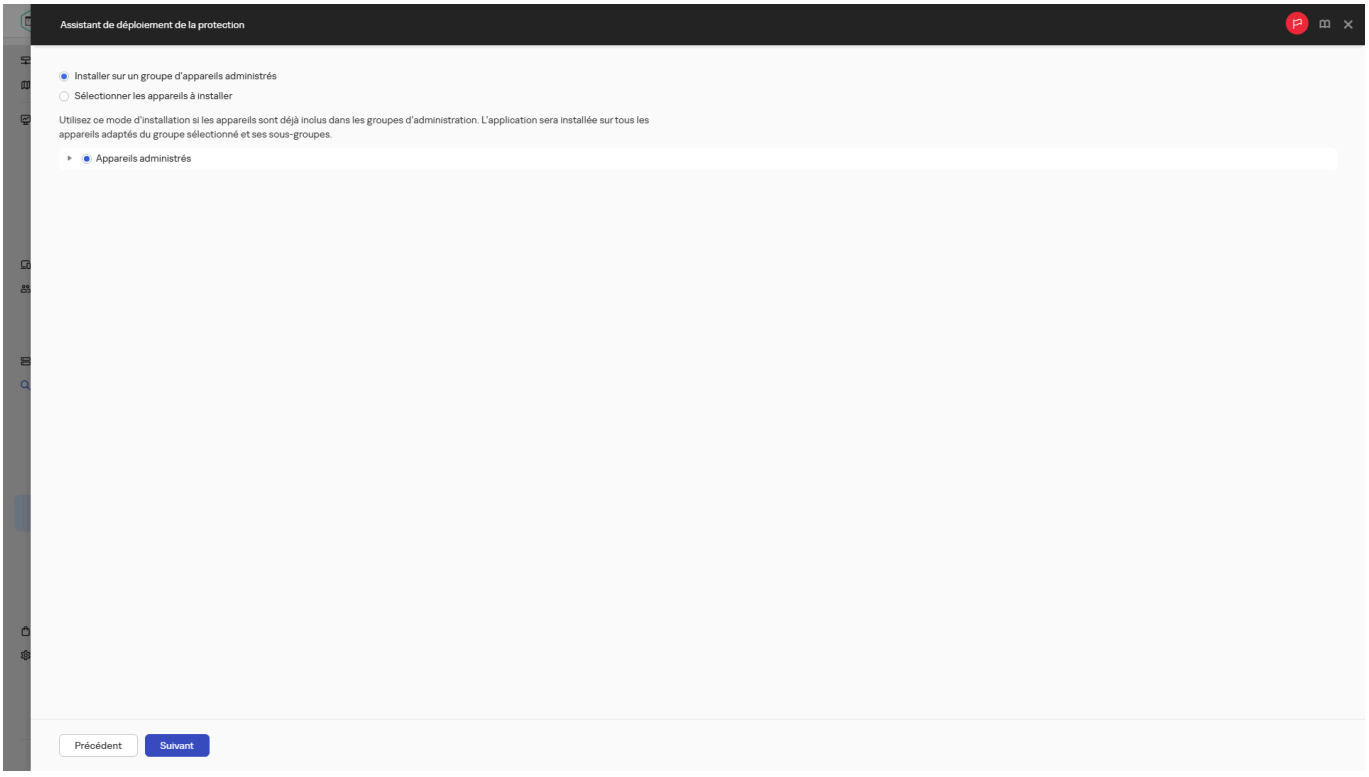
- **Installer sur un groupe d'appareils administrés**

  Si cette option a été sélectionnée, la tâche d'installation à distance de l'application sera créée pour le groupe des appareils.

- **Sélectionner les appareils à installer**

  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.



Spécification de la liste des appareils sur lesquels l'application sera installée

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 :

- **Utilisation de 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 la case est cochée, les paquets d'installation sont fournis aux appareils clients à l'aide des mécanismes du système d'exploitation via un point 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.

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.

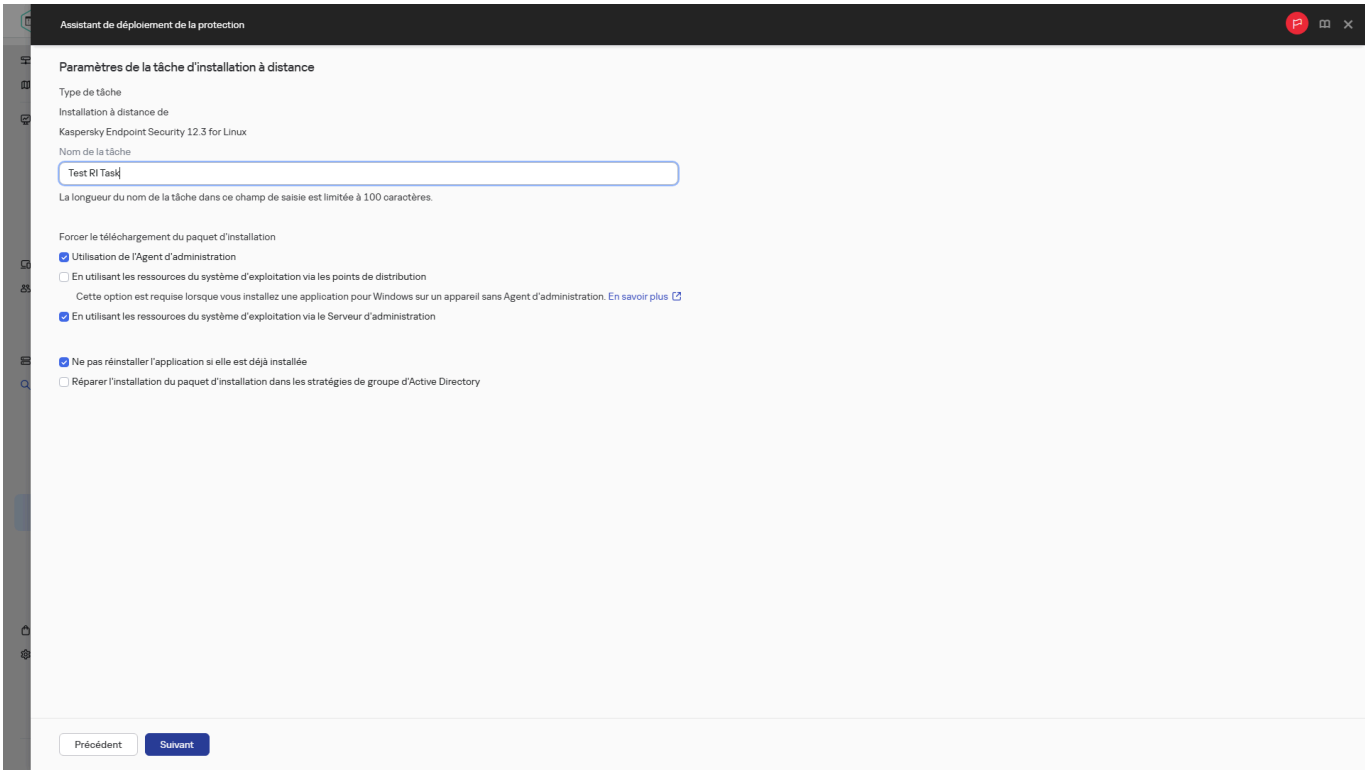
Cette option est activée par défaut.

- **Réparer l'installation du paquet d'installation dans les stratégies de groupe d'Active Directory**

Si l'option est activée, le paquet d'installation s'installera à l'aide des stratégies de groupes Active Directory.

L'option est disponible si le paquet d'installation de l'Agent d'administration est sélectionné.

Cette option est Inactif par défaut.



Indiquez les paramètres de la tâche d'installation à distance

Étape 7. Administration du redémarrage

Définir l'action à appliquer s'il faut redémarrer le système d'exploitation pendant l'installation de l'application.

- **Ne pas redémarrer l'appareil**

  Les appareils clients ne redémarrent pas automatiquement après l'opération. Pour arrêter le fonctionnement, il faut redémarrer l'appareil (par exemple, manuellement ou à l'aide d'une tâche d'administration des appareils). Les informations sur la nécessité du redémarrage sont enregistrées dans les résultats de la tâche et dans l'état de l'appareil. Cette option convient aux tâches d' sur les serveurs et autres appareils pour lesquels la continuité des opérations est critique.

- **Redémarrer l'appareil**

  Dans ce cas, le redémarrage des appareils clients est toujours exécuté automatiquement, si celui-ci est requis pour terminer l'opération. Cette option convient aux tâches d' sur des appareils pour lesquels des interruptions périodiques sont admises (débranchement, redémarrage).

- **Confirmer l'action auprès de l'utilisateur**

  Le message qui signale que l'appareil client doit être redémarré manuellement s'affiche sur l'écran de l'appareil. Pour cette option, il est possible de configurer des paramètres avancés : le texte du message pour l'utilisateur, la fréquence du message, ainsi que le délai à l'issue duquel le redémarrage sera forcé (sans confirmation de l'utilisateur). Cette option convient le mieux pour les postes de travail sur lesquels les utilisateurs doivent pouvoir sélectionner l'heure de redémarrage qui leur convient le mieux.

Cette option est sélectionnée par défaut.

- **Répéter demande périodiquement dans (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.

- **Redémarrage dans (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.

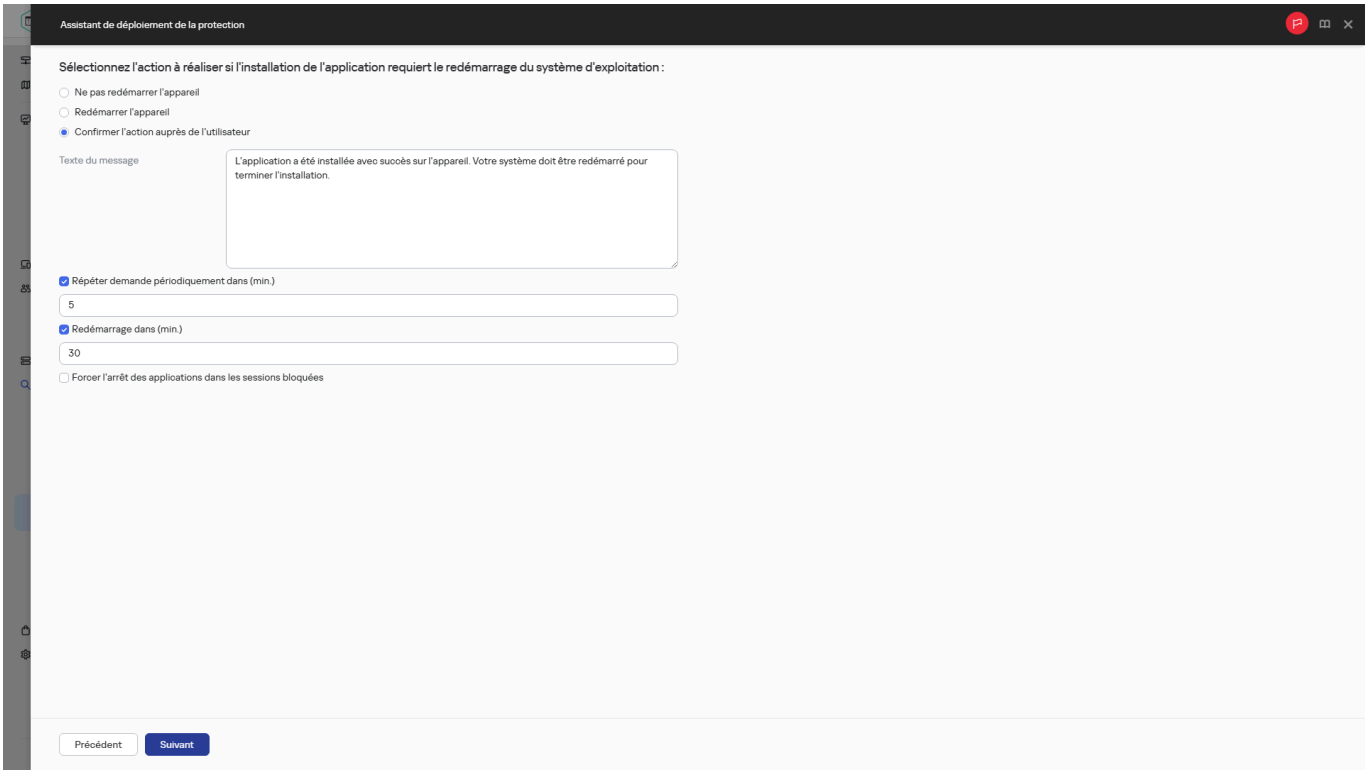
- **Forcer l'arrêt des applications dans les sessions bloquées**

  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.



Sélection de l'option de redémarrage du système d'exploitation

Étape 8. Suppression des applications incompatibles avant l'installation

Cette étape est présente uniquement si l'application que vous déployez est incompatible avec d'autres applications.

Sélectionnez cette option si vous souhaitez que Kaspersky Security Center 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 9. Déplacement des appareils vers Appareils administrés

Indiquez si les appareils doivent être déplacés vers un groupe d'administration après l'installation de l'agent d'administration.

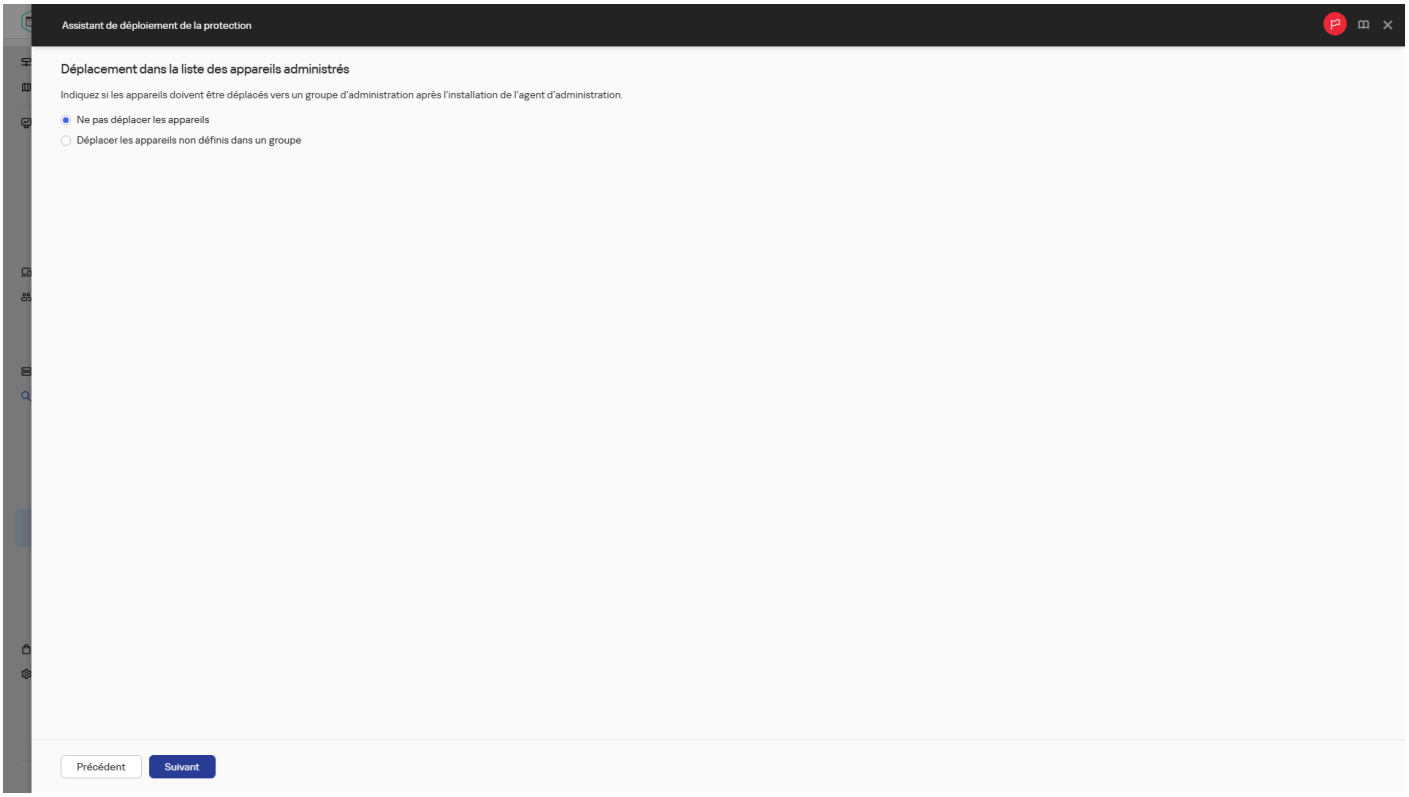
- **Ne pas déplacer les appareils**

  Les appareils demeurent dans les groupes où ils se trouvent. Les appareils qui n'ont été placés dans aucun groupe restent non définis.

- **Déplacer les appareils non définis dans un groupe**

  Les appareils sont déplacés vers le groupe d'administration que vous avez sélectionné.

L'option **Ne pas déplacer les appareils** est sélectionnée par défaut. Pour des raisons de sécurité, envisagez de déplacer les appareils manuellement.



Sélection d'une option de déplacement des appareils vers un groupe d'administration

Étape 10. Sélection des comptes pour accéder aux appareils

Si nécessaire, ajoutez les comptes utilisateurs qui seront utilisés pour démarrer la tâche d'installation à distance :

- **Compte utilisateur non requis (Agent d'administration installé)**

  Si cette option est sélectionnée, il n'est pas nécessaire d'indiquer le compte utilisateur au nom duquel l'installateur de l'application sera lancé. La tâche est lancée sous le même compte utilisateur que le compte du service du Serveur d'administration.

  Si l'agent d'administration n'est pas installé sur les appareils clients, l'option n'est pas disponible.

- **Compte 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.

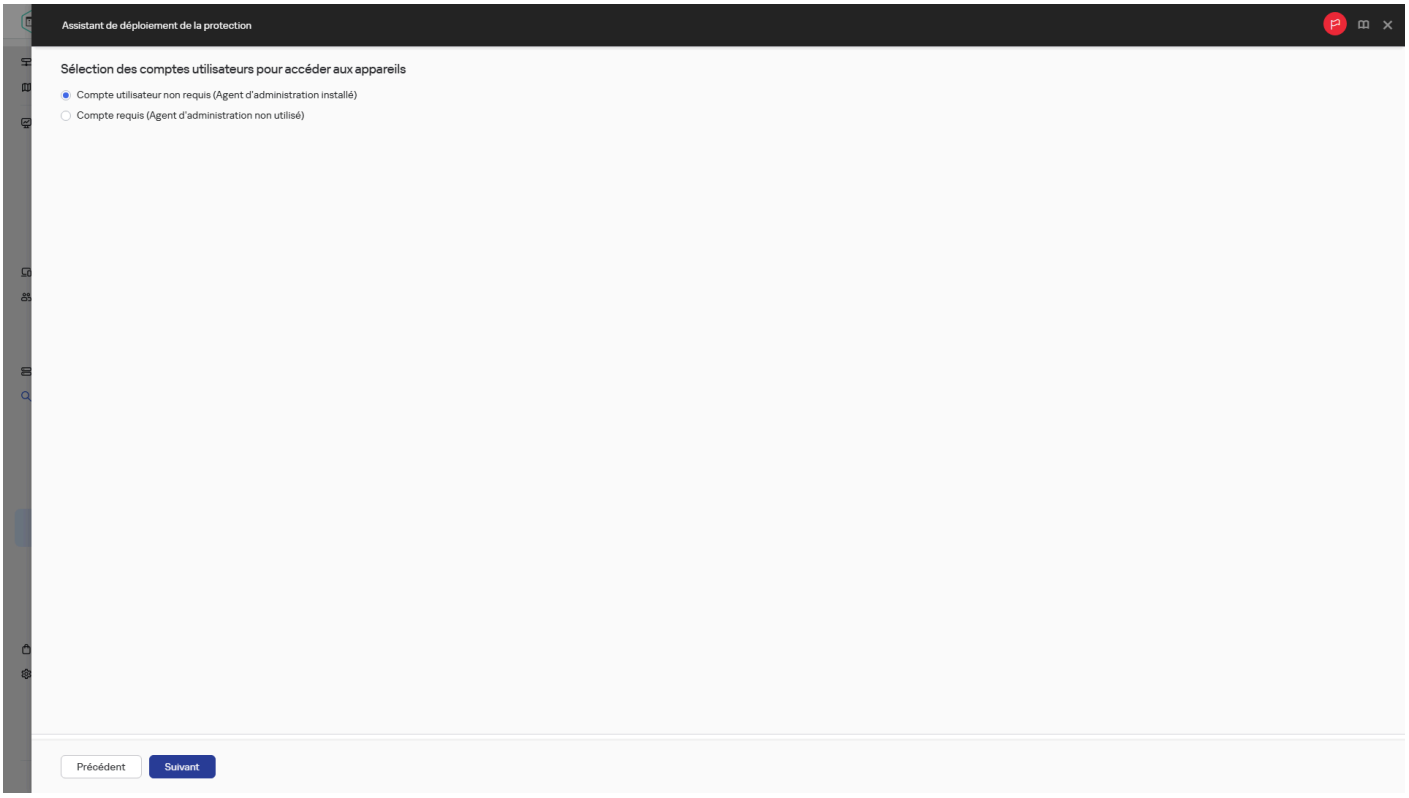
  - **Compte utilisateur local**. Si cette option est sélectionnée, spécifiez le compte utilisateur sous lequel le programme d'installation de l'application sera exécuté. Cliquez sur le bouton **Ajouter**, sélectionnez **Compte utilisateur local**, puis indiquez les informations d'identification du compte 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>"
    ```



Sélection des comptes pour accéder aux appareils

Étape 11. Démarrage de l'installation

Cette page est la dernière étape de l'assistant. À cette étape, la **Tâche d'installation à distance** a été créée et configurée avec succès.

Par défaut, l'option **Lancer la tâche à la fin de l'Assistant** n'est pas sélectionnée. Si vous sélectionnez cette option, la **Tâche d'installation à distance** démarre immédiatement après la fin de l'assistant. Si vous ne sélectionnez pas cette option, la **Tâche d'installation à distance** ne démarre pas. Vous pouvez manuellement lancer cette tâche par la suite.

Cliquez sur **OK** pour terminer l'étape finale de l'Assistant de déploiement de la protection.

Mise à jour de Kaspersky Security Center Linux

Vous pouvez installer le Serveur d'administration version 16.2 sur un appareil disposant d'une version antérieure du Serveur d'administration (à partir de la version 13). Lors de la mise à jour jusqu'à la version 16.2, tous les données et les paramètres de la version précédente du Serveur d'administration sont conservées.

Prérequis

- Avant de lancer la mise à jour, créez une copie de sauvegarde des données du Serveur d'administration.
- Lors de la mise à niveau du Serveur d'administration depuis la version 16 ou antérieure vers la version 16.1 ou ultérieure, l'authentification à deux facteurs est activée. Pour plus d'informations, consultez la section À propos de l'authentification à deux facteurs pour un compte.

  Pour permettre aux utilisateurs de se connecter à la Web Console avec leurs comptes existants à l'aide de clés secrètes d'authentification à deux facteurs configurées, et pour que les scripts d'automatisation OpenAPI continuent de fonctionner après la mise à niveau, vous devez suivre les étapes suivantes :

  - Activer l'authentification à deux facteurs pour tous les utilisateurs
  - Les administrateurs doivent configurer l'authentification à deux facteurs pour leurs propres comptes
  - Exclusion de comptes de l'authentification à deux facteurs

    Si nécessaire, ajoutez les comptes d'intégration utilisés pour exécuter des scripts via OpenAPI à la liste des exclusions.
- Assurez-vous que vous utilisez les versions du système d'exploitation et du SGBD prises en charge par la version 16.2 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.
- Lors de la mise à niveau du Serveur d'administration depuis la version 15.4 ou antérieure vers la version 16 ou ultérieure, sur le serveur SGBD, créez une base de données pour IAM. Le nom de la base de données doit être différent de celui de la base de données que vous avez installée pour utiliser Kaspersky Security Center Linux.

  - Pour PostgreSQL, exécutez la commande suivante :

    ```
    sudo -i -u postgres psql -U postgres -c "CREATE DATABASE <iam_db_name>;"
    ```

  - Pour MariaDB, exécutez la commande suivante :

    ```
    sudo mysql -u root -p -e "CREATE DATABASE <iam_db_name>;"
    ```

- Lors de la mise à niveau du Serveur d'administration depuis la version 15.4 ou antérieure vers la version 16 ou ultérieure, préparez le fichier de réponses avec les nouveaux paramètres pour IAM. Pour obtenir la liste des paramètres requis, consultez l'article Installation de Kaspersky Security Center Linux en mode silencieux. Ajoutez la variable d'environnement `KLAUTOANSWERS`. Définissez la valeur de la variable sur le chemin d'accès au fichier de réponses.

- Rendez disponible le port utilisé par le processus kliam pour l'authentification du protocole OpenID Connect. La valeur par défaut est de 4444. Reportez-vous à la description des paramètres `trusted` dans l'article suivant : Paramètres d'installation de Kaspersky Security Center Web Console.

Étapes

1. **Mise à niveau du Serveur d'administration**

   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.

2. **Exécution du script postinstall.pl (étape facultative)**

   Si le fichier de réponses ne contient pas les paramètres IAM ou si le fichier de réponses est introuvable, un message s'affiche dans le terminal pendant la mise à niveau, vous demandant d'exécuter le script postinstall.pl.

   À cette étape du scénario, procédez comme suit :

   1. Dans le système d'exploitation du Serveur d'administration, créez un compte utilisateur sans privilèges « ksciam » qui doit être membre du groupe « kladmins » :

      ```
      adduser ksciam
      gpasswd -a ksciam kladmins
      usermod -g kladmins ksciam
      ```

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

      1. Entrez le nom de domaine complet du serveur IAM. Vous devez utiliser le nom DNS du Serveur d'administration qui a été spécifié lors de l'installation de Kaspersky Security Center Linux.

      2. Saisissez le nom du compte pour lancer le service IAM. Le compte doit faire partie du groupe de sécurité saisi. Par défaut, le compte ksciam est utilisé.

3. Sélectionnez le SGBD que vous avez installé et qui doit fonctionner avec le service IAM :
   - Si vous avez installé MySQL ou MariaDB, saisissez 1.
   - Si vous avez installé PostgreSQL ou Postgres Pro, saisissez 2.
4. Saisissez l'adresse du SGBD IAM qui sera utilisé par le service IAM.
5. Saisissez le numéro de port du SGBD IAM. Ce port sert à communiquer avec le service IAM. Par défaut, les ports suivants sont utilisés :
   - Port 3306 pour MySQL ou MariaDB
   - Port 5432 pour PostgreSQL ou Postgres Pro
6. Saisissez le nom de la base de données IAM qui sera utilisée par le service IAM. Le nom de la base de données utilisée par le service IAM doit être différent de la base de données utilisée par le Serveur d'administration.

3. **Mise à niveau de Kaspersky Security Center Web Console**
4. **(Facultatif) Mise à niveau de l'Agent d'administration sur les appareils vers une nouvelle version.**
5. **Assurez-vous que la liste d'autorisation pour l'authentification à deux facteurs contient uniquement les comptes utilisateur qui doivent avoir accès au Serveur d'administration.**

   Vérifiez la liste d'autorisation pour l'authentification à deux facteurs et supprimez tout autre compte.

Veuillez noter que si vous mettez à niveau le Serveur d'administration vers la version 16.2, vous ne pourrez pas créer d'autres paquets d'installation de l'Agent d'administration de la version 15 ou toute version antérieure. Cependant, les paquets d'installation créés précédemment resteront disponibles.

Lors de la mise à jour de Kaspersky Security Center 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.

Mise à niveau de Kaspersky Security Center Linux à partir de la version 16 ou d'une version ultérieure

Cette section décrit les options suivantes pour mettre à niveau Kaspersky Security Center Linux à partir de la version 16 ou une version ultérieure vers la dernière version :

- Mise à niveau par le biais du fichier d'installation
- Mise à niveau par le biais d'une sauvegarde
- Mise à niveau sur les nœuds du cluster de basculement Kaspersky Security Center Linux

Mise à niveau de Kaspersky Security Center Linux à partir de la version 16 ou ultérieure à l'aide du fichier d'installation

Pour mettre à niveau le Serveur d'administration à partir de la version 16 ou d'une version antérieure, 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 Kaspersky Security Center Linux à partir de la version 16 ou d'une version ultérieure vers la dernière version en utilisant le fichier d'installation, procédez comme suit :

1. Téléchargez le fichier d'installation de Kaspersky Security Center Linux avec un paquet complet pour la version 16.2 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 Kaspersky Security Center Linux. Exécutez l'une des commandes suivantes dans le terminal de ligne de commande :

   - Pour les appareils exécutant un système d'exploitation basé sur RPM :

     ```
     sudo yum install ./ksc64-<version number>.x86_64.rpm
     ```

   - Pour les appareils exécutant un système d'exploitation basé sur Debian :

     ```
     sudo apt-get install ./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. Exécutez le script `/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl` pour configurer le Serveur d'administration mis à jour :

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

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 `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.

```
Enter 'Y' to confirm that you understand and accept the terms of the End
User License Agreement (EULA). You must accept the terms and conditions of
the EULA to install the application. Enter 'N' providing you do not accept
the terms of the EULA or 'R' to view it again [N]:
y

Enter 'Y' to confirm that you accept the terms of the Privacy Policy. You
must accept the terms and conditions of the Privacy Policy to install the
application. Entering 'Y' means that you are aware that your data will be
handled and transmitted (including to third countries) as described in the
Privacy Policy. Enter 'N' providing you do not accept the Privacy Policy
[N]:
y

Choose the Administration Server installation mode:
1) Standard
2) Primary cluster node
3) Secondary cluster node
Enter the range number (1, 2, or 3) [1]:
```

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. Mettez à niveau Kaspersky Security Center Web Console vers une nouvelle version.

7. 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.

   Exécutez les commandes suivantes sur les ressources basées sur Linux pour supprimer les dépendances devenues obsolètes :

   - Pour les ressources basées sur Debian, exécutez l'une des commandes suivantes :

     ```
     sudo apt-get -y autoremove
     ```

     ```
     sudo apt -y autoremove
     ```

   - Pour les ressources basées sur RPM, exécutez l'une des commandes suivantes :

     ```
     sudo dnf autoremove
     ```

     ```
     sudo yum autoremove
     ```

Mise à niveau de Kaspersky Security Center Linux à partir de la version 16 ou d'une version ultérieure par le biais d'une sauvegarde

Pour mettre à niveau le Serveur d'administration à partir de la version 16 ou d'une version ultérieure, 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 niveau Kaspersky Security Center Linux à partir de la version 16 ou d'une version ultérieure vers la dernière version par le biais d'une 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 Linux version 16.2 sur l'appareil sur lequel le Serveur d'administration a été installé auparavant.

4. Restaurez les données du Serveur d'administration à partir de la sauvegarde créée avant la mise à jour.

5. Installez Kaspersky Security Center Web Console.

   Si Kaspersky Security Center Web Console a été installé précédemment, réinstallez-le avec le même fichier de réponse.

   Connectez-vous à Kaspersky Security Center Web Console sous le compte utilisateur interne de l'administrateur.

   Le processus d'initialisation des données dure généralement jusqu'à 15 minutes après la restauration des données du Serveur d'administration. Toutefois, cette durée dépend de la performance du matériel et de la taille des données du Serveur d'administration. Pendant ce temps, Kaspersky Security Center Web Console peut ne pas réussir à se connecter et afficher alors les erreurs.

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.

   Exécutez les commandes suivantes sur les ressources basées sur Linux pour supprimer les dépendances devenues obsolètes :

   - Pour les ressources basées sur Debian, exécutez l'une des commandes suivantes :

     ```
     sudo apt-get -y autoremove
     ```

     ```
     sudo apt -y autoremove
     ```

- Pour les ressources basées sur RPM, exécutez l'une des commandes suivantes :

```
sudo dnf autoremove
```

```
sudo yum autoremove
```

Mise à jour de Kaspersky Security Center à partir de la version 16 ou d'une version ultérieure sur les nœuds du cluster de basculement Kaspersky Security Center Linux

Vous pouvez installer la dernière version du Serveur d'administration sur chaque nœud de cluster de basculement Kaspersky Security Center Linux où est installée la version 16 ou une version ultérieure du Serveur d'administration. Lors de la mise à niveau vers la dernière version, 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.

La mise à niveau de Kaspersky Security Center Linux vers la version 16.2 sur les nœuds du cluster de basculement à l'aide d'un fichier d'installation n'est pas prise en charge. Pour effectuer la mise à niveau d'une version précédente vers la version 16.2, créez une copie de sauvegarde des données du Serveur d'administration, installez la nouvelle version du cluster de basculement Kaspersky Security Center Linux, puis restaurez les données du Serveur d'administration à partir de la copie de sauvegarde. Cette restriction s'applique également à un cluster réparti géographiquement.

Pour mettre à niveau Kaspersky Security Center à partir de la version 16 ou d'une version ultérieure sur les nœuds du cluster de basculement Kaspersky Security Center Linux, procédez comme suit :

1. Téléchargez le fichier d'installation de Kaspersky Security Center Linux avec un paquet complet pour la version 16.2 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, exécutez la commande suivante dans le terminal de ligne de commande pour lancer la mise à niveau :

   - Pour les appareils exécutant un système d'exploitation basé sur RPM :

```
sudo yum install ./ksc64-<version number>-<build number>.x86_64.rpm
```

- Pour les appareils exécutant un système d'exploitation basé sur Debian :

```
sudo apt-get install ./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. Exécutez le script `/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl` pour configurer le Serveur d'administration mis à jour :

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

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 :

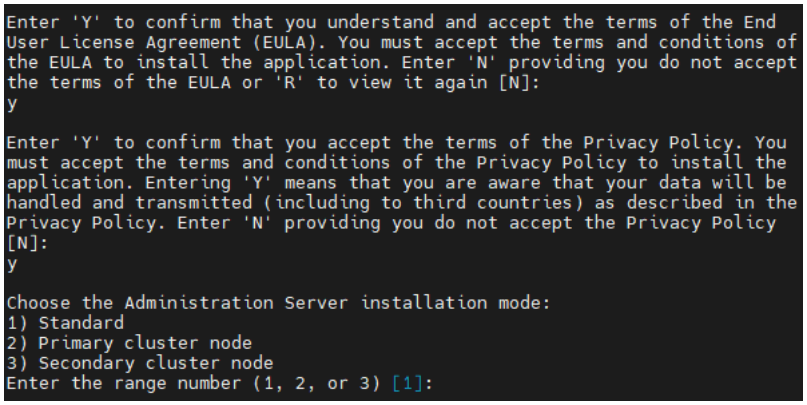
   a. Saisissez `Y` pour confirmer que vous avez entièrement lu, compris et accepté les termes et conditions du CLUF.

   b. Saisissez à nouveau `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.

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

9. 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.

   Exécutez les commandes suivantes sur les ressources basées sur Linux pour supprimer les dépendances devenues obsolètes :

   - Pour les ressources basées sur Debian, exécutez l'une des commandes suivantes :

     ```
     sudo apt-get -y autoremove
     ```

     ```
     sudo apt -y autoremove
     ```

   - Pour les ressources basées sur RPM, exécutez l'une des commandes suivantes :

     ```
     sudo dnf autoremove
     ```

     ```
     sudo yum autoremove
     ```

   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 Linux à partir de la version 15.4 ou d'une version antérieure

Cette section décrit les options suivantes pour mettre à niveau Kaspersky Security Center Linux de la version 15.4 ou toute version antérieure à la version 16 ou plus récente :

- Mise à niveau par le biais du fichier d'installation
- Mise à niveau par le biais d'une sauvegarde
- Mise à niveau sur les nœuds du cluster de basculement Kaspersky Security Center Linux

Chaque option de mise à niveau de Kaspersky Security Center Linux de la version 15.4 ou toute version antérieure à la version 16 ou plus récente inclut les étapes pour créer et configurer une base de données IAM sur un serveur SGBD, créer un compte " ksciam " sans privilèges pour exécuter le service IAM, et ajouter ce compte au groupe de sécurité " kladmins ".

Mise à niveau de Kaspersky Security Center Linux à partir de la version 15.4 ou toute version antérieure à l'aide du fichier d'installation

Pour mettre à niveau le Serveur d'administration de la version 13–15.4 à la version 16 ou une version ultérieure, vous pouvez installer une nouvelle version sur une version antérieure à l'aide du fichier d'installation de Kaspersky Security Center Linux.

Avant de commencer, **vérifiez les conditions requises pour obtenir un certificat personnalisé**.

Si vous utilisez un certificat personnalisé au lieu du certificat auto-signé, avant de mettre à niveau Kaspersky Security Center Linux vers une version plus récente, vous devez vous assurer que le certificat inclut le nom alternatif du sujet (SAN). Si ce n'est pas le cas, il est important de remplacer le certificat avant de mettre à niveau Kaspersky Security Center Linux. Sinon, vous ne pourrez pas vous connecter à Web Console après la mise à niveau.

Pour vous assurer que le certificat inclut un SAN, procédez comme suit :

1. Sur l'appareil sur lequel le Serveur d'administration est installé, exécutez la commande suivante :

   - Pour un appareil fonctionnant sous Linux :

     ```
     sudo openssl x509 -in /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -noout -ext subjectAltName
     ```

   - Pour un appareil fonctionnant sous Windows :

     ```
     certutil -dump %ProgramData%\KasperskyLab\adminkit\1093\cert\klserver.cer
     ```

2. Assurez-vous que le nom alternatif du sujet (SAN) figure dans la sortie de la commande et qu'il contient l'adresse de l'appareil du Serveur d'administration.

3. Si le nom alternatif du sujet est absent, utilisez l'utilitaire klsetsrvcert pour remplacer votre certificat utilisateur par un certificat conforme aux exigences.

Pour mettre à niveau Kaspersky Security Center Linux à partir de la version 15.4 ou d'une version antérieure vers la dernière version en utilisant le fichier d'installation, procédez comme suit :

1. Téléchargez le fichier d'installation de Kaspersky Security Center Linux avec un paquet complet pour la version 16.2 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. Sur le serveur SGBD, créez une base de données pour IAM. Le nom de la base de données IAM doit être différent de celui de la base de données que vous avez installée pour fonctionner avec Kaspersky Security Center Linux.

   - Pour PostgreSQL, exécutez la commande suivante :

     ```
     sudo -i -u postgres psql -U postgres -c "CREATE DATABASE <nom_bd_iam>;"
     ```

   - Pour MariaDB, exécutez la commande suivante :

     ```
     sudo mysql -u root -p -e "CREATE DATABASE <nom_bd_iam>;"
     ```

3. Créez un compte sans privilèges " ksciam ", ajoutez-le au groupe de sécurité " kladmins ", puis définissez le groupe " kladmins " comme le groupe principal pour le compte " ksciam ". Pour ce faire, exécutez les commandes suivantes en séquence :

   ```
   sudo adduser ksciam
   sudo gpasswd -a ksciam kladmins
   sudo usermod -g kladmins ksciam
   ```

4. Mettez à niveau Kaspersky Security Center Linux. Exécutez l'une des commandes suivantes dans le terminal de ligne de commande :

   - Pour les appareils exécutant un système d'exploitation basé sur RPM :

     ```
     sudo yum install ./ksc64-<numéro de version>.x86_64.rpm
     ```

   - Pour les appareils exécutant un système d'exploitation basé sur Debian :

     ```
     sudo apt-get install ./ksc64_<numéro de version>_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.

5. Exécutez le script `/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl` pour configurer le Serveur d'administration mis à jour :

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

6. 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 `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`.

7. Saisissez `1` pour sélectionner le mode d'installation standard du Serveur d'administration.

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

```
Enter 'Y' to confirm that you understand and accept the terms of the End
User License Agreement (EULA). You must accept the terms and conditions of
the EULA to install the application. Enter 'N' providing you do not accept
the terms of the EULA or 'R' to view it again [N]:
y

Enter 'Y' to confirm that you accept the terms of the Privacy Policy. You
must accept the terms and conditions of the Privacy Policy to install the
application. Entering 'Y' means that you are aware that your data will be
handled and transmitted (including to third countries) as described in the
Privacy Policy. Enter 'N' providing you do not accept the Privacy Policy
[N]:
y

Choose the Administration Server installation mode:
1) Standard
2) Primary cluster node
3) Secondary cluster node
Enter the range number (1, 2, or 3) [1]:
```

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

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

   a. Entrez le nom de domaine complet du serveur IAM.

      Vous devez utiliser le nom DNS du Serveur d'administration qui a été spécifié lors de l'installation de Kaspersky Security Center Linux.

   b. Saisissez le nom du compte pour lancer le service IAM. Le compte doit faire partie du groupe de sécurité saisi. Par défaut, le compte ksciam est utilisé.

   c. Sélectionnez le SGBD que vous avez installé et qui doit fonctionner avec le service IAM :

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

   d. Saisissez l'adresse du SGBD IAM qui sera utilisé par le service IAM.

   e. Saisissez le numéro de port du SGBD IAM. Ce port sert à communiquer avec le service IAM. Par défaut, les ports suivants sont utilisés :

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

   f. Saisissez le nom de la base de données IAM qui sera utilisée par le service IAM. Le nom de la base de données utilisée par le service IAM doit être différent de la base de données utilisée par le Serveur d'administration.

   g. Saisissez l'identifiant et le mot de passe du SGBD qui seront utilisés par le service IAM.

9. Mettez à niveau Kaspersky Security Center Web Console vers une nouvelle version.

10. 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.

Exécutez les commandes suivantes sur les ressources basées sur Linux pour supprimer les dépendances devenues obsolètes :

- Pour les ressources basées sur Debian, exécutez l'une des commandes suivantes :

```
sudo apt-get -y autoremove
```

```
sudo apt -y autoremove
```

- Pour les ressources basées sur RPM, exécutez l'une des commandes suivantes :

```
sudo dnf autoremove
```

```
sudo yum autoremove
```

Mise à niveau de Kaspersky Security Center Linux à partir de la version 15.4 ou d'une version antérieure par le biais d'une sauvegarde

Pour mettre à niveau le Serveur d'administration de la version 14.2–15.4 à la version 16 ou une version ultérieure, vous pouvez créer une sauvegarde des données du Serveur d'administration et la restaurer après avoir installé une nouvelle version de Kaspersky Security Center Linux. 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.

Prérequis

1. **Vérifiez les conditions requises pour obtenir un certificat personnalisé**.

Si vous utilisez un certificat personnalisé au lieu du certificat auto-signé, avant de mettre à niveau Kaspersky Security Center Linux vers une version plus récente, vous devez vous assurer que le certificat inclut le nom alternatif du sujet (SAN). Si ce n'est pas le cas, il est important de remplacer le certificat avant de mettre à niveau Kaspersky Security Center Linux. Sinon, vous ne pourrez pas vous connecter à Web Console après la mise à niveau.

Pour vous assurer que le certificat inclut un SAN, procédez comme suit :

1. Sur l'appareil sur lequel le Serveur d'administration est installé, exécutez la commande suivante :
   - Pour un appareil fonctionnant sous Linux :

     ```
     sudo openssl x509 -in /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -noout -ext subjectAltName
     ```

   - Pour un appareil fonctionnant sous Windows :

     ```
     certutil -dump %ProgramData%\KasperskyLab\adminkit\1093\cert\klserver.cer
     ```

2. Assurez-vous que le nom alternatif du sujet (SAN) figure dans la sortie de la commande et qu'il contient l'adresse de l'appareil du Serveur d'administration.
3. Si le nom alternatif du sujet est absent, utilisez l'utilitaire klsetsrvcert pour remplacer votre certificat utilisateur par un certificat conforme aux exigences.

2. Sauvegardez les données du Serveur d'administration avec une version antérieure de l'application.

La procédure de mise à niveau

Pour mettre à niveau Kaspersky Security Center Linux de la version 15.4 ou toute version antérieure vers la dernière version par le biais d'une sauvegarde, procédez comme suit :

1. Désinstallez l'ancienne version de Kaspersky Security Center Linux.
2. Sur le serveur SGBD, créez une base de données pour IAM. Le nom de la base de données IAM doit être différent de celui de la base de données que vous avez installée pour fonctionner avec Kaspersky Security Center Linux.
   - Pour PostgreSQL, exécutez la commande suivante :

     ```
     sudo -i -u postgres psql -U postgres -c "CREATE DATABASE <nom_bd_iam>;"
     ```

   - Pour MariaDB, exécutez la commande suivante :

     ```
     sudo mysql -u root -p -e "CREATE DATABASE <nom_bd_iam>;"
     ```

3. Créez un compte sans privilèges " ksciam ", ajoutez-le au groupe de sécurité " kladmins ", puis définissez le groupe " kladmins " comme le groupe principal pour le compte " ksciam ". Pour ce faire, exécutez les commandes suivantes en séquence :

   ```
   sudo adduser ksciam
   sudo gpasswd -a ksciam kladmins
   sudo usermod -g kladmins ksciam
   ```

4. Installez Kaspersky Security Center Linux version 16.2 sur l'appareil sur lequel le Serveur d'administration a été installé auparavant.

5. Restaurez les données du Serveur d'administration à partir de la sauvegarde créée avant la mise à jour.

6. Configurez la vérification des certificats par le Serveur d'administration et le serveur IAM.

7. Installez Kaspersky Security Center Web Console.

   Si Kaspersky Security Center Web Console a été installé précédemment, réinstallez-le avec le même fichier de réponse.

   Connectez-vous à Kaspersky Security Center Web Console sous le compte utilisateur interne de l'administrateur.

   Le processus d'initialisation des données dure généralement jusqu'à 15 minutes après la restauration des données du Serveur d'administration. Toutefois, cette durée dépend de la performance du matériel et de la taille des données du Serveur d'administration. Pendant ce temps, Kaspersky Security Center Web Console peut ne pas réussir à se connecter et afficher alors les erreurs.

8. 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.

   Exécutez les commandes suivantes sur les ressources basées sur Linux pour supprimer les dépendances devenues obsolètes :

   - Pour les ressources basées sur Debian, exécutez l'une des commandes suivantes :

     ```
     sudo apt-get -y autoremove
     ```

     ```
     sudo apt -y autoremove
     ```

   - Pour les ressources basées sur RPM, exécutez l'une des commandes suivantes :

     ```
     sudo dnf autoremove
     ```

     ```
     sudo yum autoremove
     ```

Mise à jour de Kaspersky Security Center à partir de la version 15.4 ou d'une version antérieure sur les nœuds du cluster de basculement Kaspersky Security Center Linux

Vous pouvez installer le Serveur d'administration version 16 ou une version ultérieure sur chaque nœud du cluster de basculement Kaspersky Security Center Linux où le Serveur d'administration version 14–15.4 est installé. Lors de la mise à niveau, tous les données et les paramètres de la version précédente du Serveur d'administration sont conservées.

Avant de commencer, **vérifiez les conditions requises pour obtenir un certificat personnalisé**.

Si vous utilisez un certificat personnalisé au lieu du certificat auto-signé, avant de mettre à niveau Kaspersky Security Center Linux vers une version plus récente, vous devez vous assurer que le certificat inclut le nom alternatif du sujet (SAN). Si ce n'est pas le cas, il est important de remplacer le certificat avant de mettre à niveau Kaspersky Security Center Linux. Sinon, vous ne pourrez pas vous connecter à Web Console après la mise à niveau.

Pour vous assurer que le certificat inclut un SAN, procédez comme suit :

1. Sur l'appareil sur lequel le Serveur d'administration est installé, exécutez la commande suivante :

   - Pour un appareil fonctionnant sous Linux :

     ```
     sudo openssl x509 -in /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -
     noout -ext subjectAltName
     ```

   - Pour un appareil fonctionnant sous Windows :

     ```
     certutil -dump %ProgramData%\KasperskyLab\adminkit\1093\cert\klserver.cer
     ```

2. Assurez-vous que le nom alternatif du sujet (SAN) figure dans la sortie de la commande et qu'il contient l'adresse de l'appareil du Serveur d'administration.

3. Si le nom alternatif du sujet est absent, utilisez l'utilitaire klsetsrvcert pour remplacer votre certificat utilisateur par un certificat conforme aux exigences.

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 niveau Kaspersky Security Center à partir de la version 15.4 ou d'une version antérieure sur les nœuds du cluster de basculement Kaspersky Security Center Linux, procédez comme suit :

1. Téléchargez le fichier d'installation de Kaspersky Security Center Linux avec un paquet complet pour la version 16.2 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 serveur SGBD, créez une base de données pour IAM. Le nom de la base de données IAM doit être différent de celui de la base de données que vous avez installée pour fonctionner avec Kaspersky Security Center Linux.

   - Pour PostgreSQL, exécutez la commande suivante :

     ```
     sudo -i -u postgres psql -U postgres -c "CREATE DATABASE <nom_bd_iam>;"
     ```

- Pour MariaDB, exécutez la commande suivante :

```
sudo mysql -u root -p -e "CREATE DATABASE <nom_bd_iam>;"
```

4. Créez un compte sans privilèges " ksciam ", ajoutez-le au groupe de sécurité " kladmins ", puis définissez le groupe " kladmins " comme le groupe principal pour le compte " ksciam ". Pour ce faire, exécutez les commandes suivantes en séquence :

```
sudo adduser ksciam
sudo gpasswd -a ksciam kladmins
sudo usermod -g kladmins ksciam
```

5. Sur le nœud actif du cluster, exécutez l'une des commandes suivantes sur la ligne de commande pour lancer la mise à niveau :

   - Pour les appareils exécutant un système d'exploitation basé sur RPM :

   ```
   sudo yum install ./ksc64-<numéro de version>-<numéro de compilation>.x86_64.rpm
   ```

   - Pour les appareils exécutant un système d'exploitation basé sur Debian :

   ```
   sudo apt-get install ./ksc64_<numéro de version>-<numéro de compilation>_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.

6. Exécutez le script `/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl` pour configurer le Serveur d'administration mis à jour :

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

7. 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 `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`.

8. Sélectionnez le nœud sur lequel vous effectuez la mise à niveau en saisissant `2`.

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

```
Enter 'Y' to confirm that you understand and accept the terms of the End
User License Agreement (EULA). You must accept the terms and conditions of
the EULA to install the application. Enter 'N' providing you do not accept
the terms of the EULA or 'R' to view it again [N]:
y

Enter 'Y' to confirm that you accept the terms of the Privacy Policy. You
must accept the terms and conditions of the Privacy Policy to install the
application. Entering 'Y' means that you are aware that your data will be
handled and transmitted (including to third countries) as described in the
Privacy Policy. Enter 'N' providing you do not accept the Privacy Policy
[N]:
y

Choose the Administration Server installation mode:
1) Standard
2) Primary cluster node
3) Secondary cluster node
Enter the range number (1, 2, or 3) [1]:
```

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

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

   a. Entrez le nom de domaine complet du serveur IAM.

      Vous devez utiliser le nom DNS du Serveur d'administration qui a été spécifié lors de l'installation de Kaspersky Security Center Linux.

   b. Saisissez le nom du compte pour lancer le service IAM. Le compte doit faire partie du groupe de sécurité saisi. Par défaut, le compte ksciam est utilisé.

   c. Sélectionnez le SGBD que vous avez installé et qui doit fonctionner avec le service IAM :

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

   d. Saisissez l'adresse du SGBD IAM qui sera utilisé par le service IAM.

   e. Saisissez le numéro de port du SGBD IAM. Ce port sert à communiquer avec le service IAM. Par défaut, les ports suivants sont utilisés :

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

   f. Saisissez le nom de la base de données IAM qui sera utilisée par le service IAM. Le nom de la base de données utilisée par le service IAM doit être différent de la base de données utilisée par le Serveur d'administration.

   g. Saisissez l'identifiant et le mot de passe du SGBD qui seront utilisés par le service IAM.

10. Effectuez l'étape 5 sur le nœud passif.

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

11. Démarrer le cluster.

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

12. 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.

    Exécutez les commandes suivantes sur les ressources basées sur Linux pour supprimer les dépendances devenues obsolètes :

    - Pour les ressources basées sur Debian, exécutez l'une des commandes suivantes :

      ```
      sudo apt-get -y autoremove
      ```

      ```
      sudo apt -y autoremove
      ```

    - Pour les ressources basées sur RPM, exécutez l'une des commandes suivantes :

      ```
      sudo dnf autoremove
      ```

      ```
      sudo yum autoremove
      ```

    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 les systèmes d'exploitation basés sur Debian : ksc-web-console-<numéro de build>.x86_64.deb
- Pour les systèmes d'exploitation basés sur RPM : ksc-web-console-[build_number].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. La localisation du fichier est /etc/ksc-web-console-setup.json.

   Si, lors de l'installation de Kaspersky Security Center Web Console, vous avez spécifié les valeurs des paramètres `webConsoleAccount`, `managementServiceAccount`, `serviceWebConsoleAccount`, `pluginAccount` et `natsMessageQueueAccount`, assurez-vous que tous ces paramètres sont indiqués dans le fichier de réponses.

   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 contenant l'ensemble minimal de paramètres

   L'ensemble des paramètres du fichier de réponse dépend de la version du Serveur d'administration auquel Kaspersky Security Center Web Console se connecte :

   - Serveur d'administration 16 ou versions ultérieures

     Exemple de fichier de réponse avec l'ensemble minimal de paramètres pour se connecter au Serveur d'administration version 16 ou version ultérieure :

```
{
    "address": "ksc-web-console.example.com",
    "port": 8080,
    "trusted":  {
        "Administration Server v16": {
            "iamHost": "ksc16.example.com",
            "iamOAuthPort": 4444,
            "iamProxyPort": 9050,
            "iamCertPath": "/var/opt/kaspersky/klnagent_srv/iam/main_certificate.pem",
            "iamPATPath": "/var/opt/kaspersky/klnagent_srv/iam/initial_token.txt",
            "kscPort": 13299,
            "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
        }
    },
    "certDomain":"ksc-web-console.example.com",
    "acceptEula": true
}
```

- Serveur d'administration 15.4 ou versions ultérieures

  Exemple de fichier de réponse avec l'ensemble minimal de paramètres pour se connecter au Serveur d'administration version 15.4 ou version antérieure :

```
{
    "address": "ksc-web-console.example.com",
    "port": 8080,
    "trusted":  {
         "Administration Server v15.4": {
             "kscHost": "ksc.example.com",
             "kscPort": 13299,
             "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
         }
    },
    "certDomain":"ksc-web-console.example.com",
    "acceptEula": true
}
```

Vous pouvez installer Kaspersky Security Center Web Console soit sur le même appareil que le Serveur d'administration, soit sur un autre appareil. Si Kaspersky Security Center Web Console est installé sur un autre appareil, l'adresse de Kaspersky Security Center Web Console (définie par `address`) et l'adresse du Serveur d'administration (définie par `iamHost` ou `kscHost`) diffèrent. Si Kaspersky Security Center Web Console est installé sur le même appareil qui héberge le Serveur d'administration, ces paramètres ont les mêmes valeurs.

La valeur `iamHost` doit correspondre à l'adresse IAM spécifiée lors de l'installation du Serveur d'administration. Pour obtenir l'adresse IAM indiquée, exécutez la commande suivante sur l'appareil sur lequel le Serveur d'administration est installé :

```
grep "iam_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml
```

Pour en savoir plus, consultez l'article : Paramètres d'installation de Kaspersky Security Center Web Console.

Vous pouvez ajouter plusieurs Serveurs d'administration de différentes versions à la liste des serveurs approuvés. Dans ce cas, les Serveurs peuvent utiliser différentes méthodes d'authentification.

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.

Composants du **paramètre d'installation** `trusted`

Si vous vous connectez au cluster de basculement de Kaspersky Security Center Linux à l'aide de l'authentification de domaine avec l'authentification unique, précisez le paramètre d'installation approuvé comme suit : si vous connectez Kaspersky Security Center Web Console au Serveur d'administration version 16 ou ultérieure, l'authentification de domaine avec l'authentification unique (SSO) fournie par le Gestionnaire des identités et des accès (IAM) sera utilisée. Dans ce cas, précisez le paramètre d'installation `trusted` comme suit :

```
"trusted":  {
  "<nom du Serveur d'administration>": {
    "iamHost": "ksc-iam.example.com",
    "iamOAuthPort": 4444,
    "iamProxyPort": 9050,
    "iamCertPath": "<dossier de données partagé>/iam/main_certificate.pem",
    "iamPATPath": "<dossier de données partagé>/iam/initial_token.txt",
    "kscPort": 13299,
    "kscCertPath": "<dossier de données partagé>/1093/cert/klserver.cer"
```

```
    }
  }
```

où :

- `< nom du Serveur d'administration >` est le nom du cluster de basculement Kaspersky Security Center Linux qui s'affichera dans la fenêtre de connexion de Kaspersky Security Center Web Console.

- `iamHost` est l'adresse de l'appareil sur lequel le Serveur d'administration et IAM sont installés. Si vous avez créé la carte réseau virtuelle lors de la préparation des nœuds du cluster, utilisez le FQDN ou le nom d'hôte de la carte comme adresse du cluster de basculement Kaspersky Security Center Linux. Dans le cas contraire, indiquez le FQDN ou le nom d'hôte du répartiteur de charge tiers que vous utilisez.

  La valeur `iamHost` doit correspondre à l'adresse IAM spécifiée lors de l'installation du Serveur d'administration. Pour obtenir l'adresse IAM indiquée, exécutez la commande suivante sur l'appareil sur lequel le Serveur d'administration est installé :

  ```
  grep "iam_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml
  ```

- `iamOAuthPort` est le port utilisé pour échanger les jetons d'authentification via le protocole d'authentification OpenID Connect (la valeur par défaut est 4444). Ce port est utilisé à la fois pour la communication entre Kaspersky Security Center Web Console Server et le Serveur d'administration, et entre le navigateur (utilisé avec Kaspersky Security Center Web Console) et le Serveur d'administration.

- `iamProxyPort` est le port utilisé pour connecter Kaspersky Security Center Web Console Server au Serveur d'administration (la valeur par défaut est 9050).

- `iamCertPath` est le chemin d'accès au certificat IAM. Le certificat IAM est créé automatiquement lors de la première exécution du Serveur d'administration. Le certificat se trouve sur l'appareil sur lequel le Serveur d'administration est installé. Le chemin par défaut vers le certificat est le suivant : `< dossier de données partagé >/iam/main_certificate.pem`. Le certificat se trouve dans le stockage de données partagé du cluster de basculement Kaspersky Security Center Linux. La rotation du certificat IAM auto-signé est effectuée automatiquement.

- `iamPATPath` est le chemin d'accès au jeton utilisé pour l'enregistrement de Kaspersky Security Center Web Console en tant que client OAuth dans IAM. Ce fichier est généré automatiquement lors de la première exécution du Serveur d'administration. Le jeton se trouve sur l'appareil sur lequel le Serveur d'administration est installé. Le chemin par défaut vers le jeton est le suivant : <dossier de données partagé>/iam/jeton_initial.txt. Le jeton se trouve dans le stockage de données partagé du cluster de basculement Kaspersky Security Center Linux. Le jeton est valide indéfiniment et ne nécessite pas de rotation.

- `kscPort` est le port OpenAPI utilisé par Kaspersky Security Center Web Console pour se connecter au Serveur d'administration (la valeur par défaut est 13299).

- `kscCertPath` est le certificat du Serveur d'administration qui 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 : `< dossier de données partagé >\1093\cert\klserver.cer`.

  > Copiez le fichier de certificat du Serveur d'administration (spécifié par `kscCertPath`), le fichier de certificat IAM (spécifié par `iamCertPath`) et le fichier du jeton (spécifié par `iamPATPath`) depuis le stockage partagé des données sur l'appareil sur lequel vous installez Kaspersky Security Center Web Console. Indiquez le chemin d'accès local au certificat du Serveur d'administration.

Si vous connectez Kaspersky Security Center Web Console à la version 15.4 ou toute version antérieure du Serveur d'administration, l'authentification s'effectuera en précisant le nom et le mot de passe de l'utilisateur du domaine ou de l'utilisateur interne. Dans ce cas, précisez le paramètre d'installation de confiance comme suit :

```
"trusted":  {
  "<nom du Serveur d'administration>": {
    "kscHost": "ksc.example.com",
    "kscPort": 13299,
    "kscCertPath": "<dossier de données partagé>/1093/cert/klserver.cer"
  }
}
```

où :

- `<nom du Serveur d'administration>` est le nom du cluster de basculement Kaspersky Security Center Linux qui s'affichera dans la fenêtre de connexion de Kaspersky Security Center Web Console.
- `kscHost` est l'adresse du Serveur d'administration (FQDN ou nom d'hôte). Si vous avez créé la carte réseau virtuelle lors de la préparation des nœuds du cluster, utilisez l'adresse de la carte comme adresse du cluster de basculement Kaspersky Security Center Linux. Dans le cas contraire, indiquez l'adresse du répartiteur de charge tiers que vous utilisez.
- `kscPort` est le port OpenAPI utilisé par Kaspersky Security Center Web Console pour se connecter au Serveur d'administration (la valeur par défaut est 13299).
- `kscCertPath` est le certificat du Serveur d'administration qui 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 : `<dossier de données partagé>\1093\cert\klserver.cer`. Copiez le fichier de certificat du stockage de données partagé sur l'appareil sur lequel vous installez Kaspersky Security Center Web Console. Indiquez le chemin d'accès local au certificat du Serveur d'administration.

Kaspersky Security Center Web Console ne peut pas être mis à jour à l'aide du même fichier d'installation. 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 yum install ksc-web-console-<numéro_compilation>.x86_64.rpm`
   - Pour les appareils exécutant un système d'exploitation basé sur Debian :
     `sudo apt-get install ksc-web-console-<numéro_compilation>.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. La localisation 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 contenant l'ensemble minimal de paramètres

   L'ensemble des paramètres du fichier de réponse dépend de la version du Serveur d'administration auquel Kaspersky Security Center Web Console se connecte :

   - Serveur d'administration 16 ou versions ultérieures

     Exemple de fichier de réponse avec l'ensemble minimal de paramètres pour se connecter au Serveur d'administration version 16 ou version ultérieure :

```
{
    "address": "ksc-web-console.example.com",
    "port": 8080,
    "trusted":  {
        "Administration Server v16": {
            "iamHost": "ksc16.example.com",
            "iamOAuthPort": 4444,
            "iamProxyPort": 9050,
            "iamCertPath": "/var/opt/kaspersky/klnagent_srv/iam/main_certificate.pem",
            "iamPATPath": "/var/opt/kaspersky/klnagent_srv/iam/initial_token.txt",
            "kscPort": 13299,
            "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
        }
    },
    "certDomain":"ksc-web-console.example.com",
    "acceptEula": true
}
```

- Serveur d'administration 15.4 ou versions ultérieures

  Exemple de fichier de réponse avec l'ensemble minimal de paramètres pour se connecter au Serveur d'administration version 15.4 ou version antérieure :

```
{
    "address": "ksc-web-console.example.com",
    "port": 8080,
    "trusted":  {
         "Administration Server v15.4": {
             "kscHost": "ksc.example.com",
             "kscPort": 13299,
             "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
         }
    },
    "certDomain":"ksc-web-console.example.com",
    "acceptEula": true
}
```

Vous pouvez installer Kaspersky Security Center Web Console soit sur le même appareil que le Serveur d'administration, soit sur un autre appareil. Si Kaspersky Security Center Web Console est installé sur un autre appareil, l'adresse de Kaspersky Security Center Web Console (définie par `address`) et l'adresse du Serveur d'administration (définie par `iamHost` ou `kscHost`) diffèrent. Si Kaspersky Security Center Web Console est installé sur le même appareil qui héberge le Serveur d'administration, ces paramètres ont les mêmes valeurs.

La valeur `iamHost` doit correspondre à l'adresse IAM spécifiée lors de l'installation du Serveur d'administration. Pour obtenir l'adresse IAM indiquée, exécutez la commande suivante sur l'appareil sur lequel le Serveur d'administration est installé :

```
grep "iam_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml
```

Pour en savoir plus, consultez l'article : [Paramètres d'installation de Kaspersky Security Center Web Console](#).

Vous pouvez ajouter plusieurs Serveurs d'administration de différentes versions à la liste des serveurs approuvés. Dans ce cas, les Serveurs peuvent utiliser différentes méthodes d'authentification.

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 Web 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 apt-get install ksc-web-console-<numéro_compilation>.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

La migration de Kaspersky Security Center Windows vers Kaspersky Security Center Linux est possible à l'aide de la copie de sauvegarde des données du Serveur d'administration (avec l'utilitaire klbackup) et de l'Assistant de migration.

Le tableau ci-dessous permet de comparer les principales caractéristiques et limites de la migration à l'aide de la copie de sauvegarde des données du Serveur d'administration et de l'Assistant de migration, afin de déterminer l'approche la plus adaptée à votre organisation.

Paramètres	Copie de sauvegarde des données du Serveur d'administration	Assistant de migration
Processus de migration	Création d'une sauvegarde complète des données du Serveur d'administration Windows de Kaspersky Security Center et restauration sur un Serveur d'administration de Kaspersky Security Center Linux	Sélection et exportation des données du Serveur d'administration pour la migration, importation de ces données vers le Serveur d'administration de Kaspersky Security Center Linux, et migration des appareils administrés sous la gestion de Kaspersky Security Center
Caractéristiques de la méthode de migration	• Migration de toutes les données du Serveur d'administration • Migration d'un nombre quelconque d'appareils administrés • Permet d'obtenir une copie complète des données du Serveur d'administration de Kaspersky Security Center Windows et de les transférer vers le Serveur d'administration de Kaspersky Security Center Linux	• Migration partielle des données du Serveur d'administration • La sélection des objets à migrer est disponible • Le groupe d'administration ou le sous-groupe à migrer ne peut pas contenir plus de 10 000 appareils • Utilisé pour transférer partiellement les données du Serveur d'administration, y compris uniquement les objets de groupe situés dans le périmètre de migration. Les objets de groupe situés en dehors du périmètre de migration doivent être restaurés manuellement
Zone de migration	Transfert complet des données du Serveur d'administration avec un nombre illimité d'appareils administrés	• Structure des groupes d'administration • Appareils administrés inclus dans les groupes d'administration (**10 000 appareils maximum**) • Tags attribués aux appareils migrés • Tâches globales de l'Agent d'administration et des applications gérées (pas pour le Serveur d'administration) • Tâches de groupe de l'Agent d'administration et des applications administrées • Stratégies des applications administrées • Modèles de rapports • Rôle de l'utilisateur • Utilisateurs et groupes de sécurité internes • Catégories d'applications personnalisées avec contenu ajouté manuellement • Sélections d'appareils personnalisés
Zone non migrée	—	• Tâches globales du Serveur d'administration • Événements enregistrés sur le Serveur d'administration • Le stockage des distributifs des applications pour l'installation à distance • Certificat du Serveur d'administration • Clés de licence utilisées par le Serveur d'administration et les applications administrées • Serveurs d'administration virtuels • Paramètres de la stratégie de l'Agent d'administration • Règles de déplacement des appareils • Règles d'exécution pour l'attribution automatique de tags aux appareils • Points de distribution • Paramètres de l'application Kaspersky enregistrés sur le Serveur d'administration
Versions de Kaspersky Security Center prenant en charge les migrations	• Toute version prise en charge de Kaspersky Security Center Windows • Kaspersky Security Center Linux version 15.2 ou ultérieure	• Kaspersky Security Center Windows version 14.2 ou ultérieure • Kaspersky Security Center Linux version 15 ou ultérieure
SGBD entre lesquels la migration est possible	• Microsoft SQL Server → MySQL, MariaDB • Microsoft SQL Server → PostgreSQL, Postgres Pro (uniquement pour la migration de Kaspersky Security Center Windows version 14.2 ou version ultérieure avec le correctif installé vers Kaspersky Security Center Linux version 15.3 ou une version ultérieure) • MySQL → MySQL, MariaDB • MariaDB → MySQL, MariaDB • PostgreSQL → PostgreSQL Postgres Pro → Postgres Pro (uniquement pour la migration de Kaspersky Security Center Windows version 15.1 ou version ultérieure vers Kaspersky Security Center Linux version 16 ou version ultérieure)	Migration entre les SGBD pris en charge sans limitations

Migration vers Kaspersky Security Center Linux à l'aide de la sauvegarde des données du Serveur d'administration

Vous pouvez utiliser une sauvegarde des données pour migrer les données du Serveur d'administration de Kaspersky Security Center Windows vers Kaspersky Security Center Linux. Avant la migration, assurez-vous que les fonctionnalités nécessaires de Kaspersky Security Center Windows sont prises en charge dans Kaspersky Security Center Linux.

Pour plus de clarté, un tutoriel vidéo sur la migration des données du Serveur d'administration vers Kaspersky Security Center Linux à l'aide d'une sauvegarde est disponible.

Restrictions

- La migration peut être effectuée entre les SGBD suivants :
  - Microsoft SQL Server → MySQL, MariaDB
  - Microsoft SQL Server → PostgreSQL, Postgres Pro
  - MySQL → MySQL, MariaDB
  - MariaDB → MySQL, MariaDB
  - PostgreSQL → PostgreSQL
  - Postgres Pro → Postgres Pro
- La migration des données du Serveur d'administration stockées dans la base de données de Microsoft SQL Server, MySQL ou MariaDB vers MySQL ou MariaDB est prise en charge pour la migration à partir de toute version prise en charge de Kaspersky Security Center Windows vers Kaspersky Security Center Linux 15.2 ou une version ultérieure.
- La migration des données du Serveur d'administration stockées dans la base de données de Microsoft SQL Server vers PostgreSQL ou Postgres Pro est prise en charge pour la migration de Kaspersky Security Center Windows version 15.1 ou une version ultérieure vers Kaspersky Security Center Linux version 15.3 ou une version ultérieure.

  Pour prendre en charge la migration vers PostgreSQL ou Postgres Pro, vous devez contacter le Support Technique de Kaspersky et installer l'un des correctifs suivants :
- Pour Kaspersky Security Center 15.1 Windows : 15.1.0.20748-pf2

  La migration vers PostgreSQL ou Postgres Pro est également disponible après la mise à jour de Kaspersky Security Center Windows vers la version 15.1.0.22239.
- Si vous utilisez MySQL ou MariaDB comme SGBD pour Kaspersky Security Center Windows et pour Kaspersky Security Center Linux, le paramètre `lower_case_table_names` doit correspondre pour le SGBD actuel et le nouveau.

  Avant de créer une sauvegarde des données, vérifiez le paramètre `lower_case_table_names`. Ainsi, lors de l'installation de MySQL ou MariaDB pour Kaspersky Security Center Linux, vous devez définir ce paramètre sur la même valeur que celle de ce paramètre pour Windows.

Prérequis

Avant de commencer, **vérifiez les conditions requises pour obtenir un certificat personnalisé**.

> Si vous utilisez un certificat personnalisé au lieu du certificat auto-signé, avant de mettre à niveau Kaspersky Security Center Linux vers une version plus récente, vous devez vous assurer que le certificat inclut le nom alternatif du sujet (SAN). Si ce n'est pas le cas, il est important de remplacer le certificat avant de mettre à niveau Kaspersky Security Center Linux. Sinon, vous ne pourrez pas vous connecter à Web Console après la mise à niveau.

Pour vous assurer que le certificat inclut un SAN, procédez comme suit :

1. Sur l'appareil sur lequel le Serveur d'administration est installé, exécutez la commande suivante :

   - Pour un appareil fonctionnant sous Linux :

     ```
     sudo openssl x509 -in /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -
     noout -ext subjectAltName
     ```

   - Pour un appareil fonctionnant sous Windows :

     ```
     certutil -dump %ProgramData%\KasperskyLab\adminkit\1093\cert\klserver.cer
     ```

2. Assurez-vous que le nom alternatif du sujet (SAN) figure dans la sortie de la commande et qu'il contient l'adresse de l'appareil du Serveur d'administration.

3. Si le nom alternatif du sujet est absent, utilisez l'utilitaire klsetsrvcert pour remplacer votre certificat utilisateur par un certificat conforme aux exigences.

Étapes

La migration à l'aide de la sauvegarde des données du Serveur d'administration se déroule par étapes :

1. **Vérifiez que vous disposez du compte utilisateur interne de l'administrateur sous lequel vous pouvez vous connecter au Serveur d'administration.**

   Le compte de l'administrateur sera utilisé pour se connecter au Serveur d'administration de Kaspersky Security Center Linux. Si vous ne disposez pas de ce compte et que vous êtes connecté uniquement sous un compte Windows local ou sous un compte de domaine, vous ne pourrez pas vous connecter au Serveur d'administration de Kaspersky Security Center Linux après la restauration de la sauvegarde. Le Serveur d'administration de Kaspersky Security Center Linux ne prend pas en charge la connexion à l'aide du compte Windows local. Il est possible de se connecter sous le compte de domaine, mais cela peut nécessiter une configuration supplémentaire du Serveur d'administration.

   Si vous ne disposez pas du compte d'administrateur, vous devrez créer ce compte après avoir restauré la copie de sauvegarde à l'aide de l'utilitaire kladduser.

2. **Création d'une copie de sauvegarde à jour des données du Serveur d'administration de Kaspersky Security Center Windows**

   En fonction du type de SGBD utilisé pour Kaspersky Security Center Windows et Kaspersky Security Center Linux, exécutez une des actions suivantes :

   - Pour la migration de MySQL ou MariaDB vers MySQL ou MariaDB : créez une copie de sauvegarde à l'aide de l'utilitaire klbackup ou une tâche de sauvegarde des données sur l'appareil sur lequel le Serveur d'administration est installé.

   - Pour la migration des données de PostgreSQL vers PostgreSQL et de Postgres Pro vers Postgres Pro : créez une copie de sauvegarde à l'aide de l'utilitaire klbackup ou de tâches de sauvegarde des données sur l'appareil sur lequel le Serveur d'administration est installé.

   - Pour la migration de Microsoft SQL Server vers MySQL ou MariaDB : créez une copie de sauvegarde à l'aide de l'utilitaire klbackup en activant l'option **Migrer au format MySQL/MariaDB**.

- Pour la migration de Microsoft SQL Server vers PostgreSQL ou Postgres Pro :

  1. Installez le correctif pour le Serveur d'administration afin de prendre en charge la migration vers PostgreSQL et Postgres Pro. Contactez le support technique de Kaspersky pour obtenir ce correctif.

     Pour Kaspersky Security Center 15.1 Windows, vous pouvez procéder à la mise à jour vers la version 15.1.0.22239 au lieu d'installer le correctif.

  2. Créez une copie de sauvegarde à l'aide de l'utilitaire klbackup.

     Si vous exécutez l'utilitaire klbackup via la ligne de commande, utilisez l'indicateur `-migrate postgres`.

     Si vous utilisez l'interface klbackup, activez l'option **Migrer vers le format Postgres**.

Après avoir créé une copie de sauvegarde, déconnectez du réseau le Serveur d'administration de Kaspersky Security Center Windows.

3. **Préparation d'un nouvel appareil en vue de l'installation de Kaspersky Security Center Linux**

À cette étape du scénario, procédez comme suit :

1. Sélectionnez un nouvel appareil sur lequel installer le Serveur d'administration. Cet appareil doit répondre à la configuration matérielle et logicielle requise. Vérifiez également que les ports utilisés sur le Serveur d'administration sont disponibles.

2. Attribuez la même adresse au nouvel appareil.

   Le nouveau Serveur d'administration peut recevoir le nom NetBIOS, le FQDN et l'adresse IP statique. Cela dépend de l'adresse du Serveur d'administration qui a été définie dans le paquet d'installation de l'Agent d'administration lors du déploiement des Agents d'administration. Vous pouvez également utiliser l'adresse de connexion qui détermine le Serveur d'administration auquel l'Agent d'administration se connecte (vous pouvez obtenir cette adresse sur les appareils administrés à l'aide de l'utilitaire klnagchk).

4. **Installation et configuration du SGBD**

À cette étape du scénario, procédez comme suit :

1. Sélectionnez le type de SGBD qui offre des performances optimales. Tenez compte du nombre d'appareils en réseau, de la topologie du réseau et de la charge de travail sur le réseau. Vous pouvez choisir n'importe quel SGBD pris en charge.

2. Installez le SGBD selon le type de SGBD sélectionné lors de la création de la sauvegarde. Pour en savoir plus sur l'installation du SGBD sélectionné, consultez sa documentation.

   Créez manuellement une base de données pour IAM.

   > La nouvelle version de la base de données ne doit pas être antérieure à la version actuelle.

3. Configurez le SGBD pour qu'il fonctionne avec Kaspersky Security Center Linux :

- 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

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

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

   Installez Kaspersky Security Center Linux sur le nouvel appareil.

   Le compte utilisateur interne de l'administrateur créé lors de l'installation, ainsi que les autres objets (groupes, stratégies, tâches, utilisateurs) créés avant que vous ne restauriez les données du Serveur d'administration à partir de la sauvegarde, seront perdus après la restauration. Ces objets seront remplacés par des objets contenus dans la sauvegarde.

6. **Restauration des données du Serveur d'administration à partir de la copie de sauvegarde**

   À cette étape du scénario, procédez comme suit :

   1. Restaurez les données du Serveur d'administration sur le nouvel appareil à l'aide de l'utilitaire klbackup.

      En raison des limitations de PostgreSQL, vous devez accorder temporairement des privilèges de superutilisateur PostgreSQL au compte que le Serveur d'administration utilise pour se connecter au SGBD.

   2. Si vous ne disposiez pas du compte utilisateur interne de l'administrateur sous lequel vous étiez connecté au Serveur d'administration de Kaspersky Security Center Windows et que vous utilisiez un compte Windows local ou un compte de domaine, créez un compte d'administrateur en utilisant l'utilitaire kladduser comme suit :

      ```
      /opt/kaspersky/ksc64/sbin/kladduser -n kscadmin -p <mot de passe>
      ```

      où le paramètre `<mot de passe>` remplit les conditions suivantes :

      - Le mot de passe utilisateur ne doit pas comporter moins de 8 ni plus de 256 caractères.
      - Le mot de passe doit compter des caractères d'au moins trois des groupes ci-dessous :
        - Lettres majuscules (A–Z)
        - Lettre minuscules (a-z)
        - Chiffres (0–9)
        - Caractères spéciaux (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)

7. **Configuration de la vérification des certificats par le Serveur d'administration et le serveur IAM.**

8. **Installation de Kaspersky Security Center Web Console et configuration du Serveur d'administration**

   À cette étape du scénario, procédez comme suit :

   1. Installez Kaspersky Security Center Web Console.

      Si Kaspersky Security Center Web Console a été installé précédemment, réinstallez-le avec le même fichier de réponse.

      Connectez-vous à Kaspersky Security Center Web Console sous le compte utilisateur interne de l'administrateur.

      Le processus d'initialisation des données dure généralement jusqu'à 15 minutes après la restauration des données du Serveur d'administration. Toutefois, cette durée dépend de la performance du matériel et de la taille des données du Serveur d'administration. Pendant ce temps, Kaspersky Security Center Web Console peut ne pas réussir à se connecter et afficher alors les erreurs.

2. Vérifiez le fonctionnement des principales fonctions du Serveur d'administration lorsque l'initialisation des données dans la base de données est terminée. Vérifiez que le Serveur d'administration se synchronise avec les appareils gérés et que les données du Serveur d'administration sont récupérées.

3. Interrogez les contrôleurs de domaine pour récupérer les informations sur la structure du domaine, les comptes utilisateurs, les groupes de sécurité et les noms DNS des appareils inclus dans les domaines.

4. Passez en revue les tâches migrées. Si l'un de leurs paramètres comprend un chemin d'accès au fichier Windows, remplacez-le par le chemin d'accès au fichier Linux correspondant.

5. Si nécessaire, désinstallez le Serveur d'administration et le serveur de base de données de l'appareil précédent.

   Il ne doit pas y avoir plusieurs Serveurs d'administration partageant la même adresse de connexion ni le même certificat de Serveur d'administration sur le même réseau.

L'administrateur a accès aux données du Serveur d'administration et aux appareils administrés qui se trouvaient dans Kaspersky Security Center Windows, en tenant compte des fonctionnalités prises en charge dans Kaspersky Security Center Linux.

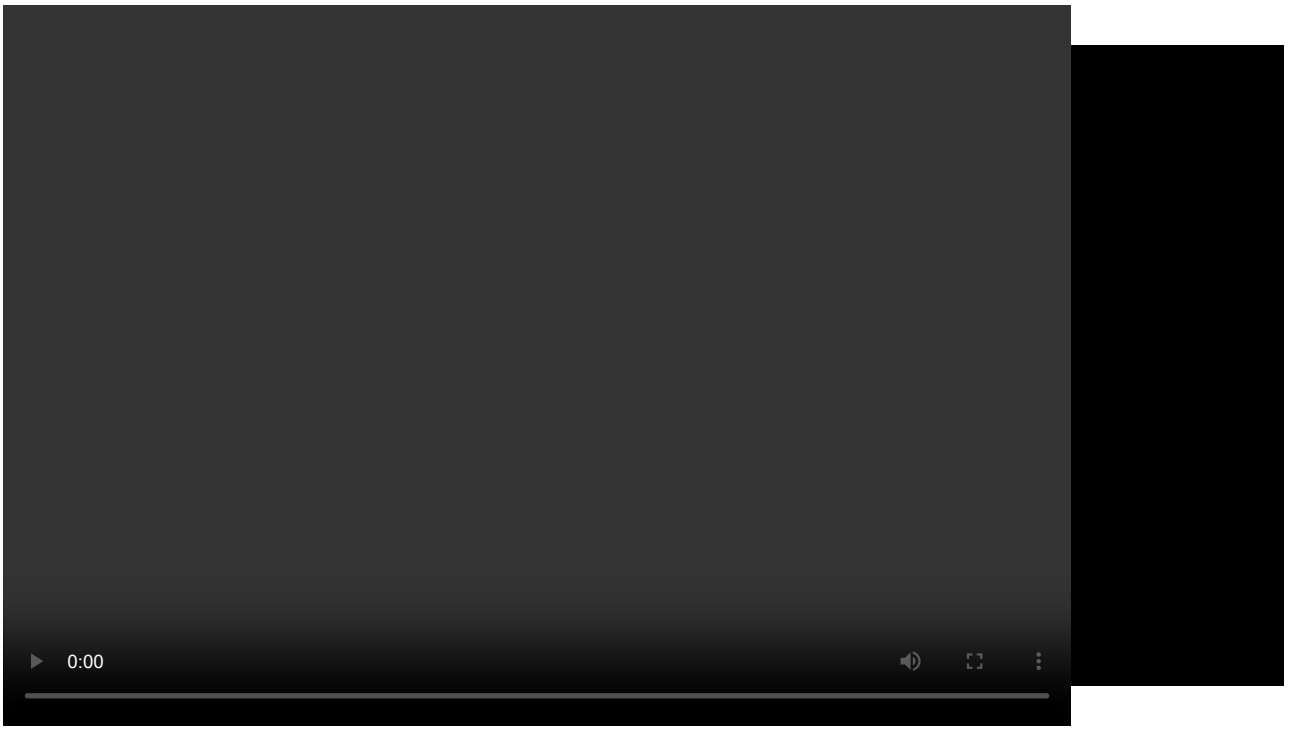
Tutoriel vidéo : Migration vers Kaspersky Security Center Linux à l'aide de la sauvegarde des données du Serveur d'administration

Regardez la vidéo pour découvrir comment migrer les données du Serveur d'administration de Kaspersky Security Center Windows vers Kaspersky Security Center Linux à l'aide de la sauvegarde des données du Serveur d'administration (avec l'utilitaire klbackup).

Pour prendre en charge la migration des données vers PostgreSQL ou Postgres Pro, contactez le Support technique de Kaspersky et installez l'un des correctifs suivants :

– Pour Kaspersky Secure Mobility Management basé sur Kaspersky Security Center 14.2 Windows : 14.2.0.48079-pf5
– Pour Kaspersky Security Center 15.1 Windows : 15.1.0.20748-pf2

La migration des données vers PostgreSQL ou Postgres Pro est également disponible après la mise à jour de Kaspersky Security Center Windows vers la version 15.1.0.22239.



Migration vers Kaspersky Security Center Linux à l'aide de la sauvegarde des données du Serveur d'administration. Enregistrements vidéo

Migration vers Kaspersky Security Center Linux à l'aide de l'Assistant de migration

Suite à ce scénario, vous pouvez transférer la structure du groupe d'administration, les appareils administrés inclus et les autres objets du groupe (stratégies, tâches, tâches globales, tags et sélections d'appareils) depuis Kaspersky Security Center Windows sous l'administration de Kaspersky Security Center Linux.

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. **Sauvegarder le certificat et la clé privée du Serveur d'administration de Kaspersky Security Center Windows (étape facultative)**

   Vous pouvez placer les appareils administrés sous la gestion du Serveur d'administration de Kaspersky Security Center Linux en restaurant le certificat et la clé privée du Serveur d'administration à partir d'une copie de sauvegarde. Dans ce cas, sauvegardez le certificat et la clé privée du Serveur d'administration de Kaspersky Security Center Windows. Ensuite, à l'étape 6, vous devez restaurer le certificat et la clé privée.

3. **Exporter des données depuis Kaspersky Security Center Windows**

   Ouvrez Kaspersky Security Center Windows, puis lancez l'Assistant de migration.

4. **Importer des données dans Kaspersky Security Center Linux**

   Poursuivez l'Assistant de migration pour importer les données exportées dans Kaspersky Security Center Linux. Si les Serveurs sont hiérarchiques, l'importation démarre automatiquement après un export réussi dans le même Assistant. Si les Serveurs ne sont pas hiérarchiques, vous continuerez l'Assistant de migration après le passage à Kaspersky Security Center Linux.

5. **Exécuter les actions complémentaires pour transférer manuellement les objets et les paramètres de Kaspersky Security Center Windows vers Kaspersky Security Center Linux (étape facultative)**

   Vous souhaiterez peut-être également transférer les objets et les paramètres qui ne peuvent pas être transférés via l'Assistant de migration. Par exemple, vous pouvez également effectuer les opérations suivantes :

   - Transférer les clés de licence utilisées par le Serveur d'administration et les applications administrées
   - Configurer les tâches globales du Serveur d'administration
   - Configurer les paramètres de la stratégie de l'Agent d'administration
   - Créez des paquets d'installation des applications
   - Créez des Serveurs virtuels
   - 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.

6. **Déplacez les appareils administrés par Kaspersky Security Center Linux administré**

   Pour terminer la migration, déplacez les appareils administrés importés sous l'administration de Kaspersky Security Center Linux. Vous pouvez le faire de l'une des manières suivantes :

   - Via l'utilitaire klmover

     Utilisez l'utilitaire klmover et définissez les paramètres de connexion pour le nouveau Serveur d'administration.

   - Via la tâche *Modification du Serveur d'administration*

     Créez une tâche *Modification du Serveur d'administration*, et définissez les appareils administrés importés, le nouveau Serveur d'administration et d'autres paramètres de la tâche. Exécutez ensuite la tâche pour placer les appareils administrés sous la gestion du Serveur d'administration de Kaspersky Security Center Linux.

   - Par la suppression (si déjà installé) et la poursuite de l'installation de l'Agent d'administration sur les appareils administrés

     Créez un nouveau paquet d'installation de l'Agent d'administration et définissez les paramètres de connexion pour le nouveau Serveur d'administration dans les propriétés du paquet d'installation. Supprimez l'Agent d'administration sur les appareils administrés importés, puis utilisez le paquet d'installation pour installer l'Agent d'administration sur les appareils administrés importés via une tâche d'installation à distance. Vous pouvez également créer et utiliser un paquet d'installation autonome pour installer l'Agent d'administration localement. Pour plus d'informations, consultez Basculer les appareils administrés sous l'administration de Kaspersky Security Center Linux.

   - Par la restauration du certificat et de la clé privée du Serveur d'administration à partir d'une copie de sauvegarde (uniquement pour la migration vers Kaspersky Security Center Linux 15.1 ou une version ultérieure)

     Attribuez la même adresse réseau à l'appareil équipé du Serveur d'administration de Kaspersky Security Center Linux que sur le Serveur d'administration de Kaspersky Security Center Windows. Lancez l'utilitaire klbackup avec le paramètre `-cert_only` pour restaurer le certificat du Serveur d'administration et la clé privée à partir de la copie de sauvegarde que vous avez enregistrée à l'étape 2. Dans la ligne de commande, exécutez la commande suivante : `/opt/kaspersky/ksc64/sbin/klbackup -path <chemin d'accès à la copie de sauvegarde du certificat du Serveur d'administration> -restore -cert_only`. Pour plus de détails, consultez la section Utilisation de l'utilitaire klbackup pour basculer des appareils administrés sous l'administration d'un autre Serveur d'administration.

7. **Mettre à jour l'Agent d'administration vers la dernière version**

   Nous vous recommandons de mettre à jour l'Agent d'administration pour Linux vers la même version que Kaspersky Security Center.

8. **Assurez-vous que les appareils administrés sont visibles sur le nouveau Serveur d'administration**

   Sur le Serveur d'administration de Kaspersky Security Center Linux, ouvrez la liste des appareils administrés (**Gestion des ressources** → **Ressources (Appareils)**) 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 **Passer à Kaspersky Security Center Linux ou à Open 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 l'application 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 **Gestion des ressources** et assurez-vous que les objets importés apparaissent dans les sous-sections correspondantes.

Notez que les appareils gérés importés sont affichés dans la sous-section **Appareils administrés**, mais ils sont invisibles sur le réseau et l'Agent d'administration n'est pas installé ni exécuté sur eux (la valeur *Non* dans les colonnes **Visible**, **L'Agent d'administration est installé** et **L'Agent d'administration est en cours d'exécution**).

Pour terminer la migration, vous devez faire en sorte que les appareils administrés soient administrés par Kaspersky Security Center Linux.

Basculer les appareils administrés vers l'administration de Kaspersky Security Center Linux

Après une importation réussie des informations sur les appareils administrés, les objets et leurs paramètres vers Kaspersky Security Center Linux, vous devez faire passer les appareils administrés sous l'administration de Kaspersky Security Center Linux pour terminer la migration.

Vous pouvez déplacer les appareils administrés vers Kaspersky Security Center Linux d'une des manières suivantes :

- Via l'utilitaire klmover.

- Via la tâche *Modification du Serveur d'administration*.

- Restauration du certificat et de la clé privée du Serveur d'administration à partir d'une copie de sauvegarde (uniquement pour la migration vers Kaspersky Security Center Linux 15.1 ou une version ultérieure).

  Pour en savoir plus, reportez-vous à l'étape 6 du scénario de migration principal.

- Installation de l'Agent d'administration sur les appareils administrés via la tâche d'installation à distance.

Pour faire passer les appareils administrés sous l'administration de Kaspersky Security Center Linux en installant l'Agent d'administration :

1. Supprimez l'Agent d'administration sur les appareils administrés importés qui passeront sous la gestion de Kaspersky Security Center Linux.

2. Basculez vers le Serveur d'administration de Kaspersky Security Center Windows.

3. Accédez à **Découverte et déploiement** → **Déploiement et attribution** → **Paquets d'installation**, puis ouvrez les propriétés d'un package d'installation existant de l'Agent d'administration.

   Si le paquet d'installation de l'Agent d'administration est absent de la liste des paquets, téléchargez-en un nouveau.

   Vous pouvez également créer et utiliser un paquet d'installation autonome pour installer l'Agent d'administration localement.

4. Sous l'onglet **Paramètres**, sélectionnez la section **Connexion**. Spécifiez les paramètres de connexion du Serveur d'administration de Kaspersky Security Center Linux.

5. Créez une tâche d'installation à distance pour les appareils administrés, puis spécifiez le paquet d'installation de l'Agent d'administration reconfiguré.

   Vous pouvez installer l'Agent d'administration via le Serveur d'administration de Kaspersky Security Center Windows ou via un appareil Windows faisant office de point de distribution. Si vous utilisez le Serveur d'administration, activez l'option **En utilisant les ressources du système d'exploitation via le Serveur d'administration**. Si vous utilisez un point de distribution, activez l'option **En utilisant les ressources du système d'exploitation via les points de distribution**.

6. Lancez la tâche d'installation à distance de l'application.

Une fois la tâche d'installation à distance terminée, accédez au Serveur d'administration de Kaspersky Security Center Linux et assurez-vous que les appareils administrés sont visibles sur le réseau et que l'Agent d'administration est installé et exécuté sur eux (la valeur *Oui* dans les colonnes **Visible**, **L'Agent d'administration est installé**, et **L'Agent d'administration est en cours d'exécution**).

Configuration du Serveur d'administration

Cette section décrit le processus de configuration et les propriétés du Serveur d'administration.

Configuration de l'adresse de connexion au Serveur d'administration

L'adresse de connexion du Serveur d'administration est l'adresse réseau utilisée aux fins suivantes :

- En tant qu'adresse par défaut lors de la création des paquets d'installation de l'Agent d'administration

  Après l'installation de l'Agent d'administration, les appareils administrés se connectent au Serveur d'administration à cette adresse.

- En tant qu'adresse du serveur proxy KSN

  Les appareils administrés se connectent au serveur proxy KSN via cette adresse.

Pour configurer l'adresse de connexion au Serveur d'administration :

1. Dans le menu principal, cliquez sur le 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. Dans la fenêtre qui s'ouvre, dans le champ **Adresse de connexion au Serveur d'administration** , indiquez la nouvelle adresse de connexion au Serveur d'administration.

   La longueur maximale de l'adresse de connexion est de 255 caractères.

   Vous pouvez spécifier l'adresse de connexion au Serveur d'administration sous la forme du nom NetBIOS, du nom de domaine complet ou de l'adresse IP du Serveur d'administration.

4. Cliquez sur **Enregistrer**.

L'adresse spécifiée est utilisée comme adresse du Serveur d'administration et comme adresse du serveur proxy KSN.

Configuration de la connexion de Kaspersky Security Center Web Console au serveur d'administration

Vous pouvez configurer la connexion de Kaspersky Security Center Web Console au Serveur d'administration via les propriétés du Serveur d'administration ou en utilisant les paramètres de la stratégie du Serveur d'administration.

Pour définir les ports de connexion via les propriétés du Serveur d'administration, procédez comme suit :

1. Dans le menu principal, cliquez sur le nom du Serveur d'administration.

   La fenêtre des propriétés du Serveur d'administration s'ouvre.

2. Sous l'onglet **Général**, sélectionnez la section **Ports de connexion**.

3. Si nécessaire, définissez le paramètre **Port SSL pour Web Console** ou définissez d'autres ports de connexion du Serveur d'administration.

Les principaux paramètres de connexion du Serveur sélectionné sont indiqués.

Pour configurer les ports de connexion via les paramètres de stratégie du Serveur d'administration, procédez comme suit :

1. Dans le menu principal, accédez à **Gestion des ressources** → **Stratégies**.

2. Cliquez sur le nom de la stratégie du Serveur d'administration, puis accédez à l'onglet **Paramètres de l'application**.

3. Si nécessaire, définissez le paramètre **Port SSL pour Web Console** ou définissez d'autres ports de connexion du Serveur d'administration.

   Si vous désactivez l'option **Ouvrir le port pour Web Console** et que ce paramètre de stratégie est appliqué à l'appareil, vous ne pourrez pas vous connecter au Serveur d'administration via Kaspersky Security Center Web Console. Dans ce cas, la connexion sera interrompue. Si vous possédez un Serveur d'administration auquel cette stratégie n'est pas appliquée, vous pouvez vous reconnecter à ce Serveur d'administration via Kaspersky Security Center Web Console.

Les principaux paramètres de connexion du Serveur sélectionné sont indiqués.

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 "<Adresses IP>" -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 "<Adresses IP>"
-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 le 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 du serveur proxy**

     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.

La hiérarchie des Serveurs d'administration prend en charge le mode multilocation. Ce mode permet à un administrateur principal de gérer indépendamment plusieurs clients de manière centralisée. Chaque entreprise cliente ou bureau client est isolé des autres et est appelé locataire. Vous pouvez allouer plusieurs appareils administrés ainsi que leurs données, paramètres, stratégies et tâches associés à un locataire, et configurer les droits des utilisateurs par locataire.

Un Serveur d'administration principal, installé dans l'infrastructure principale de l'entreprise, fait office de locataire principal. Le Serveur d'administration principal permet aux Serveurs d'administration secondaires ou virtuels (ses locataires isolés) de recevoir et de traiter indépendamment leurs propres événements et de fonctionner avec leurs propres ressources, services et configurations.

Un fournisseur de services qui compte plusieurs entreprises clientes peut proposer les fonctionnalités de Kaspersky Security Center Linux, y compris l'agrégation des alertes et les actions de réponse, à chaque entreprise cliente de manière indépendante. Pour ce faire, le fournisseur de services connecte des Serveurs d'administration secondaires ou virtuels en tant que locataires pour chaque entreprise cliente. Le fournisseur de services dispense ses services au moyen de son propre personnel et de ses propres ressources.

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 est disponible.

   Ce port sera utilisé pour l'interaction entre le Serveur d'administration principal et les Serveurs d'administration secondaires une fois la hiérarchie créée.

2. Accédez aux propriétés du futur Serveur d'administration principal :

   a. Dans le menu principal, sélectionnez une section (à l'exception de **Place de marché**, **Navigation dans la console** et **Paramètres**), puis, en haut de la page, cliquez sur le bouton **Afficher la hiérarchie**.

   b. Dans le panneau de navigation qui s'ouvre, placez le curseur de la souris sur le nom du Serveur d'administration requis, puis cliquez sur l'icône des paramètres (⚙).

      Vous pouvez également cliquer sur le nom du Serveur d'administration, puis, une fois que le nom s'affiche dans le menu principal, cliquer dessus dans le menu principal pour ouvrir la fenêtre des propriétés du serveur.

3. Dans la fenêtre 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 :

   - **Connecter le Serveur d'administration principal au Serveur d'administration secondaire dans 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.

   - **Nom d'affichage du Serveur 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 secondaire**

     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**

  Indiquez le numéro du port SSL à utiliser pour l'interaction entre le Serveur d'administration principal et le Serveur d'administration secondaire une fois la hiérarchie créée. Le numéro de port par défaut est 13000.

- **Port API du Serveur**

  Numéro du port que Web Console utilisera pour recevoir les connexions du Serveur d'administration secondaire via OpenAPI. Le numéro de port par défaut est 13299.

  Lors de la création de la hiérarchie, Web Console se connecte au futur Serveur d'administration secondaire, demande les informations d'identification, récupère le certificat public et effectue la configuration initiale.

  Une fois la hiérarchie des Serveurs d'administration créée, le port 13299 ne sera plus utilisé. Les Serveurs d'administration communiqueront via le port 13000.

- **Certificat pour le Serveur d'administration secondaire**

  Ajoutez un fichier de certificat. Vous pouvez charger manuellement le certificat depuis votre appareil ou le récupérer auprès du Serveur d'administration secondaire.

7. Indiquez les paramètres de connexion et d'authentification :

   - Saisissez l'adresse du futur Serveur d'administration primaire.

   - Sélectionnez l'option **Utiliser un serveur proxy** 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 du serveur proxy**

     - **Nom d'utilisateur**

     - **Mot de passe**

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

L'Assistant a terminé son travail, la connexion avec le futur Serveur secondaire est établie et la hiérarchie « primaire/secondaire » est créée.

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 où il a été ajouté.

La connexion échoue dans les cas suivants :

- Les paramètres de connexion sont incorrects.

  Vous devez vérifier les paramètres ou indiquer manuellement le certificat du futur Serveur secondaire.

- 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.

  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.

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 le nom du Serveur d'administration.

   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. Sélectionnez le type de Serveur d'administration principal.

   e. Dans le champ **Adresse du Serveur d'administration principal**, saisissez le nom de réseau du futur Serveur d'administration principal.

   f. Sélectionnez le fichier précédemment enregistré contenant le certificat du futur Serveur d'administration principal en cliquant sur **Indiquer le certificat du Serveur d'administration principal**.

   g. Si nécessaire, cochez la case **Connecter le Serveur d'administration principal au Serveur d'administration secondaire dans la DMZ**.

h. Si la connexion au futur Serveur d'administration principal se fait via un serveur proxy, cochez la case **Utiliser un serveur proxy** et précisez les paramètres de connexion.

i. 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) :

1. Dans le menu principal, sélectionnez une section (à l'exception de **Place de marché**, **Navigation dans la console** et **Paramètres**).

2. En haut de la page, cliquez sur le bouton **Afficher la hiérarchie**.

   Dans le panneau de navigation qui s'ouvre, la liste des Serveurs d'administration secondaires (y compris virtuels) s'affiche. Vous pouvez aller à l'un de ces serveur d'administration en cliquant sur son nom.

Vous ne pouvez pas accéder aux Serveurs d'administration virtuels si vous avez ouvert le panneau de navigation à partir des sections **Plages IP** et **Objets supprimés**.
Les groupes d'administration sont également affichés. Les groupes peuvent être administrés si vous avez ouvert le panneau de navigation à partir des sections suivantes : **Ressources (Appareils)**, **Stratégies**, **Tâches** et **Points de distribution**. Dans le cas contraire, les groupes sont grisés.

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 le nom du Serveur d'administration.
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 au Serveur d'administration**
     Vous pouvez définir le nom ou l'adresse IP de votre Serveur d'administration.

6. Dans la liste des utilisateurs, sélectionnez l'administrateur virtuel du Serveur d'administration. Si vous le souhaitez vous pouvez modifier l'un des comptes existants afin de lui attribuer le rôle de l'administrateur ou de créer un nouveau compte utilisateur.

   Si nécessaire, vous pouvez créer un compte qui agira en tant qu'administrateur du Serveur d'administration virtuel à l'aide de l'utilitaire kladduser. Pour ce faire, utilisez la commande suivante :

   ```
   kladduser -n <nom_d'utilisateur> -p <mot_de_passe> -vs <nom_du_serveur_virtuel>
   ```

   où `virtual_server_name` est le nom du Serveur d'administration virtuel.

7. Cliquez sur **Enregistrer**.

Le nouveau Serveur d'administration virtuel est créé, ajouté au groupe d'administration et s'affiche sous l'onglet **Serveurs d'administration**.

Si vous êtes connecté à votre Serveur d'administration primaire dans Kaspersky Security Center Web Console et que vous ne pouvez pas vous connecter à un Serveur d'administration virtuel administré par un Serveur d'administration secondaire, vous pouvez utiliser l'une des manières suivantes :

- **Modifiez l'installation existante de Kaspersky Security Center Web Console pour ajouter le Serveur secondaire à la liste des Serveurs d'administration de confiance**. Ensuite, vous pourrez vous connecter au Serveur d'administration virtuel dans Kaspersky Security Center Web Console.

  1. Sur l'appareil où Kaspersky Security Center Web Console est installé, exécutez le fichier d'installation 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 le 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 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'objets** dans la zone fonctionnelle **Fonctions générales** → **Autorisations d'utilisateur**.

Configuration manuelle des droits d'accès

Pour désigner un administrateur pour un Serveur d'administration virtuel, procédez comme suit :

1. Basculer vers le Serveur d'administration virtuel requis :

   a. Dans le menu principal, sélectionnez une section (à l'exception de **Place de marché**, **Navigation dans la console** et **Paramètres**), puis, en haut de la page, cliquez sur le bouton **Afficher la hiérarchie**.

   b. Dans le panneau de navigation qui s'ouvre, cliquez sur le nom du Serveur d'administration virtuel requis.

   > Vous ne pouvez pas basculer vers un Serveur d'administration virtuel à partir des sections **Plages IP** et **Objets supprimés**.

   Dans le menu principal, le Serveur d'administration devient celui que vous avez sélectionné.

2. Accédez aux propriétés du Serveur d'administration en cliquant sur son nom dans le menu principal.

   Vous pouvez également, dans le volet de navigation, survoler le nom du Serveur d'administration virtuel requis avec le curseur de la souris, puis cliquer sur l'icône des paramètres (⚙).

   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 **Lecture** dans la zone fonctionnelle **Fonctions générales** → **Fonctionnalité de base**
- Droits de **Lecture** 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. Basculer vers le Serveur d'administration virtuel requis :
   a. Dans le menu principal, sélectionnez une section (à l'exception de **Place de marché**, **Navigation dans la console** et **Paramètres**), puis, en haut de la page, cliquez sur le bouton **Afficher la hiérarchie**.
   b. Dans le panneau de navigation qui s'ouvre, cliquez sur le nom du Serveur d'administration virtuel requis.

   > Vous ne pouvez pas basculer vers un Serveur d'administration virtuel à partir des sections **Plages IP** et **Objets supprimés**.

   Dans le menu principal, le Serveur d'administration devient celui que vous avez sélectionné.
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 **Gestion des ressources** → **Tâches**.
2. Cliquez sur **Ajouter**.

   Ceci permet de lancer l'assistant de création d'une tâche. Parcourez les étapes de l'assistant à l'aide du bouton **Suivant**.
3. À l'étape **Paramètres de nouvelle tâche** de l'assistant, spécifiez les paramètres suivants :

   a. Dans la liste déroulante **Application**, sélectionnez **Kaspersky Security Center**.

   b. Dans le champ **Type de tâche**, sélectionnez **Modification du Serveur d'administration**.

   c. Dans le champ **Nom de la tâche**, renseignez le nom de la tâche que vous créez.

   Le nom de la tâche ne peut pas contenir plus de 100 symboles et contenir de symboles spéciaux ("*<>?\:|).

   d. Sélectionnez les appareils auxquels les tâches seront affectées :

   - **Attribuer la tâche à un groupe d'administration**

     > La tâche est affectée aux appareils qui appartiennent à un groupe d'administration. Vous pouvez renseigner un des groupes existants ou en créer un.
     >
     > Par exemple, vous pourriez souhaiter utiliser cette option pour exécuter une tâche d'envoi de messages pour les utilisateurs si le message est particulier pour les appareils repris dans un groupe d'administration spécifique.
     >
     > Si une tâche est attribuée à un groupe d'administration, l'onglet **Sécurité** ne s'affiche pas dans la fenêtre des propriétés de la tâche, car les tâches de groupe sont soumises aux paramètres de sécurité des groupes auxquels elles s'appliquent.

   - **Définir les adresses des appareils manuellement ou les importer à partir de la 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 d'action d'une 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 requiert une authentification, dans les champs **Nom d'utilisateur** et **Mot de passe**, indiquez les identifiants du compte sous lequel la connexion au serveur proxy est établie. Nous vous recommandons de spécifier les informations d'identification d'un compte disposant des privilèges minimaux requis uniquement pour l'authentification sur le serveur proxy.

     5. Si nécessaire, téléchargez un nouveau certificat de Serveur d'administration.

- **Passer à un autre Serveur virtuel sur ce Serveur principal**

  Sélectionnez cette option pour déplacer les appareils clients vers le Serveur d'administration virtuel sur le Serveur d'administration principal actuel. Pour ce faire, dans 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**

       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. Passez au Serveur d'administration physique principal auquel appartient le Serveur d'administration virtuel à supprimer :

   a. ,Dans le menu principal, sélectionnez n'importe quelle section (à l'exception de **Place de marché**, **Navigation dans la console** et **Paramètres**), puis, en haut de la page, cliquez sur le bouton **Afficher la hiérarchie**.

   b. Dans le panneau de navigation qui s'ouvre, cliquez sur le nom du Serveur d'administration physique principal.

   Dans le menu principal, le Serveur d'administration devient celui que vous avez sélectionné.

2. Accédez aux propriétés du Serveur d'administration physique principal d'une des façons suivantes :

   - Dans le panneau de navigation, survolez le curseur de la souris sur le nom du Serveur d'administration requis, puis cliquez sur l'icône des paramètres (⚙).

   - Dans le menu principal, cliquez sur le nom du Serveur d'administration.

3. Dans la fenêtre des propriétés qui s'ouvre, accédez à l'onglet **Serveurs d'administration**.

4. Sélectionnez le Serveur d'administration virtuel que vous souhaitez supprimer.

5. 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 le nom du Serveur d'administration.

   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 le nom du Serveur d'administration.

   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 du nom du Serveur d'administration

Les étapes à suivre pour modifier le nom du serveur peuvent varier selon votre environnement. Vous pouvez choisir l'un des scénarios suivants pour modifier le nom du serveur :

- Préservation des connexions par l'ajout d'un nouvel enregistrement DNS.
- Préservation des connexions par le passage à une connectivité basée sur les adresses IP.
- Restauration des connexions interrompues après la modification du nom du serveur.

Si vous rencontrez des difficultés pour modifier le nom du serveur, contactez le Support technique.

Préservation des connexions par l'ajout d'un nouvel enregistrement DNS

Dans ce scénario, les appareils administrés et Kaspersky Security Center Web Console continuent de se connecter à l'ancienne adresse du Serveur d'administration après le renommage du Serveur d'administration. Pour ce faire, ajoutez l'un des types d'enregistrements DNS suivants :

- Un enregistrement A pour l'ancienne adresse du Serveur d'administration qui pointe vers la nouvelle adresse IP du Serveur d'administration.
- Un enregistrement CNAME associant l'ancien nom du Serveur d'administration au nouveau nom du Serveur d'administration.

  Pour en savoir plus sur la configuration des enregistrements requis, consultez la documentation de votre serveur DNS.

Pour préserver les connexions en ajoutant un nouvel enregistrement DNS :

1. **Modifiez le nom du serveur**.

   En raison de la configuration des modules lors de l'installation, vous ne pouvez pas modifier le nom du Serveur d'administration sans réinstaller le Serveur d'administration.

   Pour modifier le nom du serveur :

   1. Créez une nouvelle sauvegarde du Serveur d'administration à l'aide de l'utilitaire klbackup.
   2. Désinstallez Kaspersky Security Center Linux et Kaspersky Security Center Web Console sur tous les postes de travail des administrateurs.
   3. Supprimez manuellement la base de données du Serveur d'administration et la base de données IAM. Le Serveur d'administration ne la supprime pas automatiquement lors de la désinstallation.

4. Renommez l'appareil dans le système d'exploitation du Serveur d'administration conformément à la documentation de votre système d'exploitation.

5. Installez le Serveur d'administration de Kaspersky Security Center Linux en utilisant le nouveau FQDN du Serveur d'administration.

6. Restaurez la sauvegarde du Serveur d'administration préparée précédemment après l'installation.

7. Vérifiez la configuration du serveur IAM et, si nécessaire, ajoutez l'adresse du Serveur d'administration dans le fichier de configuration du serveur IAM.

8. Installez la Web Console sur tous les postes de travail des administrateurs en indiquant le nouveau FQDN du Serveur d'administration dans le fichier de réponses.

2. Ajoutez un nouvel enregistrement DNS pour l'ancienne adresse du Serveur d'administration.

3. Spécifiez la nouvelle adresse dans les paramètres du Serveur d'administration, dans Kaspersky Security Center Web Console.

4. Exécutez la tâche **Modification du Serveur d'administration** sur les appareils ayant une visibilité directe sur le Serveur d'administration. Après cela, les appareils administrés pourront se connecter au Serveur d'administration en utilisant le nouveau nom.

   N'exécutez pas la tâche sur les appareils sans visibilité directe sur le serveur ; sinon, ils perdront la connexion au Serveur d'administration et aux passerelles de connexion.

   Les appareils administrés connectés par l'intermédiaire de passerelles de connexion ne vérifient pas le nom du Serveur d'administration. Par conséquent, aucune action supplémentaire n'est requise pour eux/. Les informations relatives à l'adresse du Serveur d'administration ne seront pas mises à jour dans la sortie de la commande de diagnostic klnagchk.

La connexion au Serveur d'administration est conservée après la modification du nom du serveur.

Après la modification du nom du serveur, les informations relatives au certificat ne seront plus à jour. Étant donné que cela n'affecte pas le fonctionnement des composants, nous ne recommandons pas de remplacer les certificats autosignés en dehors du calendrier prévu. Ces certificats sont générés pendant l'installation de Kaspersky Security Center et renouvelés automatiquement par le serveur. Ils seront réémis avec le nouveau nom du Serveur d'administration lors du prochain remplacement automatique des certificats.

Lors de la réinstallation, de nouveaux certificats seront émis pour le serveur IAM/ et le Web Console Server. Si nécessaire, remplacez-les par des certificats personnalisés émis par votre autorité de certification pour le nouveau nom du Serveur d'administration. Pour en savoir plus, consultez l'article suivant : À propos des certificats de Kaspersky Security Center Linux.

Préservation des connexions par le passage à une connectivité basée sur les adresses IP

Dans ce scénario, le mode de connexion des appareils administrés au Serveur d'administration est modifié. Les appareils se connectent à l'aide de l'adresse IP du Serveur d'administration au lieu du nom du Serveur d'administration. Le basculement de tous les appareils administrés peut prendre du temps, selon le nombre d'appareils et la fréquence à laquelle ils apparaissent sur le réseau avec le Serveur d'administration.

Pour préserver les connexions en passant à une connectivité basée sur l'adresse IP :

1. **Préparez l'infrastructure de Kaspersky Security Center avant de modifier le nom du Serveur d'administration**.

   1. Connectez les appareils administrés au Serveur d'administration à l'aide d'une adresse IP. Après la modification du nom du Serveur d'administration, les appareils qui utilisent son nom pour la connexion seront déconnectés du Serveur d'administration. Pour vous connecter via une adresse IP, exécutez la tâche Modifier le Serveur d'administration sur les appareils ayant une visibilité directe sur le Serveur d'administration, y compris les appareils faisant office de passerelles de connexion.

      N'exécutez pas la tâche sur les appareils sans visibilité directe sur le serveur, sinon ils perdront la connexion au Serveur d'administration et aux passerelles de connexion.

      Les appareils administrés connectés par l'intermédiaire de passerelles de connexion ne vérifient pas le nom du Serveur d'administration. Par conséquent, aucune action supplémentaire n'est requise pour eux/. Les informations relatives à l'adresse du Serveur d'administration ne seront pas mises à jour dans le résultat de la commande de diagnostic klnagchk.

   2. Assurez-vous que tous les appareils administrés sont connectés au Serveur d'administration via l'adresse IP. Pour ce faire, vérifiez les éléments suivants :

      - Les résultats de la commande de diagnostic klnagchk dans la ligne d'adresse du Serveur d'administration sur les appareils administrés ayant un accès direct au Serveur d'administration.

      - Les informations sur les propriétés du paquet d'installation de l'Agent d'administration au moment de l'installation sur les appareils.

        L'Agent d'administration doit initialement être configuré pour se connecter au Serveur d'administration à l'aide d'une adresse IP.

        Si vous installez l'Agent d'administration par-dessus l'installation existante sans le désinstaller au préalable, l'adresse de connexion au Serveur d'administration et le certificat spécifiés dans la configuration de l'Agent d'administration ne seront pas mis à jour.

   3. Spécifiez un nouveau nom dans les profils de connexion existants du Serveur d'administration.

   4. Si vous utilisez le rôle Mobile Device Management (administration des appareils Android et iOS), suivez les instructions Comment modifier l'adresse du Serveur d'administration sur les appareils mobiles qui utilisent Kaspersky Endpoint Security for Android avec le rôle MDM ou KSMM.

2. **Modifier le nom du serveur**.

   En raison de la configuration des modules lors de l'installation, vous ne pouvez pas modifier le nom du Serveur d'administration sans réinstaller le Serveur d'administration.

   Pour modifier le nom du serveur :

   1. Créez une nouvelle sauvegarde du Serveur d'administration à l'aide de l'utilitaire klbackup.

   2. Désinstallez Kaspersky Security Center Linux et Kaspersky Security Center Web Console sur tous les postes de travail des administrateurs.

3. Supprimez manuellement la base de données du Serveur d'administration et la base de données IAM. Le Serveur d'administration ne la supprime pas automatiquement lors de la désinstallation.

4. Renommez l'appareil dans le système d'exploitation du Serveur d'administration conformément à la documentation de votre système d'exploitation.

5. Installez le Serveur d'administration de Kaspersky Security Center Linux en utilisant le nouveau FQDN du Serveur d'administration.

6. Restaurez la sauvegarde du Serveur d'administration préparée précédemment après l'installation.

7. Vérifiez la configuration du serveur IAM et, si nécessaire, ajoutez l'adresse du Serveur d'administration dans le fichier de configuration du serveur IAM.

8. Installez la Web Console sur tous les postes de travail des administrateurs en indiquant le nouveau FQDN du Serveur d'administration dans le fichier de réponses.

3. **Mettez à jour les adresses du Serveur d'administration dans les paramètres du Serveur d'administration**.

Après avoir modifié le nom du Serveur d'administration, indiquez la nouvelle adresse FQDN dans les paramètres du Serveur d'administration de Kaspersky Security Center Web Console. Pour ce faire, vérifiez et mettez à jour l'adresse FQDN dans chacun des paramètres suivants :

- Adresse du serveur proxy de Kaspersky Security Network
- Serveur Web
- Propriétés des paquets d'installation de l'Agent d'administration
- Nom de l'émetteur du code de sécurité (2FA)

En outre, procédez comme suit :

- Spécifiez le nouveau nom du serveur dans les stratégies et les paramètres des autres applications Kaspersky.
- Republiez chaque paquet autonome publié et chaque paquet pour appareils mobiles.
- Reconnectez les Serveurs d'administration secondaires si vous utilisez une hiérarchie de Serveurs d'administration et si les serveurs sont connectés par leur nom et non par leur adresse IP.

4. Exécutez la tâche **Modification du Serveur d'administration** sur les appareils qui ont une visibilité directe du Serveur d'administration afin de remplacer l'adresse de connexion des appareils administrés par le nouveau nom du Serveur d'administration.

La connexion au Serveur d'administration est conservée après la modification du nom du serveur.

Après la modification du nom du serveur, les informations relatives au certificat ne seront plus à jour. Étant donné que cela n'affecte pas le fonctionnement des composants, nous ne recommandons pas de remplacer les certificats autosignés en dehors du calendrier prévu. Ces certificats sont générés pendant l'installation de Kaspersky Security Center et renouvelés automatiquement par le serveur. Ils seront réémis avec le nouveau nom du Serveur d'administration lors du prochain remplacement automatique des certificats.

Lors de la réinstallation, de nouveaux certificats seront émis pour le serveur IAM/ et le Web Console Server. Si nécessaire, remplacez-les par des certificats personnalisés émis par votre autorité de certification pour le nouveau nom du Serveur d'administration. Pour en savoir plus, consultez l'article suivant : À propos des certificats de Kaspersky Security Center Linux.

Restauration des connexions interrompues après la modification du nom du serveur

Le scénario s'applique dans les cas suivants :

- Si vous avez perdu la propriété du nom de domaine de l'appareil du Serveur d'administration, mais que vous avez toujours accès au Serveur d'administration.
- Si le Serveur d'administration ne gère plus les appareils administrés.
- S'il n'est pas possible d'ajouter des enregistrements DNS pour l'ancienne adresse de Kaspersky Security Center Linux pour d'autres raisons.

Pour restaurer les connexions interrompues après la modification du nom du serveur :

1. **Modifiez le nom du serveur**.

   En raison de la configuration des modules lors de l'installation, vous ne pouvez pas modifier le nom du Serveur d'administration sans réinstaller le Serveur d'administration.

   Pour modifier le nom du serveur :

   1. Créez une nouvelle sauvegarde du Serveur d'administration à l'aide de l'utilitaire klbackup.
   2. Désinstallez Kaspersky Security Center Linux et Kaspersky Security Center Web Console sur tous les postes de travail des administrateurs.
   3. Supprimez manuellement la base de données du Serveur d'administration et la base de données IAM. Le Serveur d'administration ne la supprime pas automatiquement lors de la désinstallation.
   4. Renommez l'appareil dans le système d'exploitation du Serveur d'administration conformément à la documentation de votre système d'exploitation.
   5. Installez le Serveur d'administration de Kaspersky Security Center Linux en utilisant le nouveau FQDN du Serveur d'administration.
   6. Restaurez la sauvegarde du Serveur d'administration préparée précédemment après l'installation.
   7. Vérifiez la configuration du serveur IAM et, si nécessaire, ajoutez l'adresse du Serveur d'administration dans le fichier de configuration du serveur IAM.
   8. Installez la Web Console sur tous les postes de travail des administrateurs en indiquant le nouveau FQDN du Serveur d'administration dans le fichier de réponses.

2. **Mettez à jour les adresses du Serveur d'administration dans les paramètres du Serveur d'administration**.

Après avoir modifié le nom du Serveur d'administration, indiquez la nouvelle adresse FQDN dans les paramètres du Serveur d'administration de Kaspersky Security Center Web Console. Pour ce faire, vérifiez et mettez à jour l'adresse FQDN dans chacun des paramètres suivants :

- Adresse du serveur proxy de Kaspersky Security Network
- Serveur Web
- Propriétés des paquets d'installation de l'Agent d'administration
- Nom de l'émetteur du code de sécurité (2FA)

En outre, procédez comme suit :

- Spécifiez le nouveau nom du serveur dans les stratégies et les paramètres des autres applications Kaspersky.
- Republiez chaque paquet autonome publié et chaque paquet pour appareils mobiles.
- Reconnectez les Serveurs d'administration secondaires si vous utilisez une hiérarchie de Serveurs d'administration et si les serveurs sont connectés par leur nom et non par leur adresse IP.

3. Restaurez la connexion au Serveur d'administration sur les appareils précédemment administrés :

- Sur les appareils ayant une visibilité directe sur le Serveur d'administration, utilisez l'utilitaire klmover pour indiquer le nouveau nom du Serveur d'administration comme adresse de connexion. Pour plus de détails, consultez l'article suivant : Connexion des Agents d'administration au Serveur d'administration à l'aide de l'utilitaire klmover.
- Sur les appareils faisant office de passerelles de connexion, réinstallez l'Agent d'administration et reconfigurez le rôle de passerelle de connexion. Pour plus d'informations, consultez l'article suivant : Ajout d'une passerelle de connexion dans la DMZ en tant que point de distribution.
- Les appareils connectés via des passerelles de connexion se reconnecteront automatiquement une fois les passerelles de connexion restaurées. L'Agent d'administration n'utilise pas le nom du Serveur d'administration lors de la connexion aux passerelles de connexion.

  N'utilisez pas l'utilitaire klmover sur les appareils connectés via des passerelles de connexion. Pour plus de détails, consultez l'article suivant : Déplacement des appareils connectés au Serveur d'administration via des passerelles de connexion vers un autre Serveur d'administration.

La connexion au Serveur d'administration est restaurée après la modification du nom du serveur.

Après la modification du nom du serveur, les informations du certificat deviendront obsolètes. Étant donné que cela n'affecte pas le fonctionnement des composants, nous ne recommandons pas de remplacer les certificats autosignés en dehors du calendrier prévu. Ces certificats sont générés pendant l'installation de Kaspersky Security Center et renouvelés automatiquement par le serveur. Ils seront réémis avec le nouveau nom du Serveur d'administration lors du prochain remplacement automatique des certificats.

Lors de la réinstallation, de nouveaux certificats seront émis pour le serveur IAM/ et le Web Console Server. Si nécessaire, remplacez-les par des certificats personnalisés émis par votre autorité de certification pour le nouveau nom du Serveur d'administration. Pour en savoir plus, consultez l'article suivant : À propos des certificats de Kaspersky Security Center Linux.

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.

Modification des identifiants de la base de données du Serveur d'administration

Pour modifier les informations d'identification des bases de données du Serveur d'administration et d'IAM dans un environnement Linux :

1. Arrêtez le Serveur d'administration. Selon le type de déploiement de Kaspersky Security Center Linux, exécutez l'une des commandes suivantes avec le compte root :

   - Pour un cluster de basculement Kaspersky Security Center Linux :

     Sur le nœud actif, exécutez la commande suivante :

     ```
     /opt/kaspersky/ksc64/sbin/klfoc -stopcluster --stp klfoc
     ```

   - Pour un cluster de basculement Kaspersky Security Center Linux géo-distribué :

     Sur les deux nœuds, exécutez la commande suivante :

     ```
     crm node standby
     ```

   - Pour un déploiement du Serveur d'administration hors cluster :

     Exécutez les commande suivantes :

     ```
     systemctl stop kladminserver_srv.service
     systemctl stop kliam_srv.service
     ```

2. Connectez-vous à la base de données du Serveur d'administration avec les privilèges de superutilisateur du SGBD et exécutez la commande suivante :

   ```
   REASSIGN OWNED BY <old_kscdbadmin> TO <new_kscdbadmin>;
   ```

   où `<old_kscdbadmin>` est l'ancien compte utilisateur du SGBD utilisé par le Serveur d'administration pour se connecter à sa base de données, et `<new_kscdbadmin>` est le nouveau compte utilisateur du SGBD.

3. Connectez-vous à la base de données IAM avec les privilèges de superutilisateur du SGBD et exécutez la commande suivante :

   ```
   REASSIGN OWNED BY <old_iamdbadmin> TO <new_iamdbadmin>;
   ```

   où `<old_iamdbadmin>` est l'ancien compte du SGBD utilisé par le Serveur d'administration pour se connecter à sa base de données, et `<new_iamdbadmin>` désigne les nouveaux comptes du SGBD.

4. Localisez le fichier de configuration IAM : /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml

5. Dans la section `dbms_iam`, indiquez les nouveaux identifiants du compte dans les champs " Utilisateur " et " Mot de passe ". Assurez-vous que le compte existe dans le SGBD et qu'il est défini comme propriétaire de la base de données IAM.

6. Exécutez le Serveur d'administration. Selon le type de déploiement de Kaspersky Security Center Linux, exécutez l'une des commandes suivantes avec le compte root :

   - Pour un cluster de basculement Kaspersky Security Center Linux :

     Sur le nœud actif, exécutez la commande suivante :

     ```
     /opt/kaspersky/ksc64/sbin/klfoc -startcluster --stp klfoc
     ```

   - Pour un cluster de basculement Kaspersky Security Center Linux géo-distribué :

     Sur les deux nœuds, exécutez la commande suivante :

     ```
     crm node online
     ```

   - Pour un déploiement du Serveur d'administration hors cluster :

     Exécutez les commande suivantes :

     ```
     systemctl start kladminserver_srv.service
     systemctl start kliam_srv.service
     ```

7. Exécutez l'utilitaire klsrvconfig :

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

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

9. Saisissez un nouveau mot de passe.

10. Indiquez le nouveau mot de passe pour confirmation.

11. Attendez que le Serveur d'administration reprenne son fonctionnement et qu'une entrée syslog apparaisse sur le nœud actif, indiquant que le Serveur d'administration est prêt pour les opérations dans l'interface graphique.

Les identifiants de la base de données du Serveur d'administration ont été modifiés.

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. A l'aide de la copie sauvegarde, vous pouvez restaurer les données lors du déplacement de la base d'information du Serveur d'administration à un autre appareil ou lors de la permutation sur la version plus récente de Kaspersky Security Center. En outre, vous pouvez utiliser la sauvegarde des données pour déplacer les données du Serveur d'administration depuis Kaspersky Security Center Windows sous l'administration de Kaspersky Security Center Linux (le déplacement des données de Kaspersky Security Center Linux vers Kaspersky Security Center Windows n'est pas pris en charge).

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, effectuez les actions suivantes :

- **Suivez les instructions pour créer une sauvegarde sur le Serveur d'administration version 16 ou antérieure et pour restaurer celle-ci sur le Serveur d'administration version 16.1 ou ultérieure**

  - Si vous créez une sauvegarde des données sur le Serveur d'administration version 16 ou antérieure et que vous la restaurez sur le Serveur d'administration version 16.1 ou ultérieure, l'authentification à deux facteurs est activée. Pour plus d'informations, consultez la section À propos de l'authentification à deux facteurs pour un compte.

    Pour permettre aux utilisateurs de se connecter à la Web Console avec leurs comptes existants à l'aide de clés secrètes d'authentification à deux facteurs configurées, et pour que les scripts d'automatisation OpenAPI continuent de fonctionner après la restauration, vous devez suivre les étapes suivantes :

    - Activer l'authentification à deux facteurs pour tous les utilisateurs
    - Les administrateurs doivent configurer l'authentification à deux facteurs pour leurs propres comptes
    - Exclusion de comptes de l'authentification à deux facteurs

      Si nécessaire, ajoutez les comptes d'intégration utilisés pour exécuter des scripts via OpenAPI à la liste des exclusions.

    S'il n'est pas possible de configurer l'authentification à deux facteurs avant de créer la sauvegarde, les comptes utilisateur sont ajoutés à la liste d'autorisation pour l'authentification à deux facteurs et peuvent configurer l'authentification à deux facteurs lorsqu'ils se connectent à la Web Console. Pour obtenir plus de détails sur les conditions d'ajout d'un compte à la liste d'autorisation, consultez la section Autorisation des utilisateurs à configurer l'authentification à deux facteurs.

- 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.

- Si vous souhaitez sauvegarder ou restaurer un cluster de basculement de Kaspersky Security Center Linux, vous devez interrompre le cluster dans son ensemble à des fins de maintenance, puis le redémarrer une fois la sauvegarde ou la restauration terminée.

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

- 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 des groupes d'administration et des appareils clients

- Le stockage des distributifs des applications pour l'installation à distance

- Certificat du Serveur d'administration

- Les clés secrètes d'authentification à deux facteurs configurées pour les comptes utilisateurs

- Liste des comptes utilisateurs exclus de l'authentification à deux facteurs

Vous pouvez créer une copie de sauvegarde des données du Serveur d'administration en créant et en exécutant une tâche de sauvegarde des données ou en utilisant l'utilitaire klbackup. La restauration des données du Serveur d'administration est possible uniquement à l'aide de l'utilitaire klbackup. Vous devez effectuer la restauration sur une instance opérationnelle du Serveur d'administration qui vient d'être installée et dont la version est identique à la version du Serveur pour lequel la copie de sauvegarde avait été créée (ou plus récente). N'utilisez aucun outil tiers pour la sauvegarde ou la restauration et, si possible, ne supprimez pas l'installation précédente de Kaspersky Security Center Linux tant que la configuration et le transfert des données ne sont pas terminés.

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 **Gestion des ressources** → **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 16.2**, 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 vous souhaitez modifier les paramètres de la tâche par défaut, activez l'option **Fin de la création de la tâche** à l'étape **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.
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 <chemin de la sauvegarde> [-linux_path <chemin de sauvegarde du SGBD>-node_cert <chemin du certificat>] [-logfile <fichier journal> [-use_ts]|[-restore] [-password <mot de passe>] [-cert_only]
```

Si le mot de passe n'est pas saisi dans la ligne de commande de l'utilitaire klbackup, l'utilitaire demandera son entrée interactivement.

Description des paramètres :

- `-path <chemin de la sauvegarde>` : enregistre les informations dans le dossier de sauvegarde ou utilise les données du dossier de sauvegarde pour la restauration (paramètre obligatoire).
- `-linux_path <chemin de sauvegarde du SGBD>` : chemin d'accès local au dossier contenant les données de sauvegarde du SGBD.

  Le compte du serveur de base de données et l'utilitaire klbackup doivent disposer des autorisations nécessaires pour modifier les données dans le dossier de sauvegarde du SGBD.
- `-node_cert <chemin du certificat>` : fichier de certificat de serveur servant à configurer le nœud de cluster de basculement inactif après la récupération. S'il n'est pas défini, il est automatiquement récupéré sur le Serveur.
- `-logfile <fichier journal>` : enregistre un rapport sur la sauvegarde et la restauration des données du Serveur d'administration.

  Le compte du serveur de base de données et l'utilitaire klbackup doivent disposer des autorisations nécessaires pour modifier les données dans le dossier de sauvegarde.

- `-use_ts` : lors de l'enregistrement des données, copiez les informations dans le dossier de sauvegarde, dans le sous-dossier avec un nom au format `klbackup AAAA-MM-JJ # HH-MM-SS`, qui inclut la date actuelle et l'heure de l'opération en UTC. Si aucune clé n'est indiquée, les données seront enregistrées à la racine du dossier de sauvegarde.

  Si vous essayez de sauvegarder des données dans le dossier dans lequel il existe déjà une copie de sauvegarde, un message d'erreur apparaît. Aucune mise à jour des données ne se produit.

  L'utilisation de la clé `-use_ts` permet de gérer les archives de données du Serveur d'administration. Par exemple, si le dossier `/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 de sauvegarde. Si aucune clé n'est disponible, la copie de sauvegarde des données s'opère dans le dossier de sauvegarde.

- `-password <mot de passe>` : mot de passe de protection des données sensibles.

  Un mot de passe oublié ne peut pas être récupéré. Il n'existe aucune exigence de mot de passe. La longueur du mot de passe est illimitée et l'absence de mot de passe est également possible.

  Lors de la restauration des données, le même mot de passe que celui utilisé pour la sauvegarde doit être indiqué. Si le chemin d'accès au dossier partagé a changé après la sauvegarde, vous devez vérifier le fonctionnement des tâches qui utilisent les données restaurées (restauration, installation à distance) une fois que les données auront été restaurées. Le cas échéant, les paramètres de ces tâches doivent être modifiés. Lors de la restauration des données au départ du fichier de sauvegarde, personne ne peut utiliser le dossier partagé du Serveur d'administration. Le compte utilisateur sous lequel l'utilitaire klbackup est lancé doit avoir un accès complet au dossier partagé. 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.

- `-cert_only` : enregistrez ou récupérez uniquement le certificat et la clé privée du Serveur d'administration.

  Cet indicateur peut être utile dans le cadre de la migration du Serveur d'administration de Kaspersky Security Center Windows vers le Serveur d'administration de Kaspersky Security Center Linux. De plus, vous pouvez migrer des appareils gérés entre Serveurs d'administration de Kaspersky Security Center Linux et entre Serveurs d'administration de Kaspersky Security Center Windows.

Vous pouvez utiliser une sauvegarde des données pour migrer les données du Serveur d'administration de Kaspersky Security Center Windows afin qu'elles soient gérées par Kaspersky Security Center Linux.
Si vous utilisez MySQL ou MariaDB comme SGBD pour Kaspersky Security Center Windows et pour Kaspersky Security Center Linux, le paramètre `lower_case_table_names` doit correspondre pour le SGBD actuel et le nouveau.
Avant de créer une copie de sauvegarde des données, vérifiez le paramètre `lower_case_table_names`. Ainsi, lors de l'installation de MySQL ou MariaDB pour Kaspersky Security Center Linux, vous devez définir le paramètre `lower_case_table_names` sur la même valeur que celle de ce paramètre pour Windows.

Si, lors de la restauration, le certificat commun du Serveur d'administration est remplacé par un autre certificat provenant d'une sauvegarde, procédez comme suit pour garantir le bon fonctionnement du système :
1. Réinstallez Web Console pour éviter l'erreur suivante :
Le Serveur d'administration utilise un certificat non approuvé. Veuillez reconfigurer l'application en indiquant un certificat valide ou contactez l'administrateur principal.

2. Vérifiez la configuration du serveur IAM et, si nécessaire, ajoutez l'adresse du Serveur d'administration dans le fichier de configuration du serveur IAM.

Utilisation de l'utilitaire klbackup pour basculer des appareils gérés sous l'administration d'un autre Serveur d'administration

L'utilitaire klbackup permet de basculer les appareils gérés sous l'administration d'un autre Serveur d'administration. Vous pouvez modifier le Serveur d'administration de Kaspersky Security Center Windows en Serveur d'administration de Kaspersky Security Center Linux à l'aide de l'utilitaire klbackup au moment de la migration. De plus, vous pouvez migrer des appareils gérés entre Serveurs d'administration de Kaspersky Security Center Linux et entre Serveurs d'administration de Kaspersky Security Center Windows.

Avant de commencer, **vérifiez les conditions requises pour obtenir un certificat personnalisé**.

Si vous utilisez un certificat personnalisé au lieu du certificat auto-signé, avant de mettre à niveau Kaspersky Security Center Linux vers une version plus récente, vous devez vous assurer que le certificat inclut le nom alternatif du sujet (SAN). Si ce n'est pas le cas, il est important de remplacer le certificat avant de mettre à niveau Kaspersky Security Center Linux. Sinon, vous ne pourrez pas vous connecter à Web Console après la mise à niveau.

Pour vous assurer que le certificat inclut un SAN, procédez comme suit :

1. Sur l'appareil sur lequel le Serveur d'administration est installé, exécutez la commande suivante :

   - Pour un appareil fonctionnant sous Linux :

     ```
     sudo openssl x509 -in /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -
     noout -ext subjectAltName
     ```

   - Pour un appareil fonctionnant sous Windows :

     ```
     certutil -dump %ProgramData%\KasperskyLab\adminkit\1093\cert\klserver.cer
     ```

2. Assurez-vous que le nom alternatif du sujet (SAN) figure dans la sortie de la commande et qu'il contient l'adresse de l'appareil du Serveur d'administration.

3. Si le nom alternatif du sujet est absent, utilisez l'utilitaire klsetsrvcert pour remplacer votre certificat utilisateur par un certificat conforme aux exigences.

Pour faire passer les appareils gérés sous l'administration d'un autre Serveur d'administration à l'aide de l'utilitaire klbackup :

1. Sur l'ancien appareil, créez une copie de sauvegarde du certificat du Serveur d'administration et de la clé privée.

   Il est possible de créer une copie de sauvegarde de l'une des manières suivantes :

   - À l'aide de l'interface de l'utilitaire klbackup (uniquement pour le Serveur d'administration de Kaspersky Security Center Windows)

     Lancez l'utilitaire klbackup situé dans le dossier d'installation de Kaspersky Security Center, puis créez une sauvegarde à l'aide de l'option **Exécuter la sauvegarde et la restauration uniquement pour le certificat du Serveur d'administration**.

- En utilisant l'invite de commande (pour les Serveurs d'administration de Kaspersky Security Center Windows et de Kaspersky Security Center Linux à partir de la version 15.1)

  Exécutez l'utilitaire klbackup avec la clé `-cert_only` via la ligne de commande pour créer une copie de sauvegarde du certificat du Serveur d'administration et de la clé privée :

  ```
  klbackup -path <chemin vers la copie de sauvegarde du certificat du Serveur d'administration> -cert_only
  ```

2. Sur l'ancien appareil, déconnectez le Serveur d'administration du réseau.

3. Attribuez le même nom de domaine à l'appareil doté d'un autre Serveur d'administration.

   Le nouveau Serveur d'administration peut recevoir le nom NetBIOS, le FQDN et l'adresse IP statique. Cela dépend de l'adresse du Serveur d'administration qui a été définie dans le paquet d'installation de l'Agent d'administration lors du déploiement des Agents d'administration. Vous pouvez également utiliser l'adresse de connexion qui détermine le Serveur d'administration auquel l'Agent d'administration se connecte (vous pouvez obtenir cette adresse sur les appareils administrés à l'aide de l'utilitaire klnagchk).

   S'il est impossible d'attribuer la même adresse aux appareils avec un autre Serveur d'administration, vous devez générer un nouveau certificat du Serveur d'administration et indiquer ce certificat dans le fichier de configuration IAM. Après l'installation du Serveur d'administration, les Agents d'administration doivent fonctionner manuellement sur le nouveau Serveur d'administration.

4. Sur l'appareil doté d'un autre Serveur d'administration, restaurez le certificat du Serveur d'administration et la clé privée à partir de la copie de sauvegarde.

   Il est possible de restaurer une copie de sauvegarde de l'une des manières suivantes :

   - À l'aide de l'interface de l'utilitaire klbackup (uniquement pour le Serveur d'administration de Kaspersky Security Center Windows)

     Lancez l'utilitaire klbackup, puis restaurez la sauvegarde à l'aide de l'option **Exécuter la sauvegarde et la restauration uniquement pour le certificat du Serveur d'administration**.

   - En utilisant l'invite de commande (pour les Serveurs d'administration de Kaspersky Security Center Windows et de Kaspersky Security Center Linux à partir de la version 15.1)

     Exécutez l'utilitaire klbackup avec la clé `-cert_only` via la ligne de commande pour restaurer une copie de sauvegarde du certificat du Serveur d'administration et de la clé privée :

     ```
     klbackup -path <chemin vers la copie de sauvegarde du certificat du Serveur d'administration> -restore -cert_only
     ```

5. Configurez la vérification des certificats par le Serveur d'administration et le serveur IAM.

Les appareils gérés sont placés sous l'administration d'un autre Serveur d'administration. Vous pouvez accéder à ce Serveur d'administration et vous assurer que les appareils administrés sont visibles sur le réseau et que l'Agent d'administration est installé et exécuté sur eux (la valeur *Oui* dans les colonnes **Visible**, **L'Agent d'administration est installé** et **L'Agent d'administration est en cours d'exécution**).

Sauvegarde et restauration des données du Serveur d'administration avec MySQL ou MariaDB

Vous pouvez utiliser une sauvegarde des données pour migrer les données du Serveur d'administration de Kaspersky Security Center Windows sous l'administration de Kaspersky Security Center Linux. La migration à l'aide de la sauvegarde des données du Serveur d'administration est prise en charge uniquement dans le cas d'une migration vers Kaspersky Security Center Linux 15.2 ou version ultérieure à partir de toute version prise en charge de Kaspersky Security Center Windows.

> Si vous utilisez MySQL ou MariaDB comme SGBD pour Kaspersky Security Center Windows et pour Kaspersky Security Center Linux, le paramètre `lower_case_table_names` doit correspondre pour le SGBD actuel et le nouveau. Sinon, les données du Serveur d'administration ne seront pas migrées correctement.

Avant de sauvegarder les données du Serveur d'administration sur Kaspersky Security Center Windows, il faut vérifier la valeur du paramètre `lower_case_table_names`. Si vous ne définissez pas ce paramètre lors de l'installation antérieure du SGBD, la valeur par défaut du paramètre est utilisée. La valeur par défaut du paramètre `lower_case_table_names` pour Windows est `1`.

Ensuite, lors de l'installation de MySQL ou MariaDB pour Kaspersky Security Center Linux, définissez pour `lower_case_table_names` la même valeur que celle indiquée pour ce paramètre sous Windows. Pour plus de détails, consultez les instructions sur le site Internet de MySQL. Si vous ne spécifiez pas ce paramètre, la valeur par défaut du paramètre est utilisée. Pour les systèmes d'exploitation Linux, la valeur par défaut du paramètre `lower_case_table_names` est différente de la valeur par défaut pour Windows.

Si vous souhaitez installer MySQL 8.0, la définition du paramètre `lower_case_table_names` conformément à cette instruction peut ne pas fonctionner. Dans ce cas, vous devez d'abord installer MySQL 5.7, spécifier le paramètre `lower_case_table_names` à l'aide de l'instruction, puis mettre à jour MySQL 5.7 vers MySQL 8.0. Si le paramètre `lower_case_table_names` ne correspond pas pour le SGBD actuel et le nouveau, les données du Serveur d'administration ne sont pas restaurées correctement.

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 **Gestion des ressources** → **Tâches**.
2. Cliquez sur le bouton **Ajouter**.

   Ceci permet de lancer l'Assistant de création d'une tâche.
3. Dans la fenêtre de l'Assistant **Paramètres de nouvelle tâche**, sélectionnez **Maintenance du Serveur d'administration** en tant que type de tâche et cliquez sur le bouton **Suivant**.
4. Suivez les étapes ultérieures de l'assistant.

La tâche qui vient d'être créée s'affiche dans la liste des tâches. Une seule tâche Maintenance du Serveur d'administration peut être exécutée pour un même Serveur d'administration. Si une tâche Maintenance du Serveur d'administration pour un Serveur d'administration est déjà créée, aucune nouvelle tâche Maintenance du Serveur d'administration ne peut être créée.

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

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, accédez à **Configuration** → **Options d'interface**.
2. Activez ou désactivez les options requises :
   - **Afficher le chiffrement et la protection des données**
   - **Afficher les fonctionnalités MDR**
   - **Afficher les alertes EDR**
3. Cliquez sur **Enregistrer**.

Une fois que les options requises ont été activées, la console affiche les sections correspondantes dans le menu principal. Par exemple, si vous activez **Afficher les alertes EDR**, la section **Surveillance** → **Alerte** s'affiche dans le menu principal.

Connexion sécurisée au Serveur d'administration

L'échange de données entre les appareils clients et le Serveur d'administration peut s'effectuer à l'aide du protocole TLS (Transport Layer Security). Le protocole SSL permet d'identifier les parties, qui coopèrent lors de la connexion, de chiffrer les données transmises et de garantir leur intégrité tout au long de la transmission. L'authentification des parties coopérants et le chiffrement des données par clés ouvertes sont à la base du protocole SSL.

Lors de la première connexion de l'appareil client au Serveur d'administration, l'Agent d'administration sur l'appareil reçoit une copie du certificat de Serveur d'administration et le sauvegarde localement.

Lors de l'installation locale de l'Agent d'administration sur l'appareil, le certificat de Serveur d'administration peut être sélectionné à la main.

Selon la copie reçue du certificat, l'analyse des privilèges et des pouvoirs du Serveur d'administration sera réalisée au cours des connexions ultérieures.

Par la suite, lors de chaque connexion de l'appareil au Serveur d'administration, l'Agent d'administration demandera le certificat de Serveur d'administration et le comparera avec sa copie locale. S'ils ne concordent pas, l'accès du Serveur d'administration à l'appareil sera interdit.

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

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

   ```
   ./klscflag -fset -pv ".core/.independent" -s Transport -n SrvUseStrictSslSettings -v < valeur > -t d
   ```

   Spécifiez le paramètre <value> de l'indicateur SrvUseStrictSslSettings :

   - `4` : Seuls les protocoles TLS 1.2 et TLS 1.3 sont activés. Les suites de chiffrement avec LS_RSA_WITH_AES_256_GCM_SHA384 sont également activées (ces suites de chiffrement sont nécessaires pour une compatibilité descendante avec les versions précédentes de Kaspersky Security Center 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 l'invite de commande Windows en utilisant les droits d'administrateur, puis remplacez votre répertoire actuel par celui contenant l'utilitaire klscflag. L'utilitaire klsclag se trouve dans le dossier dans lequel le Serveur d'administration est installé. Chemin d'installation par défaut : <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

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
     < valeur > -t d
     ```

   - Utilisez cette commande pour activer ou désactiver la prise en charge du protocole TLS 1.3 :

     ```
     ./klscflag -fset -pv ".core/.independent" -s Transport -n KLTR_TLS13_ENABLED -v
     < valeur > -t d
     ```

Spécifiez le paramètre < `valeur` > de l'indicateur :

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

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 Protocole : HTTPS	`https://activation-v2.kaspersky.com`	Activation des applications.
Port : 443 Protocole : HTTPS	`https://products.s.kaspersky-labs.com`	Le stockage des distributifs des applications pour l'installation à distance

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.

Paramètres réseau	Adresse	Description
Port : 80 Protocole : HTTP	http://p00.upd.kaspersky.com http://p01.upd.kaspersky.com http://p02.upd.kaspersky.com http://p03.upd.kaspersky.com http://p04.upd.kaspersky.com http://p05.upd.kaspersky.com http://p06.upd.kaspersky.com http://p07.upd.kaspersky.com http://p08.upd.kaspersky.com http://p09.upd.kaspersky.com http://p10.upd.kaspersky.com http://p11.upd.kaspersky.com http://p12.upd.kaspersky.com http://p13.upd.kaspersky.com http://p14.upd.kaspersky.com http://p15.upd.kaspersky.com http://p16.upd.kaspersky.com http://p17.upd.kaspersky.com http://p18.upd.kaspersky.com http://p19.upd.kaspersky.com http://downloads0.kaspersky-labs.com http://downloads1.kaspersky-labs.com http://downloads2.kaspersky-labs.com http://downloads3.kaspersky-labs.com http://downloads4.kaspersky-labs.com http://downloads5.kaspersky-labs.com http://downloads6.kaspersky-labs.com http://downloads7.kaspersky-labs.com http://downloads8.kaspersky-labs.com http://downloads9.kaspersky-labs.com http://downloads.kaspersky-labs.com http://cm.k.kaspersky-labs.com	Mise à jour des bases de données, des modules logiciels et des applications de Kaspersky.
Port : 443 Protocole : HTTPS	https://ds.kaspersky.com https://dc1.ksn.kaspersky-labs.com https://dc1-file.ksn.kaspersky-labs.com https://dc1-pp.ksn.kaspersky-labs.com https://dc1-st.ksn.kaspersky-labs.com/ https://dc1-cert.ksn.kaspersky-labs.com https://dc1-cf.ksn.kaspersky-labs.com https://dc1-file.ksn.kaspersky-labs.com https://dc1-kas.ksn.kaspersky-labs.com https://dc1-ml.ksn.kaspersky-labs.com https://dc1-pp.ksn.kaspersky-labs.com https://dc1-st.ksn.kaspersky-labs.com https://dc1.ksn.kaspersky-labs.com	Utilisation de Kaspersky Security Network.

Paramètres réseau	Adresse	Description

Port : 443, 1443
Protocole : HTTPS
	`https://ksn-file-geo.kaspersky-labs.com`
	`https://ksn-verdict-geo.kaspersky-labs.com`
	`https://ksn-url-geo.kaspersky-labs.com`
	`https://ksn-a-p2p-geo.kaspersky-labs.com`
	`https://ksn-info-geo.kaspersky-labs.com`
	`https://ksn-cinfo-geo.kaspersky-labs.com`
		Utilisation de Kaspersky Security Network.

Port : 443, 1443
Protocole : KSN
	`ksn://ksn-a-p2p-geo.kaspersky-labs.com`
	`ksn://ksn-a-stat-geo.kaspersky-labs.com`
	`ksn://ksn-ca-geo.kaspersky-labs.com`
	`ksn://ksn-cinfo-geo.kaspersky-labs.com`
	`ksn://ksn-crypto-catm-geo.kaspersky-labs.com`
	`ksn://ksn-crypto-dnscheck-geo.kaspersky-labs.com`
	`ksn://ksn-crypto-hash-geo.kaspersky-labs.com`
	`ksn://ksn-crypto-ipm-geo.kaspersky-labs.com`
	`ksn://ksn-crypto-whocalls-geo.kaspersky-labs.com`
	`ksn://ksn-crypto-wifiplus-geo.kaspersky-labs.com`
	`ksn://ksn-eu-stat-kmp.kaspersky-labs.com`
	`ksn://ksn-file-geo.kaspersky-labs.com`
	`ksn://ksn-his-geo.kaspersky-labs.com`
	`ksn://ksn-info-geo.kaspersky-labs.com`
	`ksn://ksn-kas-geo.kaspersky-labs.com`
	`ksn://ksn-kddi.kaspersky-labs.com`
	`ksn://ksn-ml-geo.kaspersky-labs.com`
	`ksn://ksn-oui-geo.kaspersky-labs.com`
	`ksn://ksn-pp.kaspersky-labs.com`
	`ksn://ksn-src.kaspersky-labs.com`
	`ksn://ksn-stat-geo.kaspersky-labs.com`
	`ksn://ksn-tcert-geo.kaspersky-labs.com`
	`ksn://ksn-url-geo.kaspersky-labs.com`
	`ksn://ksn-verdict-geo.kaspersky-labs.com`
	`ksn://mdr.ksn.kaspersky-labs.com`
	`ksn://stat-eu.ksn.kaspersky-labs.com`
	`ksn://stat-hq.ksn.kaspersky-labs.com`
	`ksn://stat-ru.ksn.kaspersky-labs.com`
	`ksn://stat-sa.ksn.kaspersky-labs.com`
	`ksn://stat-sbr.ksn.kaspersky-labs.com`
		Utilisation de Kaspersky Security Network.

Port : 443 Protocole : HTTPS	`https://click.kaspersky.com` `https://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.

Paramètres réseau	Adresse	Description
Port : 443 Protocole : HTTPS	`https://ipm-klca.kaspersky.com`	Annonces marketing.
Port : 443 Protocole : HTTPS	`https://tip.kaspersky.com`	Réponse aux menaces via Kaspersky Threat Intelligence Portal (lors de l'utilisation de la fonctionnalité Kaspersky Next XDR Optimum).
Port : 443 Protocole : HTTPS	La liste complète des adresses est présentée dans l'article Structure des adresses et des domaines	Réaction aux menaces via Kaspersky Automated Security Awareness Platform (en cas d'utilisation de la fonctionnalité Kaspersky Next XDR Optimum).

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

2. Si vous souhaitez télécharger les mises à jour via le protocole HTTP, exécutez une des commandes suivantes 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
     ```

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 le nom du Serveur d'administration.
   La fenêtre des propriétés du Serveur d'administration s'ouvre.
2. Sous l'onglet **Général**, sélectionnez la section **Sous-réseaux globaux**.
3. Cliquez sur **Ajouter**.
   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 s'affiche 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.

Vérification de l'intégrité des modules à l'aide des utilitaires klscmodchk et integrity_checker

Kaspersky Security Center Linux contient plusieurs modules binaires qui se présentent sous la forme de bibliothèques liées dynamiquement, de fichiers exécutables, de fichiers de configuration et de fichiers d'interface. Un pirate informatique pourrait remplacer un ou plusieurs modules exécutables ou fichiers d'application par d'autres fichiers contenant du code malveillant. Pour éviter la substitution de modules et de fichiers, Kaspersky Security Center Linux effectue une vérification de l'intégrité des composants à l'aide des utilitaires klscmodchk et integrity_checker. Ces utilitaires vérifient que les modules et les fichiers n'ont pas été modifiés ni endommagés sans autorisation. Si la somme de contrôle du module ou du fichier d'application est incorrecte, celui-ci est considéré comme étant endommagé.

L'utilitaire klscmodchk effectue des contrôles d'intégrité pour les modules Kaspersky Security Center Linux suivants :

- Serveur d'administration
- Agent d'administration

L'utilitaire Integrity_checker exécute des contrôles d'intégrité pour les modules Kaspersky Security Center Linux suivants :

- Serveur d'administration
- Agent d'administration
- Kaspersky Security Center Web Console

Les deux utilitaires vérifient l'intégrité des modules sur la base du fichier manifeste kl_file_integrity_manifest.xml, qui fait partie de la version Linux de Kaspersky Security Center et se trouve dans le dossier d'installation. Le fichier manifeste du module contient des fichiers dont l'intégrité est importante pour le bon fonctionnement du module Kaspersky Security Center Linux. L'intégrité des fichiers manifestes eux-mêmes est également vérifiée.

Il est fortement déconseillé de modifier le fichier manifeste kl_file_integrity_manifest.xml, car cela invaliderait la signature numérique et ferait échouer le contrôle d'intégrité.

Pour vérifier l'intégrité du module Kaspersky Security Center Linux, exécutez une des commandes suivantes :

- `klscmodchk [ paramètres ]`

  L'utilitaire klscmodchk lance l'utilitaire integrity_checker avec le paramètre `--verbose` et vérifie l'intégrité des modules.

  Paramètres de l'utilitaire klscmodchk :

  - `-logfile < log_file_path >` : indiquez le chemin d'accès au fichier sur le disque pour la journalisation. Par défaut, les informations sont affichées dans la console.
  - `-verbose` : affiche des informations élargies pendant la vérification de l'intégrité.

- `integrity_checker [ paramètres ] < manifest_file_path >`

  Paramètres de l'utilitaire integrity_checker :

  - `--help` : affiche l'aide de l'utilitaire integrity_checker.
  - `--version` : affiche la version de l'utilitaire integrity_checker.
  - `--verbose` : affiche les informations sur le fonctionnement de l'utilitaire. Lors d'une vérification de l'intégrité, il suffit d'utiliser ce paramètre dans la commande.

Le résultat de la vérification de chaque fichier manifeste est affiché à côté du nom du fichier manifeste dans le format suivant :

- SUCCEEDED : intégrité du fichier confirmée (code retour 0).
- ÉCHEC : intégrité du fichier non confirmée (code retour différent de zéro).

Vous pouvez également programmer des vérifications de l'intégrité qui s'exécuteront automatiquement au lancement de l'application. Par défaut, la vérification automatique de l'intégrité est désactivée.

Pour activer la vérification automatique de l'intégrité, procédez comme suit :

1. Sur l'appareil où le Serveur d'administration est installé, à l'invite de commande, saisissez la commande suivante :

   ```
   ./klscflag -fset -pv klserver -n KLMODCHK_ENABLE_CHECKING -t d -v 1
   ```

2. Redémarrez l'appareil.

La vérification automatique de l'intégrité est activée.

Au prochain démarrage de Kaspersky Security Center, l'utilitaire klscmodchk s'exécutera en même temps que le Serveur d'administration et lancera la vérification de l'intégrité des modules. Le résultat des vérifications d'intégrité est écrit dans le Journal des événements Kaspersky.

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 d'Open Single Management Platform et de ses Serveurs d'administration secondaires ;
- Les appareils non définis administrés par le Serveur d'administration et ses Serveurs d'administration 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.

   Utilisez des points de distribution Windows pour sonder les réseaux Windows.

3. **Configuration de règles pour l'ajout d'appareils découverts aux groupes d'administration (facultatif)**

   De nouveaux appareils apparaissent sur le réseau à la suite de leur détection lors des sondages du réseau. Ces appareils sont automatiquement placés 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 nouvellement détectés sont répartis conformément aux règles définies. En l'absence de règles, ils restent dans le groupe **Appareils non définis**.

Sondage du réseau Windows

À propos du sondage du réseau Windows

Le Serveur d'administration de Kaspersky Security Center Linux ne prend pas en charge le sondage du réseau Windows. Utilisez des points de distribution Windows pour sonder les réseaux Windows.

Lors du sondage rapide, les points de distribution ne récupèrent que les informations de la liste des noms NetBIOS des appareils de tous les domaines et des groupes de travail du réseau. Au cours d'un sondage complet, les informations suivantes sont demandées à chaque appareil client :

- Nom du système d'exploitation
- Adresse IP
- Nom DNS
- Nom NetBIOS

Les sondages rapides et complets nécessitent les éléments suivants :

- Les ports UDP 137/138, TCP 139, UDP 445 et TCP 445 doivent être disponibles sur le réseau.
- Le protocole SMB est activé.
- Le service Microsoft Computer Browser doit être utilisé et l'ordinateur du navigateur principal doit être activé sur le Serveur d'administration.
- Le service Microsoft Computer Browser doit être utilisé et l'ordinateur du navigateur principal doit être activé sur les appareils clients :
    - Sur au moins un appareil, si le nombre d'appareils en réseau ne dépasse pas 32.
    - Sur au moins un appareil pour 32 appareils en réseau.

Le sondage complet ne peut s'exécuter que si le sondage rapide a été exécuté au moins une fois.

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 requête `ICMP ECHO REQUEST` (idem qu'une commande ping) au nom reçu. Si l'appareil répond, les informations à son sujet sont ajoutées à la base de données de Kaspersky Security Center Linux. La résolution de nom inverse est nécessaire pour exclure les appareils réseau qui peuvent avoir une adresse IP mais qui ne sont pas des ordinateurs, par exemple, les imprimantes réseau ou les routeurs.

Cette méthode de sondage repose sur un service DNS local correctement configuré. Il doit avoir une zone de recherche inversée. 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.

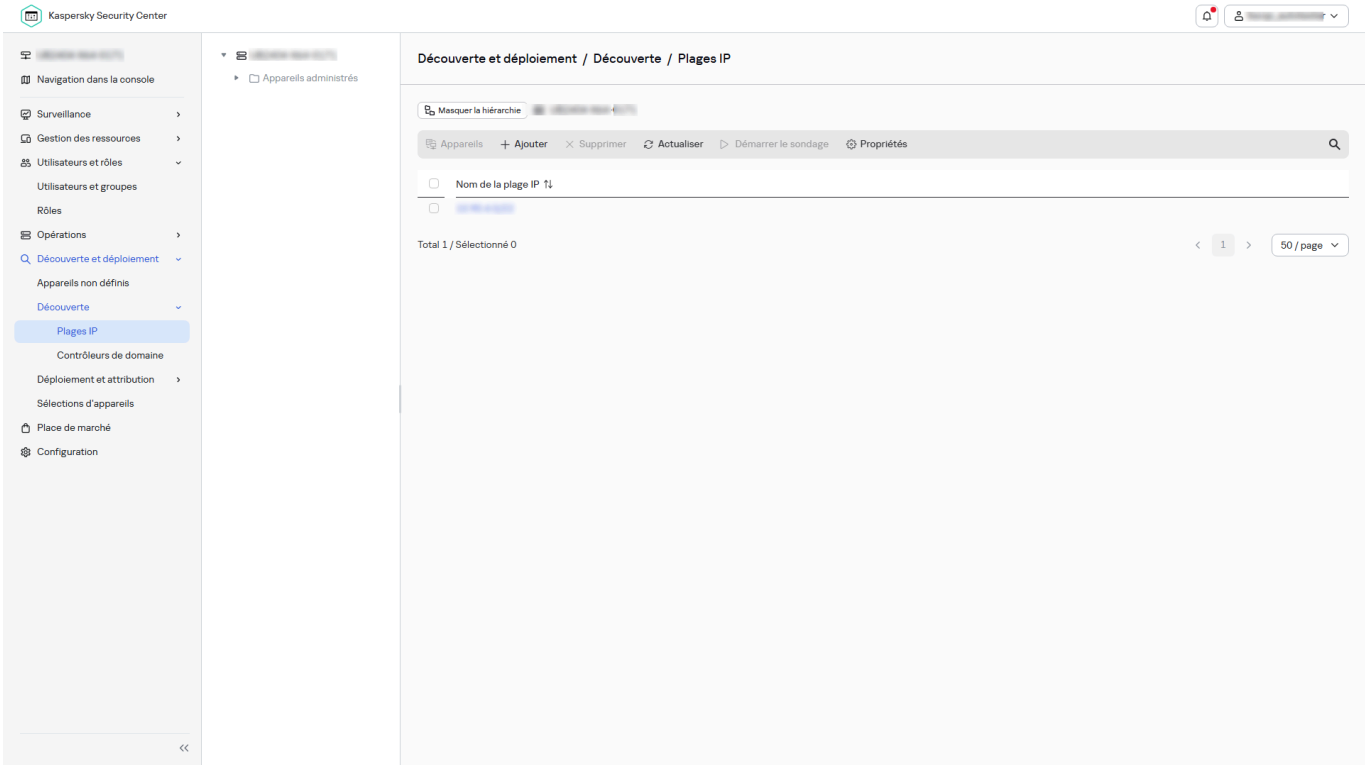
Si seul le sondage des plages IP est activé, Kaspersky Security Center Linux ne détecte que les appareils dotés d'une adresse IPv4. Si votre réseau inclut des appareils IPv6, activez le sondage Zeroconf des appareils.

Pour tous les hôtes Linux au sein d'un contrôleur de domaine Microsoft Active Directory, Samba, FreeIPA ou ALD Pro, spécifiez les paramètres `netbios name` et `workgroup` dans le fichier `/etc/samba/smb.conf`. Dans le cas contraire, les résultats du sondage peuvent contenir des hôtes en double.

Affichage et modification des paramètres de sondage des plages IP

Affichage et modification des propriétés de sondage des plages IP :

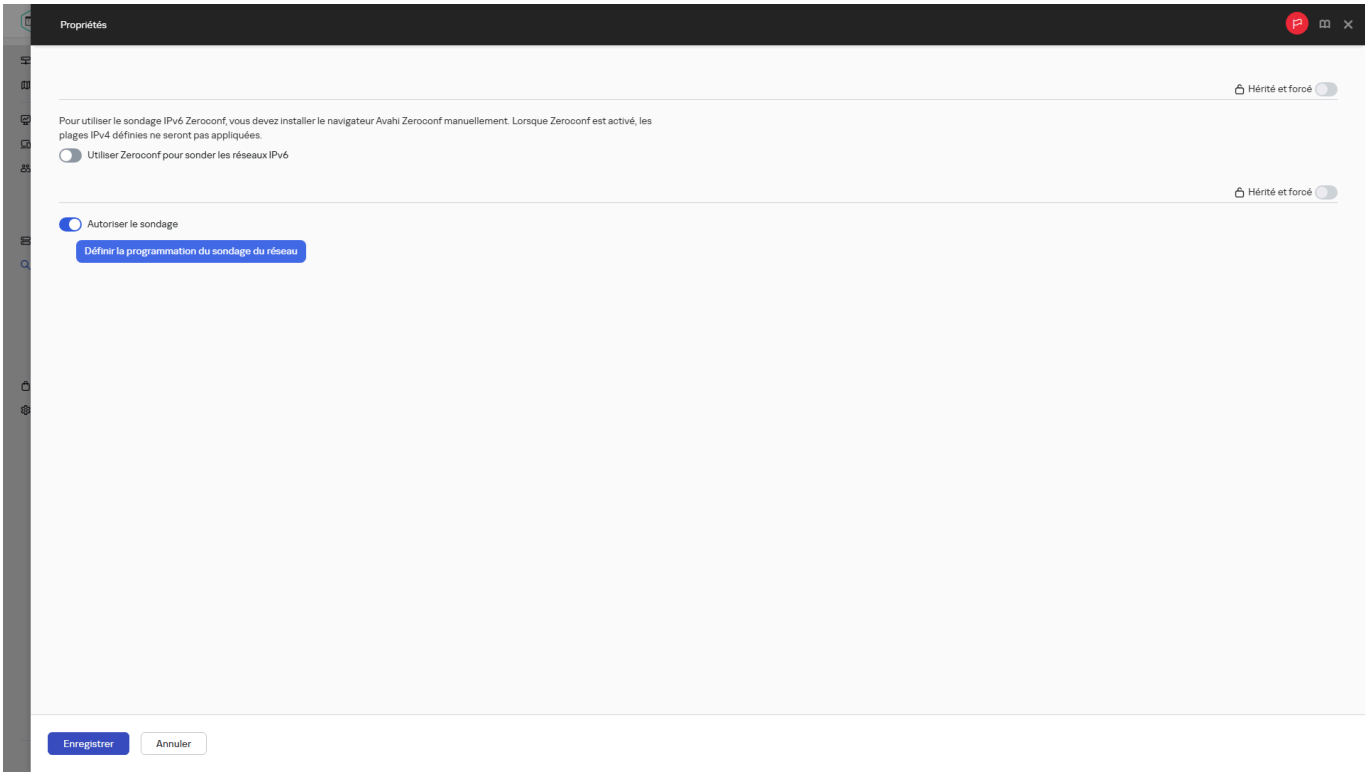
1. Dans le menu principal, accédez à **Découverte et déploiement** → **Découverte** → **Plages IP**.



Liste de la plage IP

2. Cliquez sur le bouton **Propriétés**.

   La fenêtre des propriétés de l'interrogation IP s'ouvre.



Les propriétés du sondage IP

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.

   - **Selon les jours de la semaine**

     Le sondage s'exécute régulièrement les jours définis de la semaine, à l'heure indiquée.

   - **Chaque mois, un jour de semaine donné**

     Le sondage s'exécute régulièrement les jours définis de chaque mois, à l'heure indiquée.

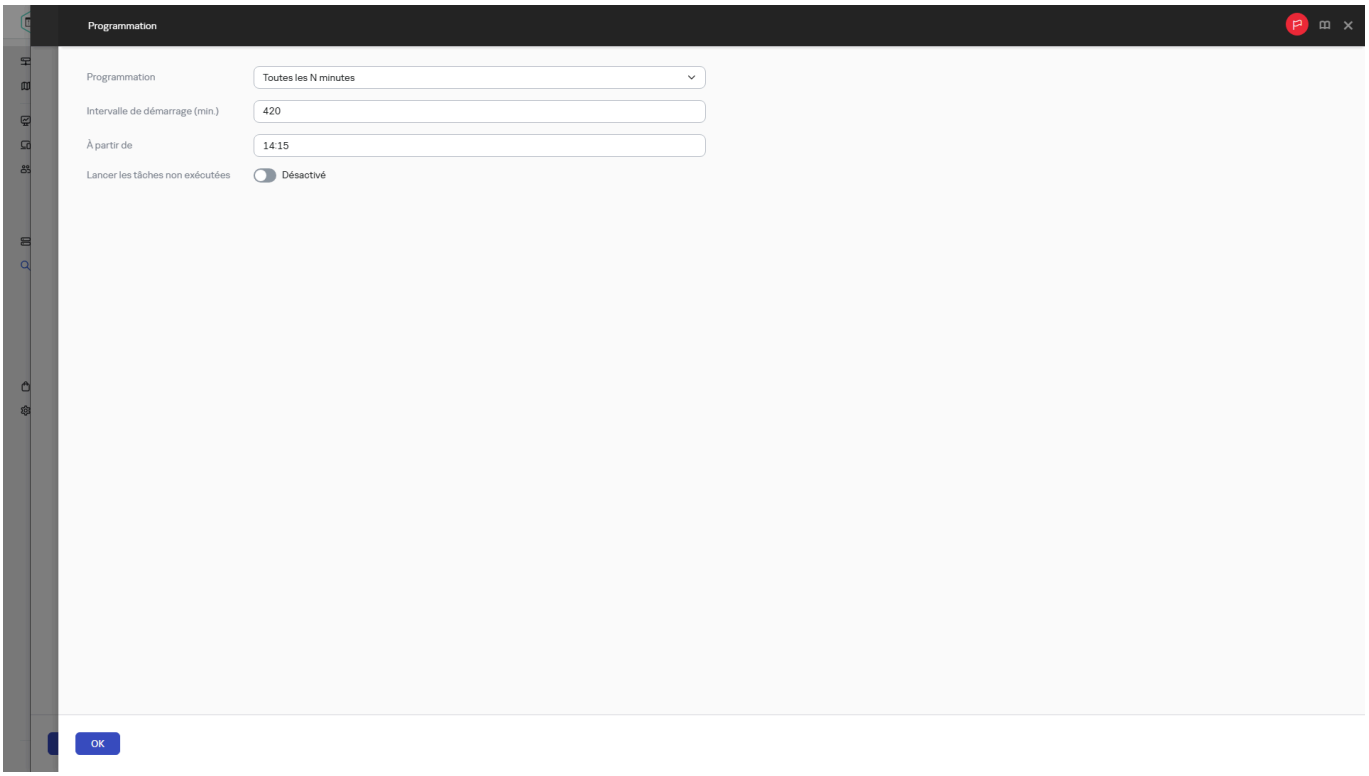
   - **Lancer les tâches non exécutées**

     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.



Configuration de la programmation du sondage

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**.

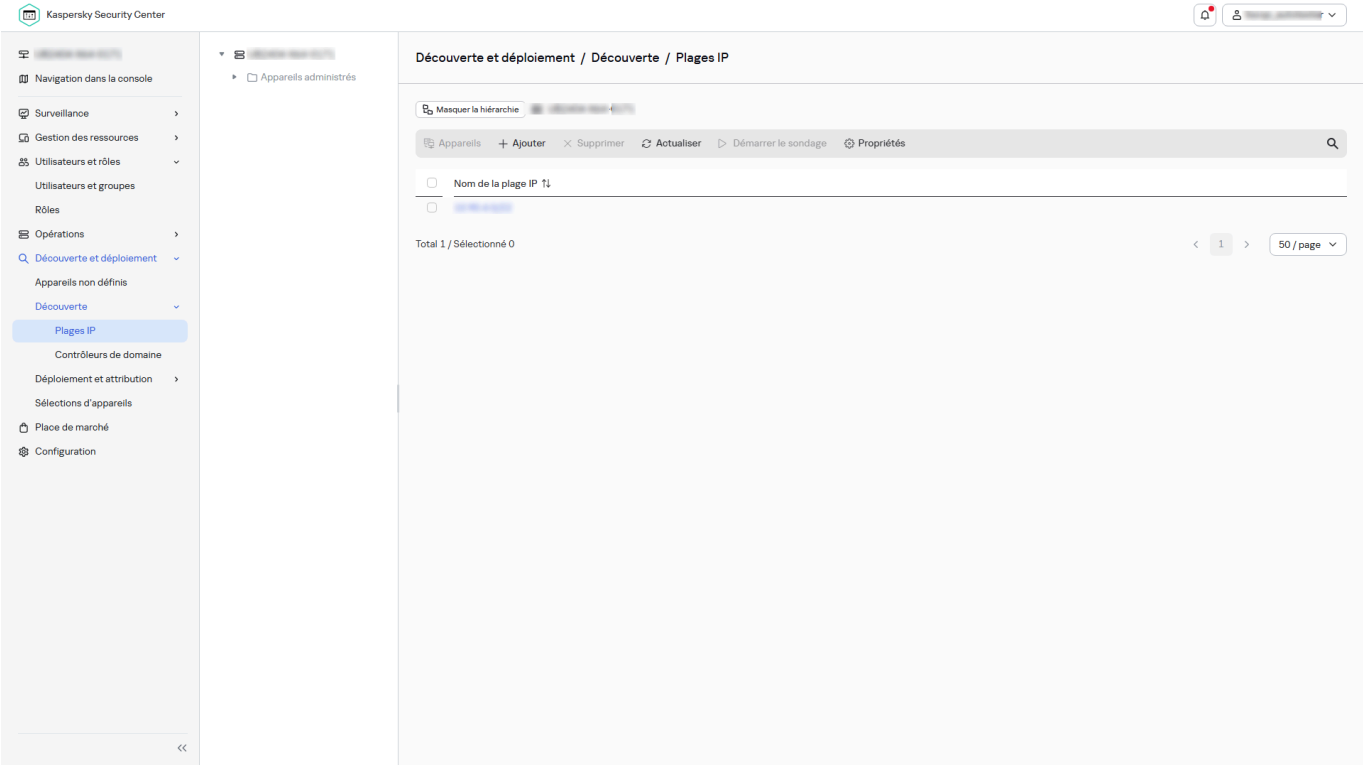
Ajout et modification d'une plage IP

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**.



Liste de la plage 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 ".

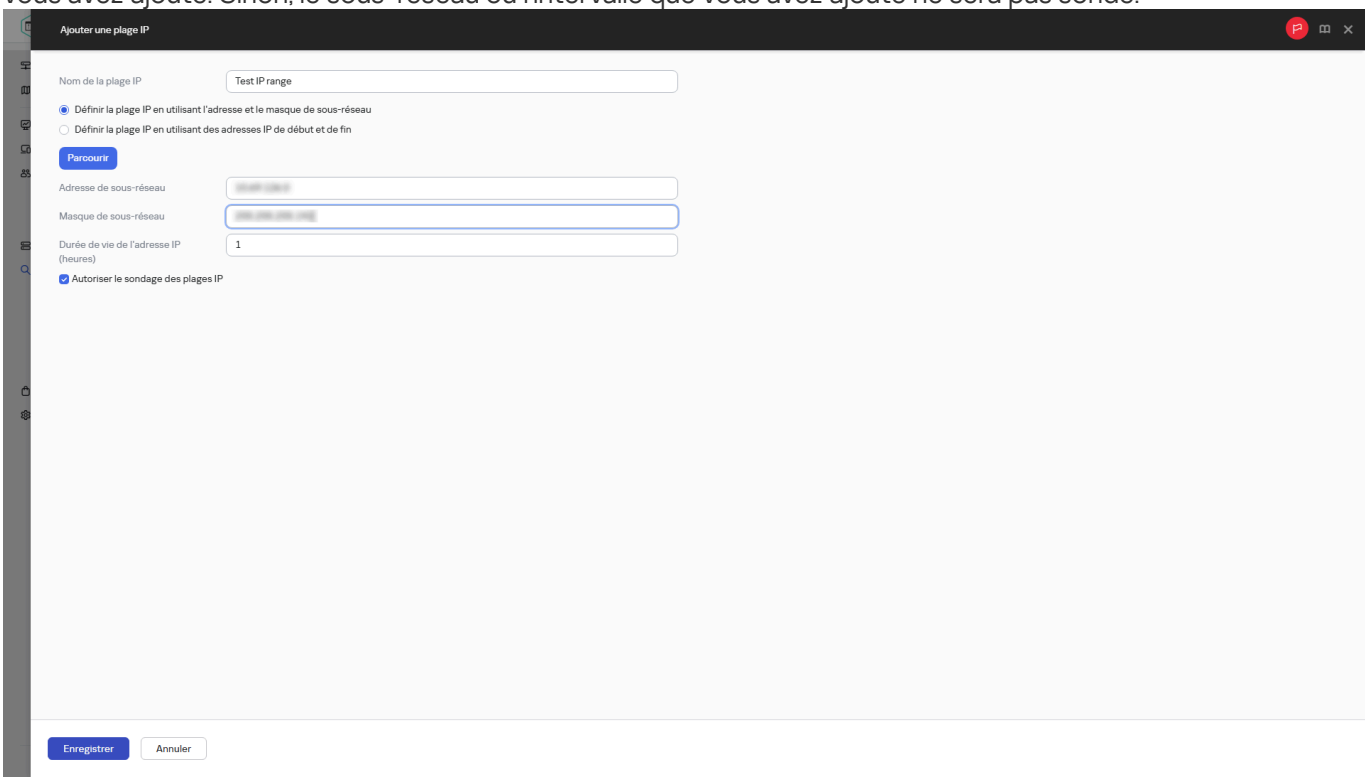
- **Masque et adresse de l'intervalle IP et du sous-réseau**

  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 des plages 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.



Indication des paramètres de la plage IP

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 les composants avahi (avahi-utils) sur l'appareil Linux qui sonde les réseaux, c'est-à-dire le Serveur d'administration ou un point de distribution.

Lors de l'utilisation de Zeroconf, le Serveur d'administration ou le point de distribution analyse le réseau pour découvrir les appareils qui prennent en charge le protocole Zeroconf et les ajoute temporairement à la liste. Un ping ICMPv6 est ensuite effectué pour chaque appareil afin de vérifier sa disponibilité, puis le service avahi effectue une recherche DNS inversée pour associer les adresses IPv6 à des noms DNS. Les informations sur le système hôte (nom DNS et type de système d'exploitation) sont enregistrées dans la base de données de Kaspersky Security Center Linux.

La portée du sondage Zeroconf est déterminée par les paramètres du service avahi. Par défaut, un sondage par diffusion est effectué au sein d'un sous-réseau. Si plusieurs interfaces réseau sont configurées sur l'appareil hébergeant le Serveur d'administration ou le point de distribution, le service avahi sonde les sous-réseaux associés à toutes les interfaces actives.

Recommandations pour réussir le sondage Zeroconf

- Assurez-vous que les paramètres suivants sont définis dans le fichier /etc/avahi/avahi-daemon.conf :
  - Sur le Serveur d'administration ou le point de distribution :
    `[server]`
    `use-ipv6=yes`
  - Sur les appareils :
    `[server]`
    `use-ipv6=yes`
    `[publish]`
    `publish-addresses=yes`
    `publish-workstation=yes`
- Assurez-vous que la ligne suivante figure dans le fichier /etc/nsswitch.conf :
  - Sur le Serveur d'administration ou le point de distribution :
    `mdns_minimal [NOTFOUND=return] dns`

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 des types de contrôleurs de domaine suivants :

- Microsoft Active Directory
- Samba
- FreeIPA
- ALD Pro

Pour un contrôleur de domaine Samba, Samba 4 est utilisé comme contrôleur de domaine Active Directory.

Lorsque vous interrogez un contrôleur de domaine, le Serveur d'administration ou un point de distribution récupère des informations sur la structure du domaine, les comptes d'utilisateurs, les groupes de sécurité et les noms DNS des appareils inclus dans le domaine.

Nous vous recommandons d'utiliser le sondage du contrôleur de domaine si tous les appareils en réseau sont membres d'un domaine. Si certains appareils en réseau ne sont pas inclus dans le domaine, ces appareils ne peuvent pas être découverts par le sondage du contrôleur de domaine.

Prérequis

Avant d'interroger un contrôleur de domaine, assurez-vous 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

> Pour FreeIPA et ALD Pro, les protocoles LDAP et LDAPS ne sont utilisés que pour le sondage du domaine. Kaspersky Security Center Linux ne prend pas en charge l'authentification des comptes FreeIPA via LDAP(S). Pour permettre aux utilisateurs de FreeIPA et d'ALD Pro de se connecter à Web Console, vous devez configurer l'authentification Kerberos via le service IAM.

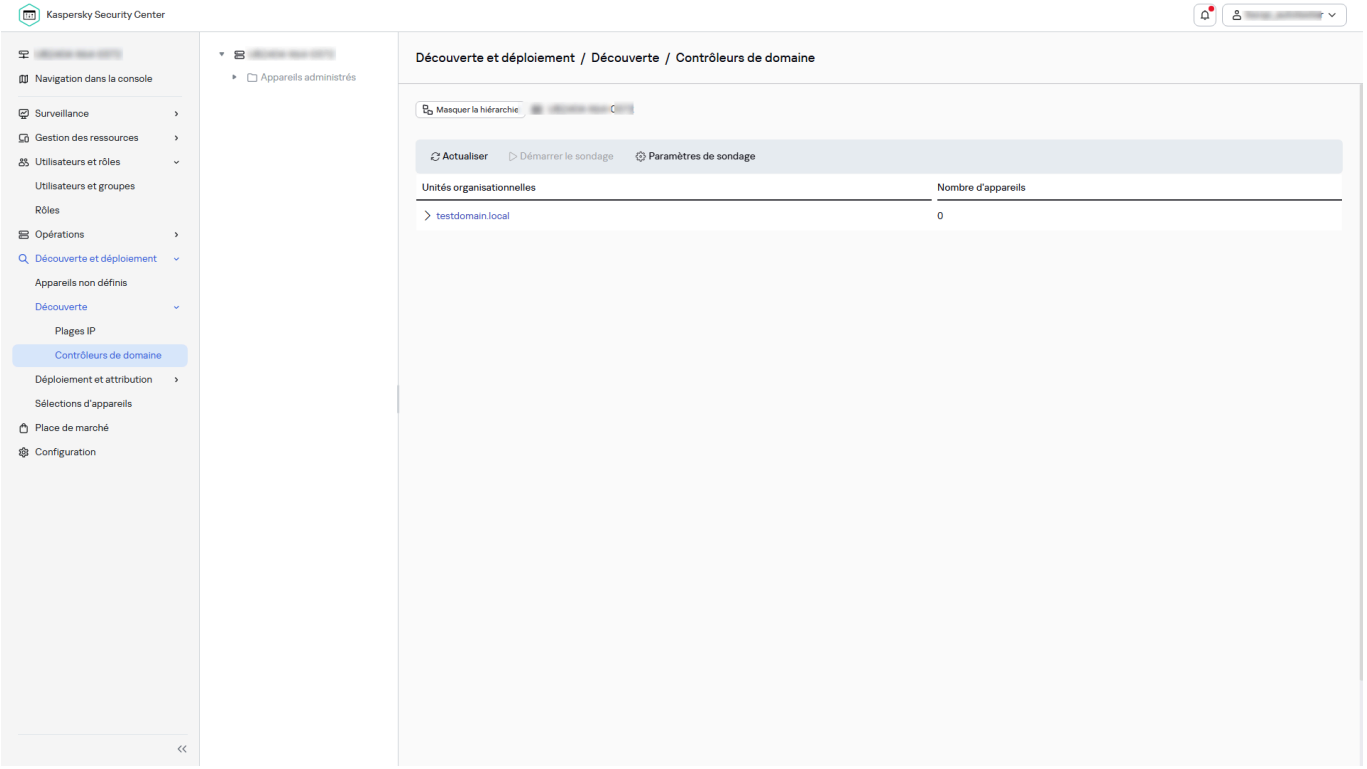
Pour tous les hôtes Linux au sein d'un contrôleur de domaine Microsoft Active Directory, Samba, FreeIPA ou ALD Pro, vous devez spécifier les paramètres `netbios name` et `workgroup` dans le fichier `/etc/samba/smb.conf`. Dans le cas contraire, les résultats du sondage peuvent contenir des hôtes en double.

> Si un domaine Microsoft Active Directory contient plusieurs contrôleurs de domaine, la sélection d'un contrôleur spécifique lors de l'interrogation du domaine n'est pas prise en charge. La connexion est établie avec le premier contrôleur de domaine détecté. Pour garantir une authentification adéquate avec le domaine Microsoft Active Directory, le champ Nom alternatif du sujet (SAN) du certificat doit inclure toutes les adresses des contrôleurs de domaine inclus dans ce domaine, ainsi que le nom NetBIOS du domaine Microsoft Active Directory.

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 :

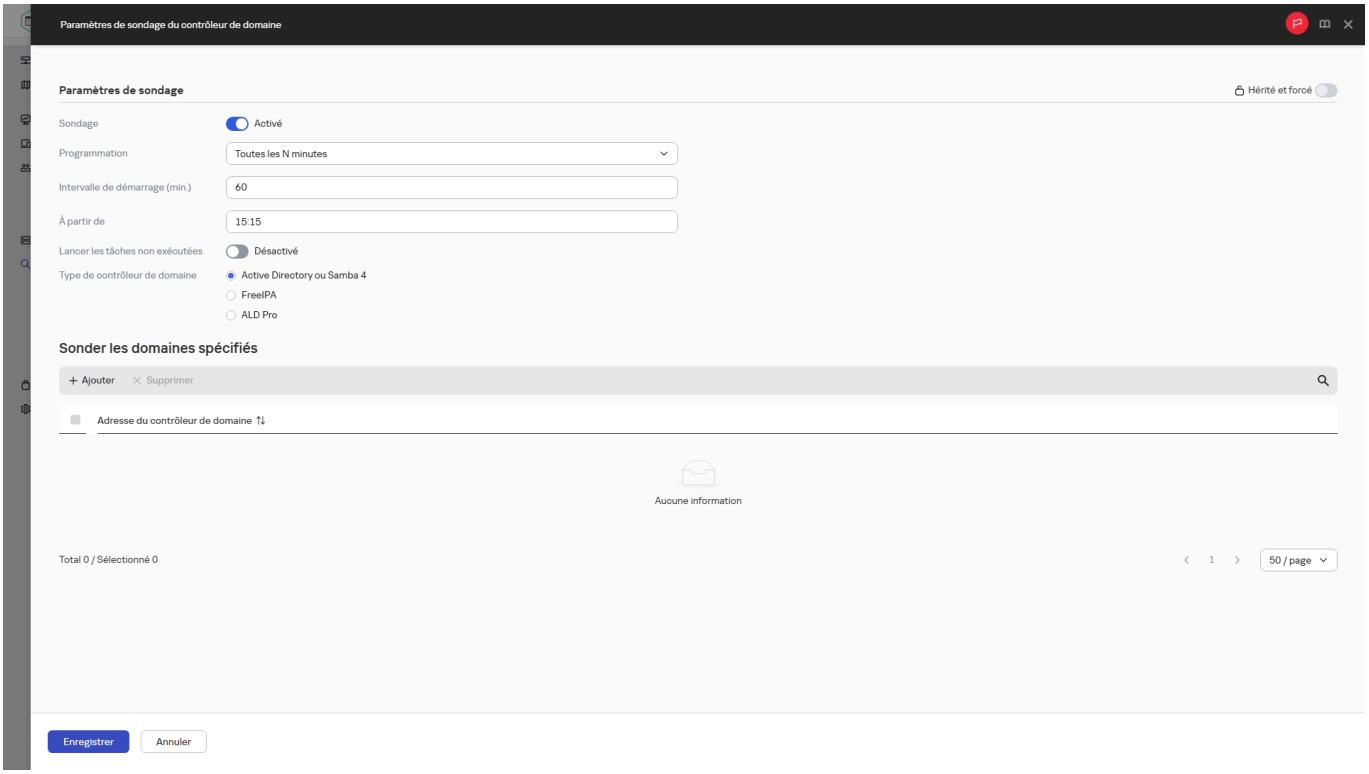
1. Dans le menu principal, accédez à **Découverte et déploiement** → **Découverte** → **Contrôleurs de domaine**.



Fenêtre de sondage du contrôleur de domaine

2. Cliquez sur **Paramètres de sondage**.

   La fenêtre **Paramètres de sondage du contrôleur de domaine** s'ouvre.



Paramètres de sondage du contrôleur de domaine

3. Dans le champ **Sondage**, placez le bouton bascule en position **Activé**.

4. Dans **Sonder les domaines spécifiés**, cliquez sur **Ajouter**, puis spécifiez l'adresse et les informations d'identification de l'utilisateur du contrôleur de domaine.

5. Dans la fenêtre **Paramètres de sondage du contrôleur de domaine**, procédez comme suit :

   - Sélectionnez le type de contrôleur de domaine à sonder : **Active Directory ou Samba 4**, **FreeIPA**, **ALD Pro**.

   - Le cas échéant, définissez la programmation de l'interrogation. 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.

     - **Selon les jours de la semaine**

       Le sondage s'exécute régulièrement les jours définis de la semaine, à l'heure indiquée.

- **Chaque mois, un jour de semaine donné**

  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 de tous les types de contrôleurs de domaine est pris en charge.
Pour un point de distribution Windows, seul 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. Dans le champ **Sondage**, placez le bouton bascule en position **Activé**.

4. Si vous utilisez un point de distribution Linux, sélectionnez le type de contrôleur de domaine à sonder : **Active Directory ou Samba 4**, **FreeIPA**, **ALD Pro**.

   Lors de la configuration du sondage à l'aide d'un point de distribution et du Serveur d'administration, il n'est pas nécessaire que vous indiquiez le même type de contrôleur de domaine.

5. Sélectionnez le contrôleur de domaine que vous souhaitez interroger.

   Si vous utilisez un point de distribution Linux, dans la section **Sonder les domaines spécifiés**, 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**

6. Cliquez sur le bouton **Planifier le sondage** pour définir les options de planification des interrogations, si nécessaire.

   Le sondage démarre uniquement selon le calendrier spécifié. Le démarrage manuel de l'interrogation 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` et `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.

> Pour FreeIPA et ALD Pro, les protocoles LDAP et LDAPS ne sont utilisés que pour le sondage du domaine. Kaspersky Security Center Linux ne prend pas en charge l'authentification des comptes FreeIPA via LDAP(S). Pour permettre aux utilisateurs de FreeIPA et d'ALD Pro de se connecter à Web Console, vous devez configurer l'authentification Kerberos via le service IAM.

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.

Pour tous les hôtes Linux au sein d'un contrôleur de domaine Samba, spécifiez le `netbios name` et les paramètres `workgroup` dans le fichier `/etc/samba/smb.conf`. Dans le cas contraire, les résultats du sondage peuvent contenir des hôtes en double.

Inventaire du matériel

La liste du matériel (**Opérations** → **Stockages** → **Matériel**) que vous utilisez pour faire l'inventaire du matériel est alimentée de deux façons : automatiquement et manuellement. Après chaque sondage du réseau, tous les appareils détectés sont automatiquement ajoutés à la liste. Cependant, vous pouvez également ajouter des appareils manuellement si vous ne souhaitez pas sonder le réseau. Vous pouvez ajouter manuellement d'autres appareils à la liste, par exemple des routeurs, des imprimantes ou du matériel informatique.

Il est possible de consulter et de modifier les informations détaillées sur les appareils dans les propriétés de l'appareil.

La liste du matériel détecté peut contenir les types suivants des appareils :

- Ordinateurs
- Appareils mobiles
- Appareils réseau
- Appareils virtuels
- Modules d'ordinateur
- Périphérie d'ordinateur
- Appareils connectés
- Téléphonie VoIP
- Stockages réseau

L'administrateur peut attribuer l'indice *Matériel corporatif* aux appareils détectés. Cet indice peut être manuellement attribué dans les propriétés de l'appareil ou définir les critères pour son attribution automatique. Dans ce cas, l'indice *Matériel corporatif* est attribué selon le type d'appareil.

Kaspersky Security Center Linux permet d'exécuter l'amortissement du matériel. Pour cela, sélectionnez l'option **Retiré du service** dans les propriétés d'un appareil. Un tel appareil ne s'affiche pas dans la liste du matériel.

L'administrateur peut manipuler la liste des contrôleurs logiques programmables (PLC) dans le dossier **Matériel**. Les informations détaillées sur la manipulation des listes de contrôleurs logiques programmables figurent dans le *Manuel de l'utilisateur de Kaspersky Industrial CyberSecurity for Nodes*.

Ajout d'informations sur les nouveaux appareils

Pour ajouter les informations sur les nouveaux appareils dans le réseau, procédez comme suit :

1. Dans le menu principal, accédez à **Opérations** → **Stockages** → **Matériel**.
2. Cliquez sur le bouton **Ajouter** pour ouvrir la fenêtre **Nouvel appareil**.
3. Dans la fenêtre **Nouvel appareil**, dans la liste déroulante **Type d'appareil**, sélectionnez le type d'appareil que vous souhaitez ajouter.
4. Cliquez sur le bouton **OK**.

   La fenêtre des propriétés de l'appareil s'ouvre sur la section **Général**.

5. Dans la section **Général**, remplissez les champs de saisie avec les données sur l'appareil. La section **Général** répertorie les paramètres suivants :

   - **&Appareil d'entreprise**. Cochez la case si vous voulez attribuer l'indice *Corporatif* à l'appareil. Avec cet attribut, il est possible de rechercher des appareils dans le dossier **Matériel**.

   - **Retiré du service**. Cochez la case si vous ne voulez pas afficher l'appareil dans la liste des appareils dans le dossier **Matériel**.

6. Cliquez sur le bouton **Appliquer**.

Le nouvel appareil s'affiche dans l'espace de travail de la page **Matériel**.

Configuration des critères de définition des appareils d'entreprise

Pour configurer les critères de définition des appareils d'entreprise, procédez comme suit :

1. Dans le menu principal, accédez à **Opérations** → **Stockages** → **Matériel**.

2. En haut de la page **Matériel**, cliquez sur le lien **Configurer la règle pour les appareils d'entreprise**.

   Un panneau **Configurer la règle pour les appareils d'entreprise** est invoqué.

3. Dans le panneau **Configurer la règle pour les appareils d'entreprise**, activez l'option **Établir &automatiquement l'Attribut Appareil d'entreprise pour l'appareil**. Spécifiez les types d'appareils auxquels l'attribut *Entreprise* est attribué automatiquement.

   Cette option affecte uniquement les appareils qui ont été ajoutés via l'interrogation du réseau. Pour les appareils ajoutés manuellement, définissez l'indice *Entreprise* manuellement.

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

Les critères de détection des appareils d'entreprise sont configurés.

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 **Gestion des ressources** → **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 **Partie de Virtual Desktop Infrastructure** sur **Oui**.
5. Cliquez sur le bouton **Enregistrer**.

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 **Gestion des ressources** → **Ressources (Appareils)**.
   La liste des appareils administrés s'affiche.
2. Cliquez sur le lien avec le nom de l'appareil requis dans la liste des appareils administrés.

La fenêtre des propriétés de l'appareil sélectionné s'affiche.

Les onglets suivants s'affichent dans la partie supérieure de la fenêtre des propriétés et représentent les principaux groupes de paramètres :

- **Général**

  Cet onglet comprend les sections suivantes :

  - La section **Général** contient les informations générales sur l'appareil client. La boîte de dialogue affiche des informations mises à jour lors de la dernière synchronisation de l'appareil client avec le Serveur d'administration :
    - **Nom**

      Champ à consulter et à modifier le nom de l'appareil client dans le groupe d'administration.

- **Description**

  Champ de saisie d'une description complémentaire de l'appareil client.

- **État de l'appareil**

  État de l'appareil client formé d'après les critères d'état de la protection antivirus et de l'activité réseau de l'appareil, tels que déterminés par l'administrateur.

- **Nom complet du groupe**

  Groupe d'administration contenant l'appareil client.

- **Dernière mise à jour des bases antivirus**

  Date de la dernière mise à jour des bases de données antivirus ou des applications sur l'appareil.

- **Connexion au Serveur d'administration**

  Date et heure de la dernière connexion de l'Agent d'administration installé sur l'appareil client au Serveur d'administration.

- **Heure de la dernière connexion**

  Date et heure où l'appareil a été visible sur le réseau pour la dernière fois.

- **Version de l'Agent d'administration**

  Version de l'Agent d'administration installé.

- **Date de création**

  Date de création de l'appareil au sein de Kaspersky Security Center Linux.

- **Propriétaire de l'appareil**

  Nom du propriétaire de l'appareil. Vous pouvez désigner ou supprimer un utilisateur en tant que propriétaire de l'appareil en cliquant sur le lien **Administrer le propriétaire de l'appareil**.

- **Maintenir la connexion au Serveur &d'administration**

  Si cette option est activée, la connectivité continue entre l'appareil administré et le Serveur d'administration est conservée. Vous pouvez utiliser cette option si vous n'utilisez pas 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 :
  - **SE**
  - **Architecture du processeur**
  - **Nom de l'appareil**
  - **Type d'une 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 affiche la liste de toutes les applications Kaspersky installées sur l'appareil client : Cet onglet contient les boutons **Démarrer** et **Arrêter**, qui permettent de démarrer 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 un serveur push ne peut pas atteindre l'appareil administré, 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.

  Vous pouvez exporter, copier et supprimer les événements de l'appareil.

- **Problèmes de sécurité**

  L'onglet **Problèmes de sécurité** permet de consulter, de modifier et de créer des problèmes de sécurité pour l'appareil client. Les problèmes de sécurité peuvent être créés automatiquement, à l'aide des applications administrées de Kaspersky installées sur l'appareil client, ou manuellement par l'administrateur. Ainsi, si un utilisateur transfère toujours des applications malveillantes de son disque amovible personnel vers d'autres appareils, l'administrateur peut créer un problème de sécurité. L'administrateur peut fournir une brève description du cas et recommandés des actions, (comme des mesures disciplinaires à adopter contre un utilisateur) dans le texte du problème de sécurité et il peut ajouter un lien vers le ou les utilisateurs.

  Un problème de sécurité pour lequel les actions nécessaires ont été exécutées est un problème *traité*. La présence de problèmes de sécurité non traités peut être sélectionnée comme condition pour faire passer l'état de l'appareil à *Critique* ou *Avertissement*.

La section contient la liste des problèmes de sécurité créés pour l'appareil. Les problèmes de sécurité sont classés par niveau de gravité et par type. C'est l'application Kaspersky qui crée le problème de sécurité qui en définit le type. Les problèmes de sécurité traités peuvent être identifiés dans la liste en cochant la case de la colonne **Traité**.

- **Tags**

  L'onglet **Tags** permet d'administrer la liste des mots-clés utilisés pour effectuer la recherche d'appareils clients : consulter la liste des tags existants, désigner les tags de la liste, configurer des règles de désignation automatique des tags, ajouter de nouveaux tags, renommer d'anciens tags et supprimer des tags.

- **Avancé**

  Cet onglet comprend les sections suivantes :

  - **Registre des applications**. Cette section permet de consulter le registre des applications installées sur l'appareil client, ainsi que leurs mises à jour, et de configurer l'affichage du registre des applications.

    Les informations relatives aux applications installées sont présentées si l'Agent d'administration installé sur l'appareil client transmet les informations nécessaires au Serveur d'administration. Les paramètres de transfert des informations sur le Serveur d'administration peuvent être configurés dans la fenêtre des propriétés de l'Agent d'administration ou de sa stratégie, dans la section **Stockages**.

    Cliquez sur le nom d'une application pour ouvrir une fenêtre contenant les détails de l'application ainsi qu'une liste des paquets de mise à jour installés pour l'application.

  - **Fichiers exécutables**. Cette section affiche les fichiers exécutables trouvés sur la machine cliente.

  - **Points de distribution**. Cette section présente la liste des points de distribution avec lesquels l'appareil interagit.

    - **Exporter dans un fichier**

      Le bouton **Exporter dans un fichier** vous permet d'enregistrer dans le fichier la liste des points de distribution avec lesquels l'appareil interagit. Par défaut, l'application exporte la liste des appareils dans un fichier au format CSV.

    - **Propriétés**

      Le bouton **Propriétés** vous permet de consulter et de configurer les paramètres du point de distribution avec lequel l'appareil interagit.

  - **Registre du matériel**. Cette section permet de consulter les informations sur le matériel installé sur l'appareil client.

    Si l'Agent d'administration est installé sur un appareil exécutant Windows, il envoie au Serveur d'administration les informations suivantes sur le matériel de l'appareil :

    - Mémoire vive

    - Appareils de stockage de masse

- Carte mère
- Processeur
- Adaptateurs réseau
- Surveillance
- Adaptateur vidéo
- Carte son

Si l'Agent d'administration est installé sur un appareil exécutant Linux ou macOS, il envoie au Serveur d'administration les informations suivantes sur le matériel de l'appareil, si ces informations sont fournies par le système d'exploitation :

- Volume total de mémoire vive
- Volume total des appareils de stockage de masse
- Carte mère
- Processeur
- Adaptateurs réseau

- **Mises à jour non installées**. Cette section permet de consulter la liste des mises à jour du logiciel, non installées détectées sur l'appareil.

- **Vulnérabilités dans les applications**. Cette section permet de consulter les informations relatives aux vulnérabilités d'applications tierces installées sur les appareils clients.

  Pour enregistrer les vulnérabilités dans un fichier, cochez les cases en regard des vulnérabilités que vous souhaitez enregistrer, puis cliquez sur le bouton **Exporter vers un fichier CSV** ou sur le bouton **Exporter vers un fichier TXT**.

  Cette section contient les paramètres suivants :

  - **Afficher uniquement les vulnérabilités qui peuvent être corrigées**

    Si l'option est activée, la section reprend les vulnérabilités qui peuvent être éliminées par un correctif.

    Si l'option est désactivée, la section reprend les vulnérabilités qui peuvent être éliminées par un correctif et celles pour lesquelles il n'existe pas de correctifs.

    Cette option est activée par défaut.

  - **Propriétés de la vulnérabilité**

    Cliquez sur une vulnérabilité logicielle dans la liste pour afficher les propriétés de la vulnérabilité logicielle sélectionnée dans une fenêtre distincte. Dans la fenêtre, vous pouvez effectuer l'une des opérations suivantes :

    - Ignorer la vulnérabilité logicielle sur cet appareil administré (dans Kaspersky Security Center Web Console).
    - Afficher la liste des correctifs recommandés pour la vulnérabilité.

- Spécifier manuellement les mises à jour logicielles permettant de corriger la vulnérabilité (dans Kaspersky Security Center Web Console).
- Afficher les instances de vulnérabilité.
- Afficher la liste des tâches existantes pour corriger la vulnérabilité et créer de nouvelles tâches pour corriger la vulnérabilité.

- **Diagnostic à distance**. Cette section permet d'effectuer un diagnostic à distance des appareils clients.

Si vous utilisez un SGBD PostgreSQL, MariaDB ou MySQL, l'onglet **Événements** peut afficher une liste incomplète des événements pour l'appareil client sélectionné. Cette situation se produit lorsque le SGBD stocke un très grand nombre d'événements. Vous pouvez augmenter le nombre d'événements affichés d'une des manières suivantes :

- Suppression des événements inutiles.
- Réduction de la durée de conservation des événements inutiles.

Pour consulter la liste complète des événements enregistrés sur le Serveur d'administration pour l'appareil, accédez à Rapports.

Vérification de la connexion de l'appareil client avec le Serveur d'administration. L'utilitaire klnagchk

Vous pouvez vérifier la connexion et recevoir les informations détaillées sur les paramètres de connexion de l'appareil client au Serveur d'administration à l'aide de l'utilitaire klnagchk. L'utilitaire klnagchk se trouve dans le dossier d'installation de l'Agent d'administration.

Lors du lancement depuis la ligne de commande, l'utilitaire klnagchk exécute les actions suivantes selon les clés utilisées :

- Renvoyer à l'écran ou enregistrer dans le fichier journal les valeurs des paramètres de connexion de l'Agent d'administration installé sur l'appareil, utilisés afin de se connecter au Serveur d'administration.
- Enregistrer dans le fichier journal les statistiques de l'Agent d'administration (à partir de son dernier démarrage) et les résultats d'exécution de l'utilitaire, ou afficher les informations sur l'écran.
- Tenter d'établir une connexion entre l'Agent d'administration et le Serveur d'administration.

  Si la connexion n'a pas pu être établie, l'utilitaire envoie un paquet ICMP au poste sur lequel est installé le Serveur d'administration afin de vérifier l'état de l'appareil.

Pour vérifier la connexion de l'appareil client au Serveur d'administration à l'aide de l'utilitaire klnagchk,

Sur l'appareil où est installé l'Agent d'administration, démarrez l'utilitaire klnagchk à partir de la ligne de commande sous un compte d'administrateur local.

Syntaxe de l'utilitaire :

```
klnagchk [-logfile <nom de fichier>] [-sp] [-savecert <chemin vers le fichier du
certificat>] [-restart][-sendhb]
```

Description des paramètres :

- `-logfile <nom du fichier>` : enregistrer les valeurs des paramètres de connexion utilisées par l'Agent d'administration pour se connecter au Serveur d'administration, ainsi que les résultats de l'exécution de l'utilitaire dans le fichier journal.

  Par défaut, les informations sont conservées dans le flux de sortie standard (stdout). Si la clé n'est pas utilisée, les paramètres, les résultats et les messages d'erreur sont affichés à l'écran.

- `-sp` : afficher le mot de passe utilisé pour authentifier l'utilisateur sur le serveur proxy.

  Cette clé est utilisée si la connexion au Serveur d'administration est effectuée via un serveur proxy.

- `-savecert <nom du fichier>` : enregistre le certificat pour l'authentification de l'accès au Serveur d'administration dans un fichier spécifié.

- `-restart` : lance l'Agent d'administration après exécution de l'utilitaire.

- `-sendhb` : lance la synchronisation de l'Agent d'administration avec le Serveur d'administration.

Après le lancement, l'utilitaire klnagchk accède aux fichiers de configuration de l'Agent d'administration et affiche les paramètres de connexion. Ces paramètres sont définis lors de l'installation de l'Agent d'administration et dans les paramètres de stratégie de l'Agent d'administration :

- `Current device` : nom de l'appareil client sur le réseau Windows.

- `Network Agent version` : numéro complet de la version d'Agent d'administration (avec correctifs) installée sur l'appareil.

- `Server address` : adresse du Serveur d'administration.

- `Use SSL` : paramètre qui indique si la connexion sécurisée au Serveur d'administration est utilisée.

  Valeurs possibles :

  - 0 : la connexion sécurisée n'est pas utilisée.

  - 1 : la connexion sécurisée est utilisée.

- `Compress traffic` : paramètre qui indique si le trafic entre l'appareil client et le Serveur d'administration est compressé.

- `Server SSL ports` : numéros des ports valides pour la communication avec le Serveur d'administration lors de l'utilisation d'une connexion sécurisée.

- `Server ports` : numéros des ports valides pour la communication avec le Serveur d'administration lors de l'utilisation d'une connexion classique.

- `Use proxy server` : paramètre qui indique si un serveur proxy est utilisé.

  Valeurs possibles :

  - 0 : le serveur proxy n'est pas utilisé.

  - 1 : le serveur proxy est utilisé.

- `Address` : adresse et port du serveur proxy, séparés par deux points. Ce paramètre s'affiche uniquement en cas d'utilisation d'un serveur proxy.

- `User name` : nom d'utilisateur permettant d'accéder au serveur proxy. Ce paramètre s'affiche uniquement en cas d'utilisation d'un serveur proxy.

- `Password` : mot de passe permettant d'accéder au serveur proxy. Ce paramètre s'affiche uniquement en cas d'utilisation d'un serveur proxy. Pour afficher le mot de passe du serveur proxy, vous devez utiliser la clé `sp` dans la commande.

- `Certificate` : paramètre qui indique si l'appareil client possède un certificat du Serveur d'administration. Par exemple, il peut ne pas exister de certificat si l'Agent d'administration ne s'est jamais correctement connecté au Serveur d'administration.

  Valeurs possibles :

  - `not installed` : l'appareil client ne possède pas de certificat de Serveur d'administration.

  - `present` : l'appareil client dispose d'un certificat du Serveur d'administration.

- `Open UDP port` : paramètre qui indique si l'Agent d'administration utilise le port UDP pour recevoir les requêtes de synchronisation du Serveur d'administration.

  Valeurs possibles :

  - 0 : le port UDP est fermé pour la réception des requêtes de synchronisation du Serveur d'administration.

  - 1 : le port UDP est ouvert pour recevoir les requêtes de synchronisation du Serveur d'administration.

- `UDP ports` : numéros des ports UDP pouvant être utilisés par l'Agent d'administration.

- `Location name` : emplacement réseau de l'appareil.

- `State of network location` : paramètre qui indique si l'appareil client peut être basculé d'un profil de connexion du Serveur d'administration à un autre.

  Valeurs possibles :

  - `Enabled` : le profil de connexion du Serveur d'administration pour l'appareil client peut être modifié.

  - `Disabled` : le profil de connexion du Serveur d'administration pour l'appareil client ne peut pas être modifié.

- `Profile to use` : profil de connexion pour le Serveur d'administration.

- `Condition` : adresse IP et masque de sous-réseau du réseau auquel l'appareil client est connecté.

- `Ping period, minutes` : intervalle standard entre les synchronisations.

- `Conn timeout, s` : délai d'expiration de la connexion.

- `RW timeout, s` : délai d'expiration de la connexion pour les opérations de lecture et d'écriture.

- `Host ID` : identifiant de l'appareil sur le réseau. L'identifiant `Device ID` est unique parmi les appareils clients administrés par le même Serveur d'administration.

- `Locations of connection gateways` : paramètres de connexion de l'appareil client au Serveur d'administration via la passerelle de connexion.

- `Location of distribution points` : paramètres de connexion de l'appareil client au Serveur d'administration via le point de distribution.

- `Connection with server` : paramètre qui indique si la passerelle de connexion dispose d'une connexion permanente au Serveur d'administration. Le paramètre s'affiche uniquement si l'appareil client agit comme une passerelle de connexion.

  Valeurs possibles :

  - `active` : la passerelle de connexion dispose d'une connexion permanente au Serveur d'administration.
  - `inactive` : la passerelle de connexion ne dispose pas de connexion permanente au Serveur d'administration.

- `Connection with server through connection gateway` : paramètre qui indique si la connexion au Serveur d'administration via une passerelle de connexion est correctement établie. Le paramètre s'affiche uniquement si l'appareil client agit comme une passerelle de connexion.

  Valeurs possibles :

  - `active` : la connexion au Serveur d'administration via une passerelle de connexion est correctement établie.
  - `inactive` : la connexion au Serveur d'administration via une passerelle de connexion n'est pas établie correctement.

De plus, le résultat de l'utilitaire klnagchk peut contenir l'une des lignes suivantes :

- `Administration Server is installed on this device` : l'utilitaire klnagchk est lancé sur l'appareil avec le Serveur d'administration.
- `This device has been assigned a connection gateway but is not yet registered on Administration Server` : l'utilitaire klnagchk est lancé sur l'appareil sur lequel l'Agent d'administration est installé, en mode passerelle de connexion. La passerelle de connexion configurée attend une connexion du Serveur d'administration, mais le Serveur d'administration ne répertorie pas l'appareil parmi les appareils administrés. Vous devez vous assurer que le Serveur d'administration amorce une connexion avec la passerelle de connexion.
- `This device is a connection gateway` : l'utilitaire klnagchk est exécuté sur l'appareil qui agit comme une passerelle de connexion.
- `Acts as a distribution point` : l'utilitaire klnagchk est exécuté sur l'appareil qui agit comme un point de distribution.

L'utilitaire klnagchk vérifie l'état du service de l'Agent d'administration. Si le service est désactivé, l'utilitaire s'arrête. Si le service est en cours d'exécution, l'utilitaire affiche les statistiques de connexion suivantes :

- `Ping count` : nombre de tentatives de connexion de l'appareil client au Serveur d'administration.
- `Succ. pings` : nombre de tentatives réussies de connexion de l'appareil client au Serveur d'administration.
- `Sync count` : nombre de tentatives de synchronisation des paramètres de l'appareil client avec ceux du Serveur d'administration.
- `Succ. syncs` : nombre de tentatives réussies de synchronisation des paramètres de l'appareil client avec le Serveur d'administration.
- `Last ping` : date et heure de la dernière connexion.

Vous devez utiliser les paramètres `Ping count` et `Succ. pings` pour analyser la connexion entre le Serveur d'administration et l'Agent d'administration. Les paramètres de l'appareil client ne se synchronisent avec les paramètres du Serveur d'administration que si les paramètres du Serveur d'administration ont été modifiés (par exemple, si de nouvelles tâches ont été ajoutées ou des paramètres d'une stratégie ont été modifiés). Dans le cas contraire, les valeurs des paramètres `Ping count` et `Succ. pings` restent inchangées.

Pour apprendre à résoudre les problèmes de connexion de l'Agent d'administration au Serveur d'administration, consultez la FAQ de Kaspersky Security Center Linux.

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 **Gestion des ressources** → **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.

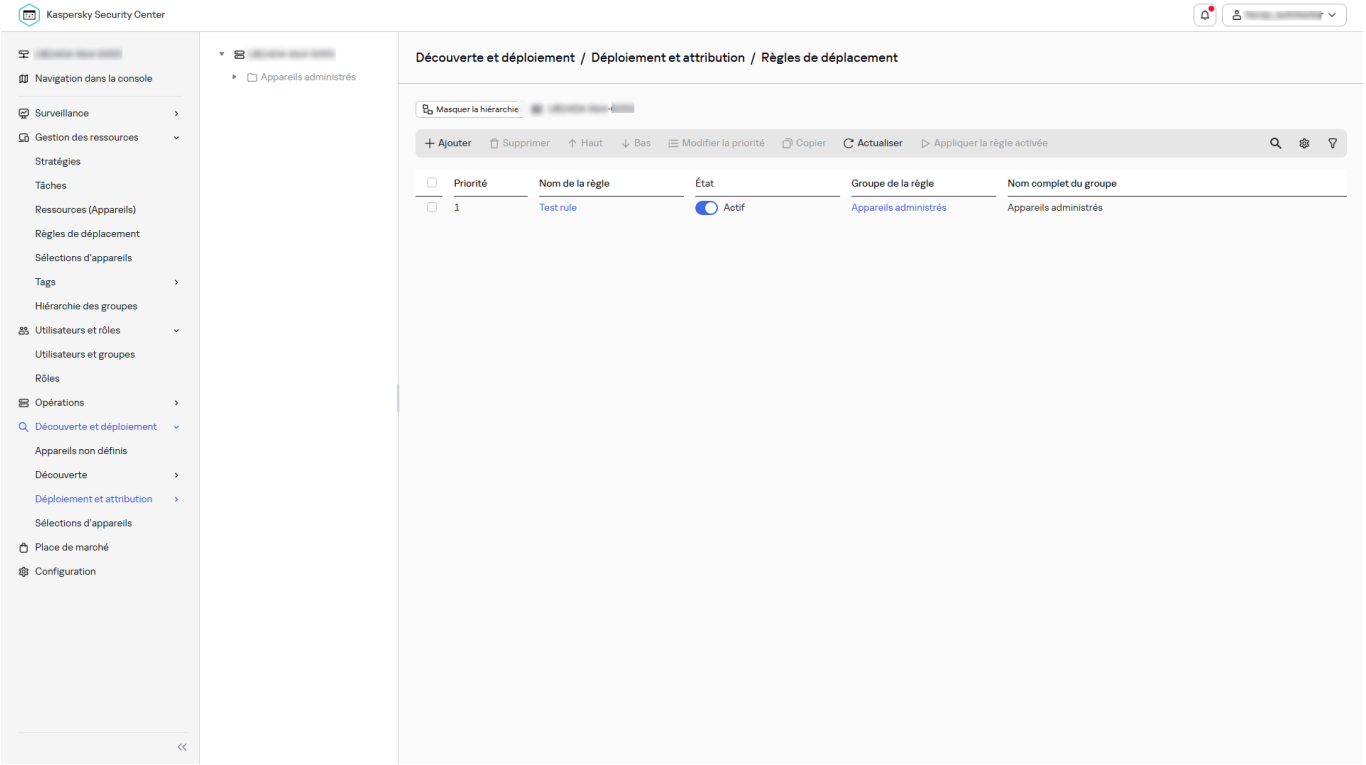
Ces scénarios ne sont pas pris en charge car ils ne sont pas efficaces en termes de charge sur le Serveur d'administration et de trafic réseau. De plus, ils sont en contradiction avec les modèles de fonctionnement de Kaspersky Security Center Linux (surtout au niveau des privilèges d'accès, des événements 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

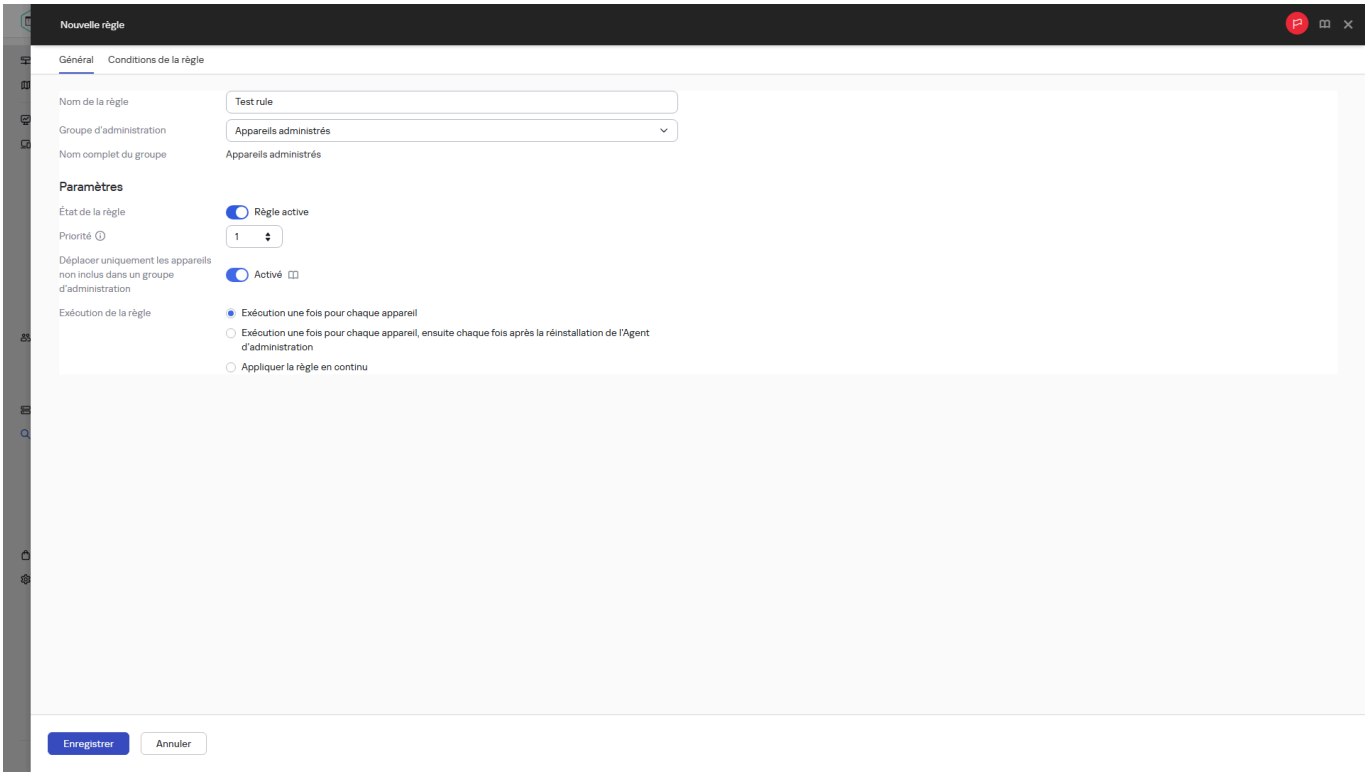
Vous pouvez configurer les règles de déplacement des appareils qui attribuent automatiquement des appareils à des groupes d'administration.

Pour créer une règle de déplacement, procédez comme suit :

1. Dans le menu principal, accédez à **Gestion des ressources** → **Règles de déplacement**.



2. Cliquez sur **Ajouter**. La fenêtre **Nouvelle règle** s'ouvre.



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.

- **État de la règle**

  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.

- **Priorité**

  Vous pouvez définir la priorité de la règle de déplacement. La priorité la plus élevée est 1. Plus la valeur **Priorité** est élevée, plus la priorité de la règle est faible et plus elle se trouve en bas de la liste.

  Si aucune priorité n'est attribuée, la règle se voit attribuer la priorité la plus basse.

  Lorsque vous copiez une règle, la copie de cette règle hérite de la priorité de la règle d'origine. La priorité de la règle d'origine est alors augmentée de 1.

- **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 :

  - **Exécution une fois pour chaque appareil**

    La règle est appliquée une fois pour chaque appareil qui correspond à vos critères.

  - **Exécution 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 modifier la priorité :

1. Cochez la case d'une règle de déplacement.

2. Exécutez une des actions suivantes :

   - Cliquez sur le bouton **Modifier la priorité** et indiquez la nouvelle priorité.

   - Déplacez la règle vers le haut ou vers le bas dans la liste en cliquant sur les boutons **Haut** ou **Bas**.

3. Cliquez sur **Enregistrer**.

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.

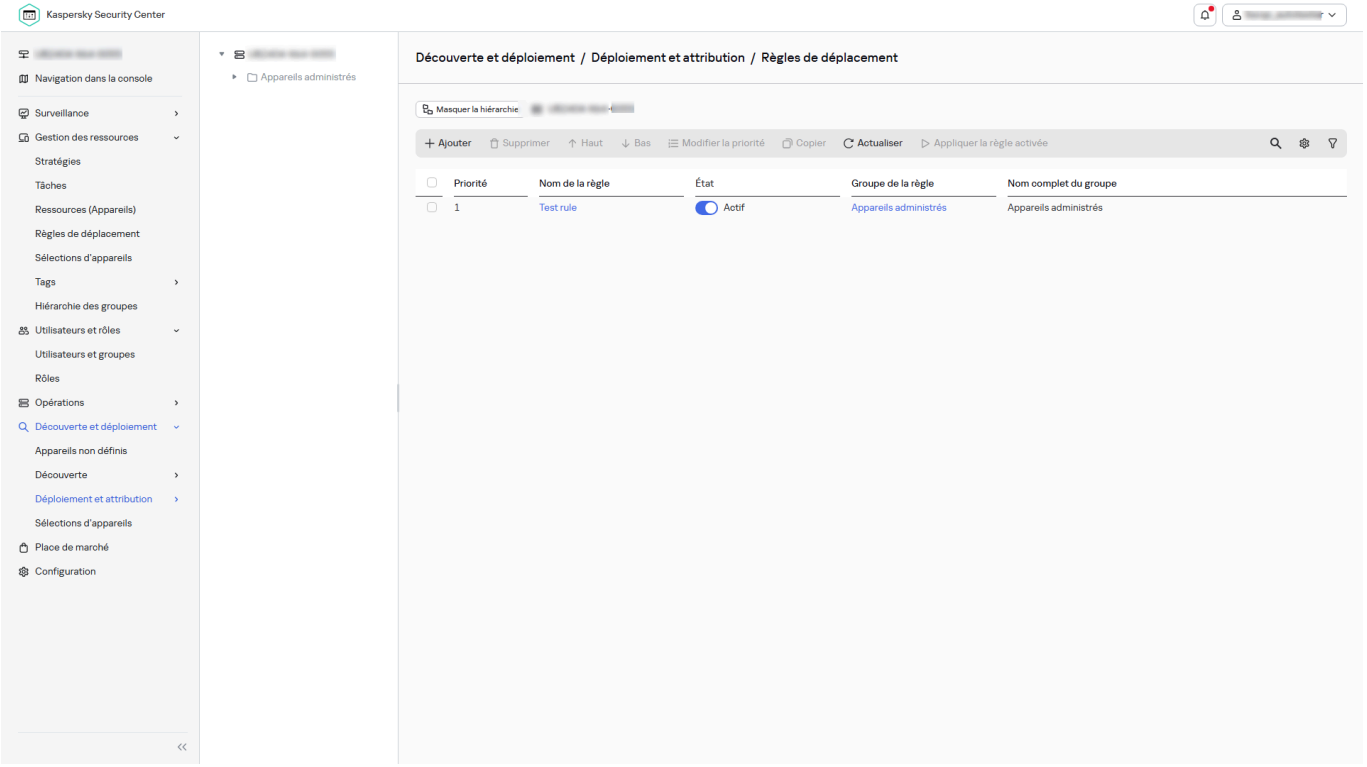
Pour copier une règle de déplacement existante, procédez comme suit :

1. Exécutez une des actions suivantes :

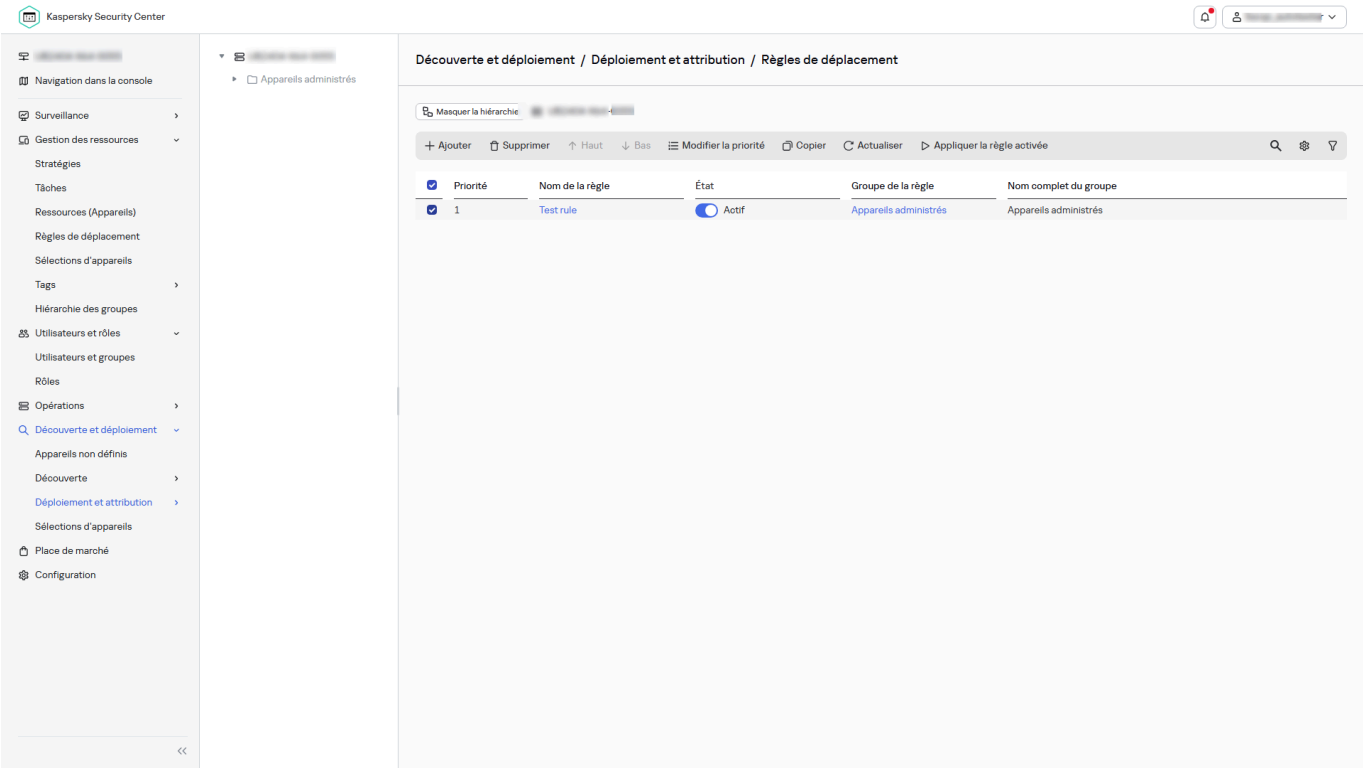
   - Dans le menu principal, accédez à **Gestion des ressources** → **Règles de déplacement**.

   - 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.

- **État de la règle**

  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.

- **Priorité**

  Vous pouvez définir la priorité de la règle de déplacement. La priorité la plus élevée est 1. Plus la valeur **Priorité** est élevée, plus la priorité de la règle est faible et plus elle se trouve en bas de la liste.

  Si aucune priorité n'est attribuée, la règle se voit attribuer la priorité la plus basse.

Lorsque vous copiez une règle, la copie de cette règle hérite de la priorité de la règle d'origine. La priorité de la règle d'origine est alors augmentée de 1.

- **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 :

  - **Exécution une fois pour chaque appareil**

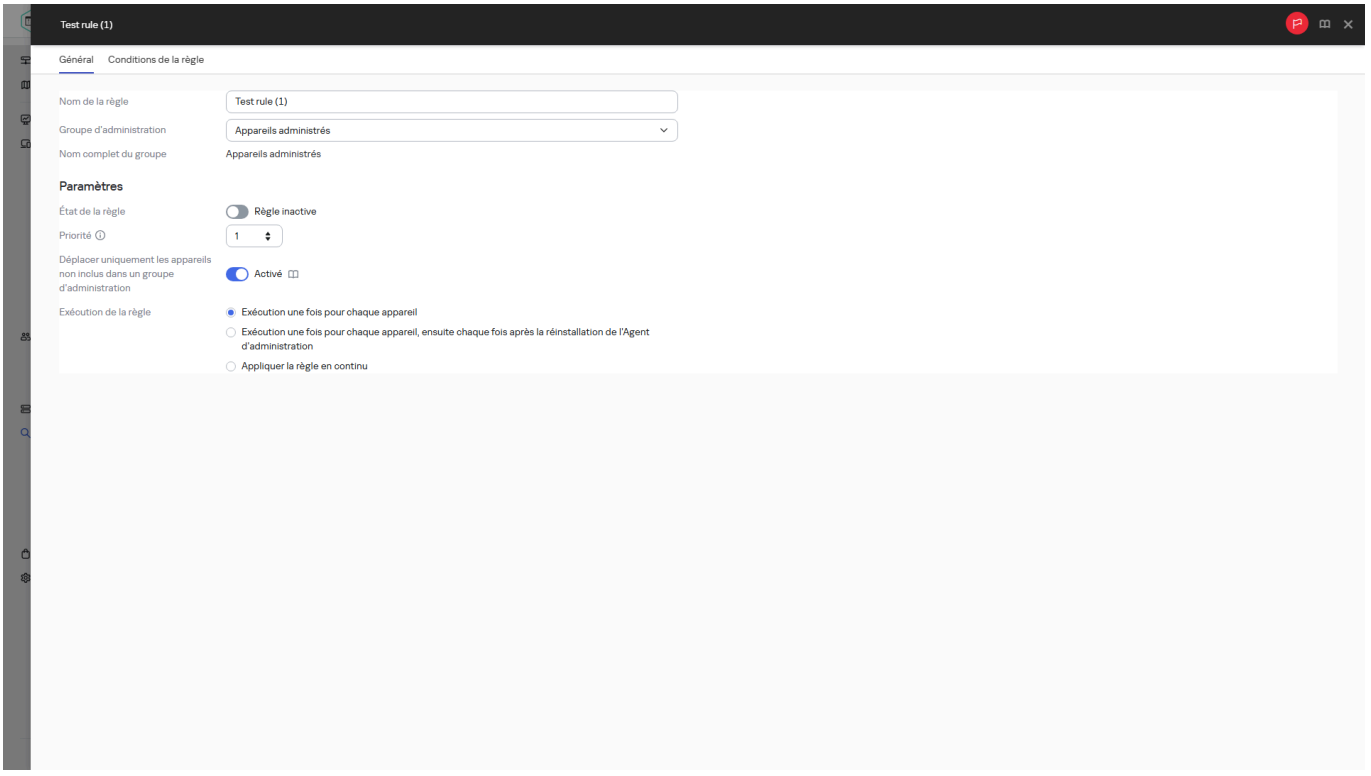
    La règle est appliquée une fois pour chaque appareil qui correspond à vos critères.

  - **Exécution 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.
- Propriétaire de l'appareil, son rôle et son appartenance à un groupe de sécurité.
- 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.
- Unités d'organisation du contrôleur de domaine.
- Segments dans le Cloud.

Vous trouverez ci-dessous la description de la manière de spécifier ces informations dans une règle de déplacement des appareils.

Si vous spécifiez plusieurs conditions dans la règle, l'opérateur logique ET fonctionne et toutes les conditions s'appliquent en même temps. Si vous ne sélectionnez aucune option ou si vous laissez certains champs vides, ces conditions ne s'appliquent pas.

Onglet Tags

Sur cet onglet, vous pouvez configurer une règle de déplacement de l'appareil basée sur les tags de l'appareil qui ont été précédemment ajoutés aux descriptions des appareils clients. Pour ce faire, sélectionnez les balises requises. Vous pouvez également activer les options suivantes :

- **Appliquer aux appareils sans les tags sélectionnés**

  Si cette option est activée, tous les appareils avec les tags indiqués sont exclus de la règle de déplacement des appareils. Si cette option est désactivée, la règle de déplacement des appareils s'applique aux appareils avec tous les tags sélectionnés.

  Cette option est Inactif par défaut.

- **Appliquer si au moins un tag sélectionné coïncide**

  Si cette option est activée, une règle de déplacement des appareils s'applique aux appareils clients avec au moins une des balises sélectionnées. Si cette option est désactivée, la règle de déplacement des appareils s'applique aux appareils avec tous les tags sélectionnés.

Cette option est Inactif par défaut.

Onglet Réseau

Sous cet onglet, vous pouvez spécifier les données réseau des appareils pris en compte par une règle de déplacement des appareils :

- **Nom de l'appareil sur le réseau Windows**

  Nom de réseau Windows (nom NetBIOS) de l'appareil ou adresse IPv4 ou IPv6.

- **Domaine Windows**

  Une règle de déplacement des appareils s'applique à tous les appareils inclus dans le domaine Windows indiqué.

- **Nom 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 pour la connexion au Serveur d'administration**

  Si cette option est activée, vous pouvez définir les adresses IP par lesquelles les appareils clients sont connectés au Serveur d'administration. Pour ce faire, spécifiez la plage IP qui comprend toutes les adresses IP nécessaires.

  Cette option est Inactif par défaut.

- **L'appareil se trouve dans un sous-groupe du groupe Domaines**

  Si cette option est activée, vous pouvez sélectionner un sous-groupe du groupe Domaines. Les appareils concernés doivent se trouver dans le sous-groupe sélectionné.

  Cette option est Inactif par défaut.

- **L'appareil appartient à la plage IP**

  Si cette option est activée, vous pouvez sélectionner une plage IP que vous avez précédemment ajoutée dans la section **Plages IP**. Les appareils concernés doivent être inclus dans la plage IP sélectionnée.

  Cette option est Inactif par défaut.

- **Profil de connexion modifié**

  Sélectionnez l'une des valeurs ci-dessous :

  - **Oui**. Une règle de déplacement des appareils s'applique uniquement aux appareils clients dont le profil de connexion a été modifié.
  - **Non**. La règle de déplacement des appareils s'applique uniquement aux appareils clients dont le profil de connexion n'a pas changé.
  - **La valeur n'est pas sélectionnée**. La condition ne s'applique pas.

- **Administrés par un autre Serveur d'administration**

  Sélectionnez l'une des valeurs ci-dessous :

  - **Oui**. Une règle de déplacement des appareils s'applique uniquement aux appareils clients administrés par d'autres Serveurs d'administration. Ces Serveurs sont différents du Serveur sur lequel vous configurez la règle de déplacement des appareils.
  - **Non**. La règle de déplacement des appareils s'applique uniquement aux appareils clients administrés par le Serveur d'administration actuel.
  - **La valeur n'est pas sélectionnée**. La condition ne s'applique pas.

Onglet Propriétaire de l'appareil

Dans cet onglet, vous pouvez configurer une règle de déplacement d'appareils en fonction du propriétaire de l'appareil, de son appartenance à un groupe de sécurité et de son rôle :

- **Propriétaire de l'appareil**

  Sélectionnez le nom d'utilisateur du propriétaire de l'appareil dans le groupe de sécurité interne. Apprenez-en plus à propos des utilisateurs et des rôles des utilisateurs dans cette section.

Un seul utilisateur peut être enregistré en tant que propriétaire de l'appareil.

- **Appartenance du propriétaire de l'appareil au groupe de sécurité Active Directory**

  Sélectionnez un groupe de sécurité externe Active Directory auquel appartient le propriétaire de l'appareil.

  L'utilisateur peut appartenir à un groupe de sécurité Active Directory ou faire partie d'un groupe inclus dans ce groupe de sécurité Active Directory.

- **Rôle du propriétaire de l'appareil**

  Sélectionnez le rôle attribué au propriétaire de l'appareil. Apprenez-en plus à propos des rôles des utilisateurs dans cet article.

- **Appartenance du propriétaire de l'appareil au groupe de sécurité interne**

  Sélectionnez un groupe de sécurité interne auquel appartient le propriétaire de l'appareil.

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 16.2** ou **Serveur d'administration de Kaspersky Security Center 16.2**.

  Si vous ne sélectionnez aucune application administrée, la condition ne s'applique pas.

- **Version du système**

  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. Cette option est Inactif par défaut.

- **Architecture du système d'exploitation**

  Vous pouvez sélectionner les appareils clients en fonction de la taille des bits du système d'exploitation. Dans le champ **Architecture du système d'exploitation**, vous pouvez sélectionner une des valeurs suivantes :

  - **Inconnu**
  - **x86**
  - **AMD64**
  - **IA64**

  Pour vérifier l'architecture du système d'exploitation des appareils clients, procédez comme suit :

  1. Dans le menu principal, accédez à la section **Gestion des ressources** → **Ressources (Appareils)**.
  2. Cliquez sur le bouton **Paramètres des colonnes** (⚙) à droite.
  3. Sélectionnez l'option **Architecture du système d'exploitation**, puis cliquez sur le bouton **Enregistrer**.

     Ensuite, l'architecture du système d'exploitation s'affiche pour chaque appareil administré.

- **Gestionnaire de paquets du système d'exploitation**

  Vous pouvez sélectionner les appareils clients en fonction du gestionnaire des paquets du système d'exploitation. Dans le champ **Gestionnaire de paquets du système d'exploitation**, vous pouvez sélectionner une des valeurs :

  - rpm : pour les appareils exécutant les systèmes d'exploitation Red Hat Enterprise Linux, CentOS, Fedora, SUSE, Oracle Linux
  - apt (dpkg) : pour les appareils exécutant les systèmes d'exploitation Debian, Ubuntu, Kali
  - pkg : pour les appareils exécutant les systèmes d'exploitation FreeBSD et OpenBSD

Pour vérifier le gestionnaire des paquets du système d'exploitation des appareils clients, procédez comme suit :

1. Dans le menu principal, accédez à la section **Gestion des ressources** → **Ressources (Appareils)**.
2. Cliquez sur le bouton **Paramètres des colonnes** (⚙) à droite.
3. Sélectionnez l'option **Gestionnaire de paquets du système d'exploitation**, puis cliquez sur le bouton **Enregistrer**.

Le gestionnaire des paquets 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 :

  - **Installée**. Une règle de déplacement des appareils s'applique uniquement aux appareils mobiles dotés d'un certificat mobile.
  - **Non installée**. 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.

- **Compilation 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 aussi configurer une règle de déplacement de l'appareil pour tous les numéros de version, à l'exception du numéro 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 d'une machine virtuelle**
- **Partie de 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 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 unités enfants vers les sous-groupes correspondants**

- **Créer des sous-groupes qui correspondent aux conteneurs des appareils détectés pour la première fois**
- **Supprimer les sous-groupes qui ne sont pas présents dans le domaine**
- **L'appareil est inclus dans le groupe de sécurité de domaine suivant**

  Si cette option est activée, une règle de déplacement d'appareil s'applique aux appareils du groupe de sécurité de domaine spécifié dans la liste sous l'option.

  Cette option est Inactif par défaut.

Onglets Segments dans le Cloud

Sous cet onglet, vous pouvez indiquer qu'il est nécessaire de déplacer les appareils inclus dans le segment dans le Cloud. Vous pouvez également déplacer des appareils de toutes les unités organisationnelles enfants de l'unité organisationnelle de domaine spécifiée :

- **L'appareil se trouve dans le segment dans le Cloud**

  Si vous sélectionnez cette option, une règle de déplacement des appareils s'applique aux appareils clients qui appartiennent à un segment dans le Cloud. Vous pouvez sélectionner le segment dans le Cloud requis jusqu'au niveau d'un sous-réseau dans la liste sous l'option.

  Cette option est Inactif par défaut.

- **Objets enfants inclus**

  Si l'option est activée, la sélection inclut les appareils de toutes les unités organisationnelles enfants du segment dans le Cloud spécifié.

  Cette option est Inactif par défaut.

- **Déplacer les appareils des objets enfants vers les sous-groupes correspondants**
- **Créer des sous-groupes qui correspondent aux conteneurs des appareils détectés pour la première fois**
- **Supprimer les sous-groupes n'ayant pas de correspondance dans les segments du Cloud**
- **L'appareil est détecté via l'utilisation de l'API**

  Dans la liste déroulante, vous pouvez sélectionner une des options suivantes :

  - Aucune valeur n'est sélectionnée. La condition ne s'applique pas.
  - **Non**. Déplacer les appareils qui ne sont pas détectés via l'utilisation de l'API.
  - **AWS**. Déplacer les appareils détectés via l'API AWS.
  - **Azure**. Déplacer les appareils détectés via l'API Azure.
  - **Google Cloud**. Déplacer les appareils détectés via l'API Google Cloud.

Ensuite, selon la valeur sélectionnée, vous pouvez renseigner les champs suivants :

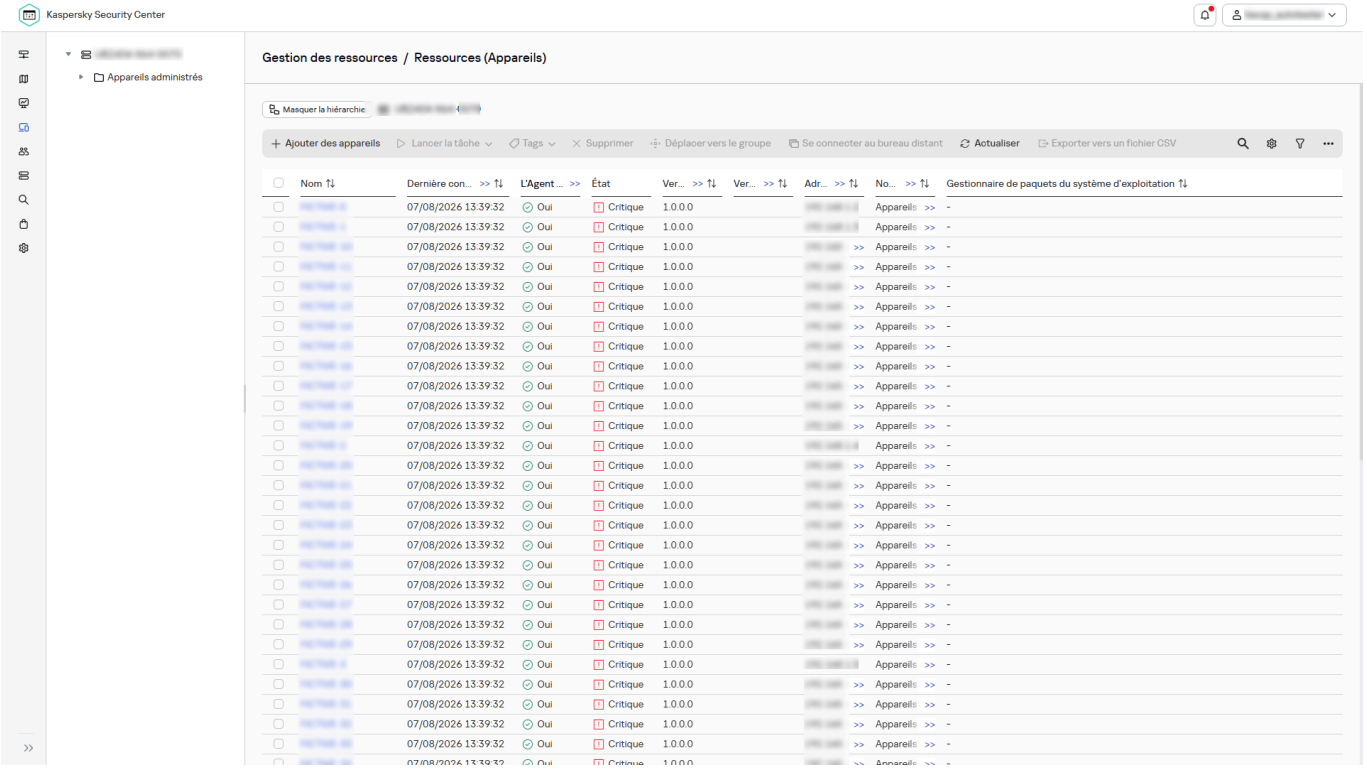
- **Sous-réseau de l'appareil cloud**.
- **Zone de disponibilité de l'appareil cloud**.
- **Groupe de déplacement de l'appareil cloud**.

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 **Gestion des ressources** → **Ressources (Appareils)**.



La liste des appareils administrés

2. Sélectionnez le groupe d'administration auquel vous souhaitez ajouter les appareils :

   - Pour le groupe racine :

     Dans ce cas, vous pouvez passer à l'étape suivante.

- Pour un sous-groupe :

  a. Cliquez sur le bouton **Afficher la hiérarchie** en haut de la page.

  Le nom du bouton devient **Masquer la hiérarchie**.

  b. Dans la fenêtre qui s'ouvre, cliquez sur le nom du sous-groupe.

  Le chemin vers le groupe sélectionné est affiché en haut de la page. Si nécessaire, vous pouvez cliquer sur un lien avec le nom du groupe d'administration pour accéder au groupe. Par défaut, le dernier lien du chemin est inactif. Vous pouvez également fermer la fenêtre de la hiérarchie en cliquant sur le bouton **Masquer la hiérarchie**.

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

   L'Assistant de déplacement des appareils est ensuite démarré.

4. 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.

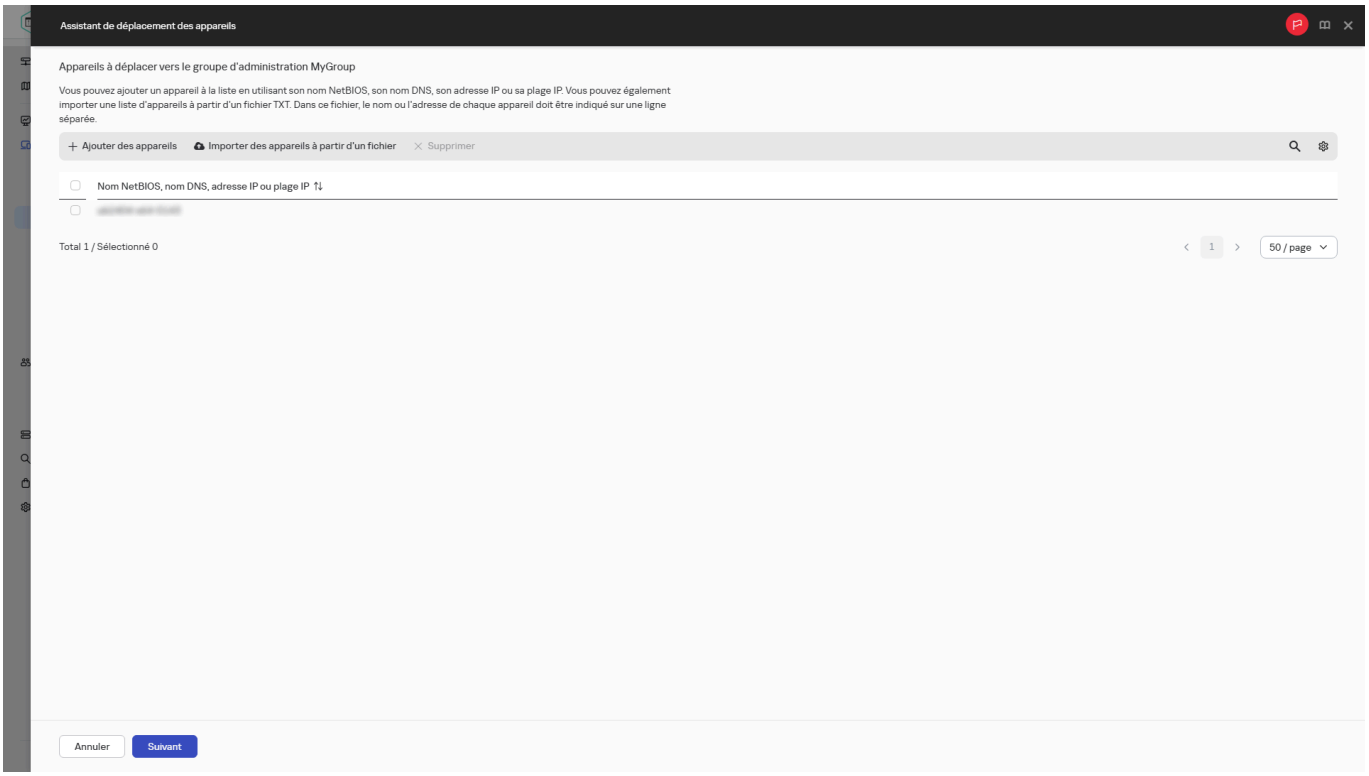
       > La plage IP ne doit pas dépasser 1 048 576 adresses.

     - 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 : , \ / * ; : & ` ~ ! @ # $ ^ & ( ) = + [ ] { } | , < > %



Sélection des appareils à déplacer dans le groupe d'administration

5. Affichez la liste des appareils à ajouter au groupe d'administration. Vous pouvez modifier la liste en ajoutant ou en supprimant des appareils.

6. Une fois que vous vous assurez que la liste est correcte, cliquez sur le bouton **Suivant**.

   L'Assistant traite la liste des appareils et affiche le résultat. Les appareils traités correctement sont inclus dans les groupes d'administration et s'affichent dans la liste des appareils sous les noms établis pour eux par le Serveur d'administration.

Déplacement manuel des appareils ou des clusters à un groupe d'administration

Vous pouvez déplacer des appareils d'un groupe d'administration vers un autre ou du groupe d'appareils non définis vers un groupe d'administration.

Vous pouvez également déplacer d'un cluster ou d'un groupe de serveurs d'un groupe d'administration à un autre. Lorsque vous déplacez un cluster ou un groupe de serveurs vers un autre groupe, tous ses nœuds se déplacent avec lui, car un cluster et l'un de ses nœuds appartiennent toujours au même groupe d'administration. Lorsque vous sélectionnez un seul nœud de cluster sous l'onglet **Appareils**, le bouton **Déplacer vers le groupe** devient indisponible.

Pour déplacer un ou plusieurs appareils ou clusters dans un groupe d'administration sélectionné, procédez comme suit :

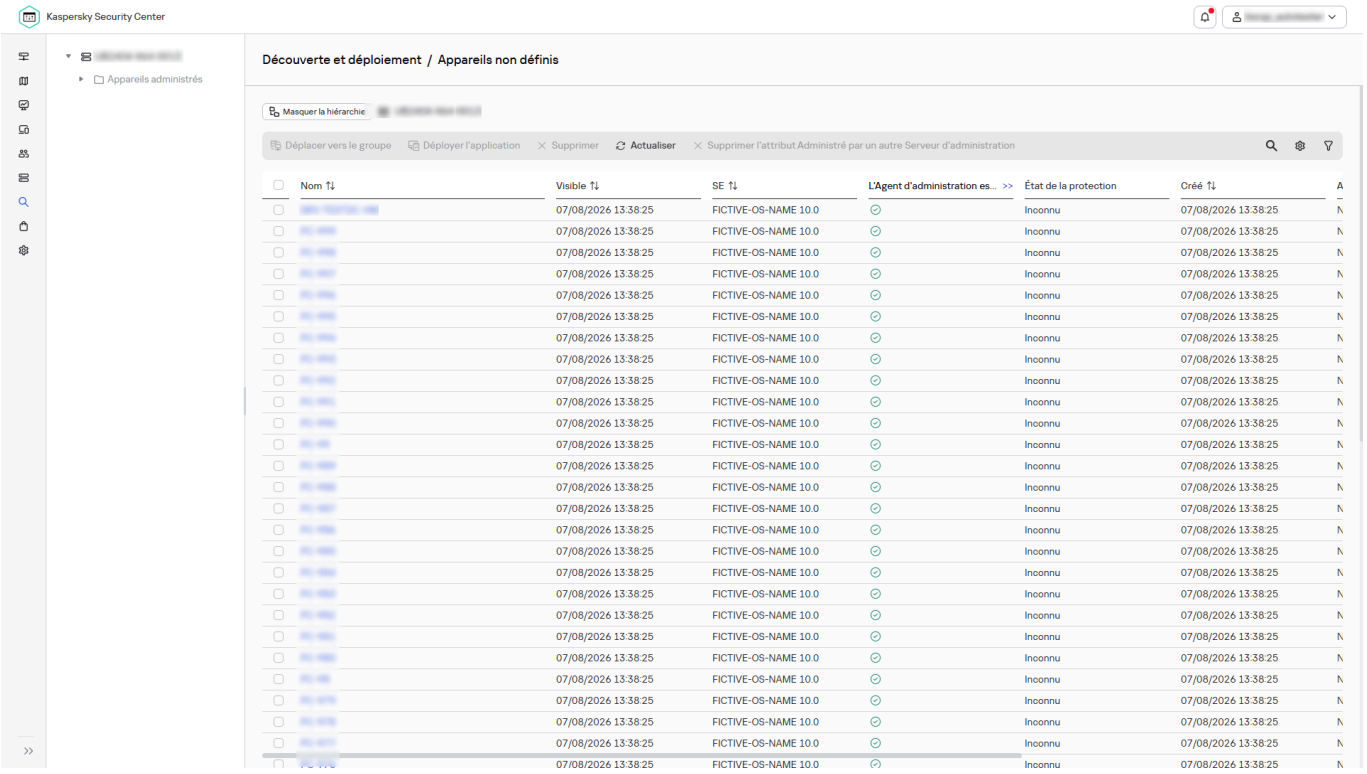
1. Ouvrez le groupe d'administration à partir duquel vous souhaitez déplacer les appareils. Pour ce faire, procédez de l'une des manières suivantes :

   - Pour ouvrir un groupe d'administration, dans le menu principal, accédez à **Gestion des ressources** → **Ressources (Appareils)**, puis sélectionnez le groupe d'administration requis.

     - Pour le groupe racine, vous pouvez passer à l'étape suivante.

     - Pour un sous-groupe, cliquez sur le bouton **Afficher la hiérarchie** en haut de la page, puis, dans la fenêtre qui s'ouvre, sélectionnez un groupe d'administration requis.

   - Pour ouvrir le groupe **Appareils non définis**, dans le menu principal, accédez à **Découverte et déploiement** → **Appareils non définis**.



La liste des appareils non attribués

2. Si le groupe d'administration contient des clusters ou des groupes de serveurs, la section **Ressources (Appareils)** est divisée en deux onglets : l'onglet **Appareils** et l'onglet **Clusters et matrices des 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 **Ressources (Appareils)** 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 des 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 **Gestion des ressources** → **Ressources (Appareils)** → **Clusters et matrices des 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.

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.

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).

Le groupe Appareils administrés comprend les groupes contenant des Serveurs d'administration, ainsi que les groupes Bureau 1 et Bureau 2.

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 dédiés dans un réseau comprenant un seul segment de réseau, en fonction du nombre d'appareils du réseau

Nombre d'appareils clients par segment de 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 dédiés dans un réseau comprenant plusieurs segments de réseau, en fonction du nombre d'appareils du réseau

Nombre d'appareils clients dans chaque 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 par segment de 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 dans chaque 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.

Les appareils fonctionnant sous Microsoft Windows sur l'architecture ARM ne peuvent pas servir de points de distribution.

Pour assigner automatiquement des points de distribution :

1. Dans le menu principal, cliquez sur le nom du Serveur d'administration.

   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 calculé leur quantité et leur configuration.

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

Les appareils fonctionnant sous Microsoft Windows sur l'architecture ARM ne peuvent pas servir de points de distribution.

Pour désigner manuellement un appareil comme point de distribution :

1. Dans le menu principal, cliquez sur le nom du Serveur d'administration.

   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 par défaut est 13000.

     - **Activé**

       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 diffusion multiple 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 de réseau via laquelle les appareils distants se connectent au point de distribution.

- **Activé**

  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 et la configuration des points de distribution pour votre réseau afin d'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.

- **Activé**

  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 et la configuration des points de distribution pour votre réseau afin d'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.

- **Activé**

  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 la source des mises à jour pour le point de distribution :

    - Pour que le point de distribution récupère les mises à jour du Serveur d'administration, sélectionnez **Récupérer depuis le Serveur d'administration**.

    - Pour autoriser le point de distribution à recevoir les mises à jour à l'aide d'une tâche, sélectionnez **Utiliser la tâche d'obtention des mises à jour** de téléchargement des mises à jour, puis spécifiez une tâche *Télécharger les mises à jour dans les référentiels des points de distribution* :

      - Si une telle tâche existe déjà sur l'appareil, sélectionnez-la dans la liste.

      - Si aucune tâche de ce type n'existe encore sur l'appareil, cliquez sur le lien **Créer la tâche** pour créer une tâche. Ceci permet de lancer l'Assistant de création d'une tâche. Suivez les étapes 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 cette case est cochée, un serveur proxy internet est utilisé pour connecter les points de distribution aux serveurs de mise à jour de Kaspersky. Dans les champs de saisie, vous pouvez 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.

- **Utiliser le protocole HTTPS**

  Si vous souhaitez que les appareils administrés se connectent au serveur proxy KSN via un port HTTPS, activez l'option **Utiliser le protocole HTTPS** et spécifiez un numéro **HTTPS par port**. Par défaut, la connexion au serveur proxy KSN est exécutée via le port HTTPS 17111.

- **Port HTTPS**

  Le numéro du port HTTPS 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 HTTPS 17111.

- 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 sondage du réseau Windows par le point de distribution Windows.
  - **Domaines Windows**

    Vous pouvez autoriser la recherche d'appareils pour les domaines Windows et programmer la recherche.

- 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.

    Dans le champ **Sondage**, une fois que vous avez placé le bouton bascule en position **Activé**, vous pouvez sélectionner les contrôleurs de domaine à sonder et également spécifier la programmation du sondage pour ces derniers.

    Si vous utilisez un point de distribution Linux, dans la section **Sonder les domaines spécifiés**, cliquez sur **Ajouter**, puis spécifiez l'adresse et les informations d'identification de l'utilisateur du contrôleur de domaine. Vous pouvez également spécifier le type de domaine à sonder : Active Directory ou Samba, FreeIPA, ALD Pro.

    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.

Ajout d'une passerelle de connexion dans la DMZ en tant que point de distribution

Si le Serveur d'administration se trouve en dehors de la zone démilitarisée (DMZ), les Agents d'administration installés sur les appareils externes ne peuvent pas se connecter au Serveur d'administration. Dans ce cas, vous pouvez utiliser un point de distribution comme passerelle de connexion dans la DMZ. Le point de distribution ouvre un port pour permettre au Serveur d'administration d'établir la connexion. Au lancement, le Serveur d'administration se connecte au point de distribution et n'interrompe pas la connexion avec ce dernier tout au long de son fonctionnement.

Si vous devez établir une connexion entre le Serveur d'administration et vos appareils administrés en dehors de la période de synchronisation entre l'Agent d'administration et le Serveur d'administration, vous devez activer un serveur push et ouvrir le port 13295 au niveau du point de distribution.

Nous vous recommandons d'utiliser un appareil spécialement dédié comme passerelle de connexion. Pour en savoir plus sur le nombre maximal d'appareils clients (y compris les appareils mobiles), consultez le guide de dimensionnement.

Une passerelle de connexion attend les connexions du Serveur d'administration au lieu d'établir des connexions avec le Serveur d'administration. Cela signifie que juste après l'installation d'une passerelle de connexion sur un appareil dans la DMZ, le Serveur d'administration n'énumère pas l'appareil parmi les appareils administrés. Par conséquent, vous avez besoin d'une procédure spéciale pour vous assurer que le Serveur d'administration amorce une connexion à la passerelle de connexion.

Pour ajouter un appareil avec une passerelle de connexion comme point de distribution :

1. Dans le menu principal, cliquez sur le nom du Serveur d'administration.

   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. Dans la barre d'outils, cliquez sur le bouton **Désigner**.

5. Dans le volet droit qui s'ouvre, réalisez les opérations suivantes :

   a. Sélectionnez l'option **Utiliser la passerelle de connexion DMZ par adresse**.

   b. Dans le champ **Adresse de la passerelle de connexion**, indiquez l'adresse IP ou le nom DNS de l'appareil.

   c. Cliquez sur le bouton **Attribuer**.

   d. Le volet se ferme, et le point de distribution s'affiche avec le nom **L'enregistrement temporaire pour la passerelle de connexion**.

6. Cliquez sur **Enregistrer**.

   Le Serveur d'administration tente de se connecter à la passerelle de connexion à l'adresse que vous avez indiquée. Si l'opération réussit, le nom de l'entrée devient le nom de l'appareil de la passerelle de connexion. Ce processus prend jusqu'à cinq minutes.

Si vous ouvrez les propriétés du point de distribution en cliquant sur le nom **L'enregistrement temporaire pour la passerelle de connexion**, toutes les options sont grisées. Vous pouvez uniquement consulter l'onglet Général qui affiche le nom du point de distribution. Le numéro du port est de 13000 par défaut. Vous ne pouvez configurer le point de distribution qu'une fois que le Serveur d'administration s'y est connecté. Pendant que l'entrée temporaire pour la passerelle de connexion est convertie en une entrée nommée, la passerelle de connexion s'affiche également dans le groupe Appareils non définis.

Pour ajouter une passerelle de connexion à un réseau précédemment configuré, procédez comme suit :

1. Installer l'Agent d'administration en mode passerelle de connexion.

2. Réinstallez l'Agent d'administration sur les appareils que vous souhaitez connecter à la passerelle de connexion récemment ajoutée.

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 **Gestion des ressources** → **Ressources (Appareils)**.

2. Sélectionnez un groupe d'administration pour lequel vous souhaitez afficher les points de distribution attribués en cliquant sur le bouton **Afficher la hiérarchie** en haut de la page, puis dans la fenêtre qui s'ouvre, cliquez sur le nom du groupe requis.

   Cela active l'option de menu **Points de distribution**.

   Le chemin vers le groupe sélectionné est affiché en haut de la page. Si nécessaire, dans ce chemin, vous pouvez cliquer sur un lien avec le nom du groupe d'administration pour accéder au groupe. Par défaut, le dernier lien du chemin est inactif.

3. Dans le menu principal, accédez à **Gestion des ressources** → **Points de distribution**.

4. Pour ajouter de nouveaux points de distribution pour le groupe d'administration, cliquez sur le bouton **Désigner**.

5. 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 le nom du Serveur d'administration.

   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 **Activé**.

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.

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 basé sur Linux qui sert de point de distribution, exécutez la commande suivante :

   ```
   systemctl edit klnagent64.service
   ```

2. Spécifiez les limites souples et maximales des descripteurs de fichiers dans le paramètre `LimitNOFILE` de la section `[Service]` :

   ```
   LimitNOFILE=<limite de ressource souple>:<limite de ressources rigide>
   ```

   Par exemple, `LimitNOFILE=32768:131072`. Notez que la limite logicielle des descripteurs de fichier doit être inférieure ou égale à la limite stricte.

3. 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.

4. Exécutez la commande suivante pour recharger le processus systemd :

   ```
   systemctl daemon-reload
   ```

5. Exécutez la commande suivante pour redémarrer le service de l'Agent d'administration :

   ```
   systemctl restart klnagent
   ```

6. Exécutez la commande suivante pour vous assurer que les paramètres indiqués sont appliqués correctement :

   ```
   less /proc/<nagent process id>/limits
   ```

   où le paramètre `<nagent process id>` est l'identifiant du processus de l'Agent d'administration. Vous pouvez exécuter la commande suivante pour obtenir l'identifiant :

   ```
   ps -ax | grep klnagent
   ```

Pour le point de distribution Linux, la limite d'ouvertures de fichiers est augmentée.

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). 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*. 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. • 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.

Condition	Description de la condition	Valeurs possibles
Durée requise depuis le redémarrage	L'appareil est visible sur le réseau, mais une application a demandé son redémarrage depuis plus longtemps que la durée indiquée.	Plus de 0 minute.
Raison du redémarrage	L'appareil est visible sur le réseau, mais une application nécessite son redémarrage pour l'une des raisons sélectionnées.	• Raison de redémarrage inconnue • L'application ne peut s'exécuter avant le redémarrage • Le redémarrage est requis pour terminer la mise à jour. L'application est exécutée • Le redémarrage est requis pour le lancement de la mise à jour • Le redémarrage est requis pour la fin de l'analyse ou la désinfection • Le redémarrage est requis pour terminer l'installation/la désinstallation à distance • Fin de chiffrement des données sur le disque
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.
Des vulnérabilités dans les applications ont été détectées	L'appareil est visible sur le réseau, et l'Agent d'administration est installé sur l'appareil, mais la tâche *Recherche de vulnérabilités et de mises à jour requises* a détecté des vulnérabilités avec le niveau de gravité indiqué dans les applications installées sur l'appareil.	• Critique • Élevé. • Normal. • Ignorer s'il est impossible de fermer la vulnérabilité. • Ignorer si la mise à jour a été désignée à l'installation.
La licence a expiré	L'appareil est visible sur le réseau, mais la licence a expiré.	• Le bouton radio est éteint. • Le bouton radio est allumé.
La licence expire bientôt	L'appareil est visible sur le réseau, mais la licence expirera sur l'appareil dans moins de jours que le nombre indiqué.	Plus de 0 jour.

Condition	Description de la condition	Valeurs possibles
La vérification de mises à jour Windows Update n'a pas eu lieu depuis longtemps	L'appareil est visible sur le réseau, mais la tâche *Recherche de vulnérabilités et des mises à jour requises* n'a plus été exécutée dans la période indiquée.	Plus de 1 jour.
État de chiffrement non valide	L'Agent d'administration est installé sur l'appareil mais le résultat du chiffrement de l'appareil est égal à la valeur indiquée.	• Ne correspond pas à la stratégie à cause du refus de l'utilisateur (uniquement pour les appareils externes). • Ne correspond pas à la stratégie à cause de l'erreur. • Stratégie en cours d'application – le redémarrage est requis. • La stratégie de chiffrement n'est pas définie. • Non pris en charge. • Stratégie en cours d'application.
Les paramètres de l'appareil mobile ne correspondent pas à la stratégie	Les paramètres de l'appareil mobile se distinguent des paramètres définis dans la stratégie Kaspersky Endpoint Security for Android lors de l'analyse des règles de concordance.	• Le bouton radio est éteint. • Le bouton radio est allumé.
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. Les appareils administrés peuvent voir leur état défini par les applications administrées, indépendamment des paramètres de Kaspersky Security Center Linux. Une fois que cet état renvoie l'un des états définis par Kaspersky Security Center Linux, le Serveur d'administration attribue à un appareil administré l'état le plus critique parmi ceux renvoyés par l'application administrée et attribués par le Serveur d'administration. Les états définis par les applications gérées sont accompagnés de descriptions transférées par les applications gérées. Vous pouvez consulter les descriptions dans la liste des appareils administrés, dans la colonne **Description de l'état**.	• 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.

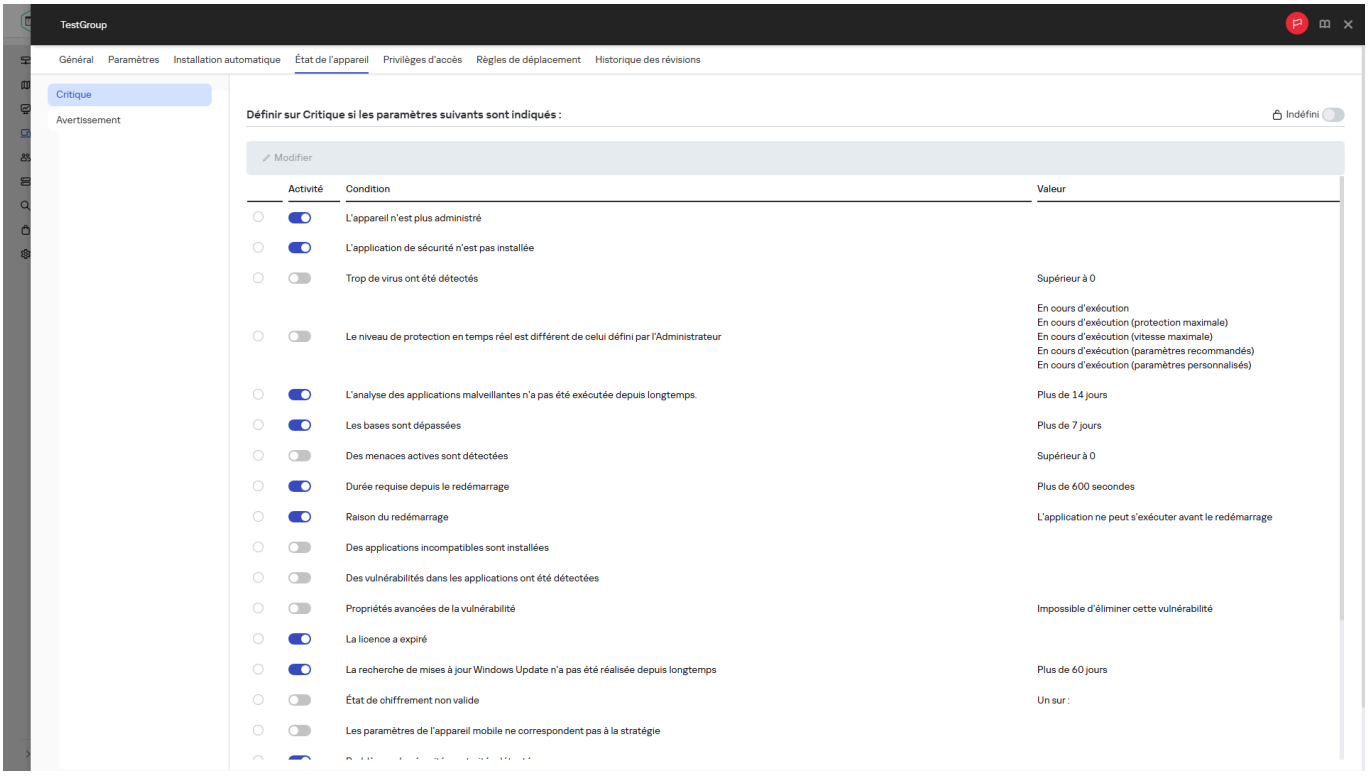
Configuration de la permutation des états des appareils

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 **Gestion des ressources** → **Hiérarchie des groupes**.
2. Accédez aux propriétés du groupe d'administration pour lequel vous souhaitez modifier l'état des appareils de l'une des manières suivantes :
   - Cliquez sur le nom du groupe d'administration.
   - Cliquez sur le bouton **Afficher la hiérarchie** en haut de la page. Dans le panneau de navigation qui s'ouvre, placez le curseur de la souris sur le nom du groupe requis, puis cliquez sur l'icône des paramètres (⚙).

   La fenêtre des propriétés du groupe d'administration s'ouvre.
3. Dans la fenêtre des propriétés, sélectionnez l'onglet **État de l'appareil**.
4. Dans le volet de gauche, sélectionnez **Critique**.
5. Dans le volet droit, dans la section **Définir sur Critique si les paramètres suivants sont indiqués**, 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**.
10. Cliquez sur **Enregistrer** pour enregistrer les modifications.

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 **Gestion des ressources** → **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 sur Avertissement si les paramètres suivants sont indiqués,** 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**.
10. Cliquez sur **Enregistrer** pour enregistrer les modifications.

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 **Gestion des ressources** → **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 **Gestion des ressources** → **Sélections d'appareils**.

   Une page comportant une liste de sélections d'appareils s'affiche.

2. Cliquez sur **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 **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 **Enregistrer**.

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 **Gestion des ressources** → **Sélections d'appareils**.

   Une page comportant une liste de sélections d'appareils s'affiche.

2. Sélectionnez la sélection d'appareils définie par l'utilisateur pertinente, puis cliquez sur le bouton **Propriétés**.

   La fenêtre **Paramètres de sélection d'appareils** s'ouvre.

3. Sous l'onglet **Général**, cliquez sur le lien **Nouvelle condition**.

4. Définissez les conditions à remplir pour inclure les appareils dans cette sélection.

5. Cliquez sur le bouton **Enregistrer**.

Les paramètres sont appliqués et enregistrés.

Les paramètres des conditions d'ajout des appareils à une sélection sont décrits ci-dessous. Les conditions sont combinées à l'aide de l'opérateur logique " ou " : la sélection reprend les appareils qui répondent au moins à une des conditions présentées.

Général

La section **Général** permet de modifier le nom de la condition de la sélection et d'indiquer si cette condition doit être intervertie :

Inverser la condition de sélection

Cette option est Inactif par défaut.

Si vous activez cette option, la condition de sélection définie sera inversée. Tous les appareils qui ne correspondent pas à la condition feront partie de la sélection.

L'exemple suivant montre la logique du travail d'inversion :

- **Condition** : sur votre appareil, il y a un système d'exploitation avec le type Linux et le numéro de build 00.0.000.

- **Condition inversée** : sur votre appareil, il existe un système d'exploitation avec NOT (le type de version Linux et le numéro de build 00.0.000), ce qui équivaut à ce qui suit :

  Il existe un système d'exploitation de type NOT Linux OU numéro de build NOT 00.0.000.

Ainsi, la sélection inclura les appareils équipés d'un système d'exploitation, par exemple, de type Windows et dont le numéro de build est 00.0.000, ou de type Linux et dont le numéro de build est différent de 00.0.000.

Infrastructure réseau

La sous-section **Réseau** permet de configurer les critères d'inclusion des appareils dans une sélection sur la base de leurs données de réseau.

- **Nom de l'appareil**

  Nom de réseau Windows (nom NetBIOS) de l'appareil ou adresse IPv4 ou IPv6.

- **Domaine**

  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 du 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.

- **L'appareil est 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 de l'appareil

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 protection en temps réel ;**

  Liste déroulante vous permettant de sélectionner l'état de la protection en temps réel. Les appareils avec l'état indiqué de la protection en temps réel seront inclus dans la sélection.

- **Description d'état de l'appareil**

  Ce champ permet de cocher les cases en regard des conditions qui, lorsqu'elles sont remplies, affectent l'un des états suivants à l'appareil : *OK, Critique* ou *Avertissement*.

La sous-section **État des modules des applications administrées** permet de configurer les critères d'inclusion des appareils dans une sélection sur la base de l'état des modules dans les applications administrées :

- **État de la protection contre les fuites de données**

  Recherchez des appareils sur la base de l'état de la Protection contre les fuites de données (*Inconnu, Arrêté(e), En cours de démarrage, Suspendu(e), En cours d'exécution, Échec*).

- **État de la protection des serveurs de collaboration**

  Recherchez des appareils sur la base de l'état de la protection de collaboration du serveur (*Inconnu*, *Arrêté(e)*, *En cours de démarrage, Suspendu(e)*, *En cours d'exécution*, *Échec*).

- **État de la protection antivirus des serveurs de messagerie**

  Recherchez des appareils sur la base de l'état de la protection du Serveur de messagerie (*Inconnu, Arrêté(e), En cours de démarrage, Suspendu(e), En cours d'exécution, Échec*).

- **État d'Endpoint Sensor**

  Recherchez des appareils sur la base de l'état du module Endpoint Sensor (*Inconnu, Arrêté(e), En cours de démarrage, Suspendu(e), En cours d'exécution, Échec*).

La sous-section **Problèmes ayant 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 du système

La section **SE** 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.

- **Architecture 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.

- **Compilation 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 :

  - **Indéfini**.
  - **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 :

  - **Indéfini**.
  - **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.

- **Fournisseur**

  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 de l'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, 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 cœurs de processeur virtuel, 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 cœurs de CPU virtuels, 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, en Go, à partir de**

  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, en Go, à**

  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 mémoire vive, en Mo, à partir de**

  La taille minimale de la RAM de l'appareil. Les appareils dont la RAM correspond à la plage de valeurs indiquée dans les champs de saisie (incluse) sont inclus dans la sélection.

- **Taille de la mémoire vive, en Mo, à**

  La taille maximale de la RAM de l'appareil. Les appareils dont la RAM correspond à la plage de valeurs indiquée dans les champs de saisie (incluse) sont inclus dans la sélection.

Détails du logiciel 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.

- **Fournisseur**

  La liste déroulante qui permet de sélectionner l'éditeur de l'application installée sur l'appareil.

- **l'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.

Déploiement d'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**. La sélection inclut les appareils qui ne sont pas administrés par Kaspersky Security Center.
  - **La valeur n'est pas sélectionnée**. Les critères ne sont pas appliqués.

- **L'application de sécurité est installée**

  La liste déroulante permet d'ajouter à la sélection d'appareils ceux sur lesquels l'application de sécurité est installée :

  - **Oui**. L'application inclut les appareils sur lesquels l'application de sécurité est installée dans la sélection d'appareils.
  - **Non**. L'application inclut les appareils sur lequel l'application de sécurité n'est pas installée dans la sélection d'appareils.
  - **La valeur n'est pas sélectionnée**. Les critères ne sont pas appliqués.

La sous-section **Endpoint Protection** permet de configurer les critères d'inclusion d'appareils dans une sélection sur la base de leur état de la protection :

- **Les bases de données sont publiées**

  Si l'option est activée, la recherche d'appareils clients s'exécute selon la date de publication des bases antivirus. Les champs de saisies permettent d'indiquer l'intervalle de temps sur la base duquel la recherche aura lieu.

  Cette option est Inactif par défaut.

- **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 Next Expert View.

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 **Tags**. Indiquez s'il faut inclure ou exclure les appareils avec les tags sélectionnés dans la sélection d'appareils.

- **Tous les appareils qui présentent ce tag**

  Si vous avez choisi cette option, les résultats de la recherche reprennent les appareils dont la description contient le tag sélectionné. Dans le cadre de la recherche d'appareils, vous pouvez utiliser le caractère * qui remplace n'importe quelle chaîne quel que soit le nombre de caractères.

  Cette option est sélectionnée par défaut.

- **Tous les appareils qui ne présentent pas ce tag**

  Si vous avez choisi cette option, les résultats de la recherche reprennent les appareils dont la description ne contient pas le tag sélectionné. Dans le cadre de la recherche d'appareils, vous pouvez utiliser le caractère * qui remplace n'importe quelle chaîne quel que soit le nombre de caractères.

Utilisateurs

La section **Utilisateurs** permet de configurer les critères d'inclusion des appareils dans une sélection sur la base des comptes utilisateurs utilisés pour ouvrir la session dans le système d'exploitation.

- **Dernier utilisateur ayant accédé au système**

  Si cette option est activée, vous pouvez sélectionner le compte pour configurer le critère. Les résultats de la recherche incluent les appareils sur lesquels l'utilisateur sélectionné a effectué la dernière connexion au système.

- **Utilisateur ayant déjà accédé au système**

  Si l'option est activée, cliquez sur le bouton **Parcourir** pour définir un compte utilisateur. Les résultats de recherche comprennent les appareils sur lesquels l'utilisateur indiqué a déjà accédé au système.

Propriétaire de l'appareil

Dans la section **Propriétaire de l'appareil**, vous pouvez configurer les critères d'inclusion des appareils dans la sélection en fonction des propriétaires enregistrés, de leurs rôles et de leur appartenance à des groupes de sécurité :

- **Propriétaire de l'appareil**

  Sélectionnez le nom d'utilisateur du propriétaire de l'appareil dans le groupe de sécurité interne. Apprenez-en plus à propos des utilisateurs et des rôles des utilisateurs dans cette section.

  Un seul utilisateur peut être enregistré en tant que propriétaire de l'appareil.

- **Appartenance du propriétaire de l'appareil au groupe de sécurité Active Directory**

  Sélectionnez un groupe de sécurité externe Active Directory auquel appartient le propriétaire de l'appareil.

  L'utilisateur peut appartenir à un groupe de sécurité Active Directory ou faire partie d'un groupe inclus dans ce groupe de sécurité Active Directory.

- **Rôle du propriétaire de l'appareil**

  Sélectionnez le rôle attribué au propriétaire de l'appareil. Apprenez-en plus à propos des rôles des utilisateurs dans cet article.

- **Appartenance du propriétaire de l'appareil au groupe de sécurité interne**

  Sélectionnez un groupe de sécurité interne auquel appartient le propriétaire de l'appareil.

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 **Gestion des ressources** → **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.

Vous ne pouvez ajouter qu'une seule règle de balisage automatique par balise. Si vous créez une nouvelle règle pour la même balise, la règle précédente sera remplacée.

Un tag est automatiquement supprimé d'un appareil dans les cas suivants :

- Dès que l'appareil cesse de remplir les conditions de la règle qui attribue le tag.
- Lorsque la règle qui attribue la balise est désactivée ou supprimée.

La liste des tags et la liste des règles sur chaque Serveur d'administration sont indépendantes de tous les autres Serveurs d'administration, y compris du Serveur d'administration principal ou des Serveurs d'administration secondaires virtuels. Une règle est appliquée uniquement aux appareils du même Serveur d'administration sur lequel la règle est créée.

Création d'un tag de l'appareil

Pour créer un tag de l'appareil, procédez comme suit :

1. Dans le menu principal, accédez à **Gestion des ressources** → **Tags** → **Tags de l'appareil**.
2. Cliquez sur **Ajouter**.

   Une fenêtre de nouveau tag s'ouvre.
3. Dans le champ **Tags**, saisissez le nom du tag.
4. Cliquez sur **Enregistrer** pour 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 **Gestion des ressources** → **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 **Tags**, 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 **Gestion des ressources** → **Tags** → **Tags de l'appareil**.
   La liste des tags s'affiche.
2. Sélectionnez le tag de l'appareil que vous souhaitez supprimer.
3. Ensuite, 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 gérer ce type de tags, 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 **Gestion des ressources** → **Tags** → **Tags de l'appareil**.

2. Cliquez sur le lien **Consulter les appareils** en regard du tag pour lequel vous souhaitez voir les appareils associés.

   Vous serez redirigé vers la section **Ressources (Appareils)** du menu principal, avec les appareils filtrés en fonction du tag pour lequel vous avez cliqué sur le lien **Consulter les appareils**.

3. Pour revenir à la liste des tags de l'appareil, cliquez sur le bouton **Retour** de votre navigateur.

Après avoir consulté les appareils auxquels le tag est attribué, vous pouvez créer et attribuer un nouveau tag ou attribuer le tag existant à d'autres appareils. Dans ce cas, vous devez supprimer le filtre par tag, sélectionner les appareils, puis attribuer le tag.

Consultation des tags attribués à un appareil

Pour voir les tags attribués à un appareil :

1. Dans le menu principal, accédez à **Gestion des ressources** → **Ressources (Appareils)**.

2. Cliquez sur le nom de l'appareil dont vous souhaitez voir les tags.

3. Dans la fenêtre des propriétés de l'appareil qui s'ouvre, sélectionnez l'onglet **Tags**.

   La liste des tags attribués à l'appareil sélectionné s'affiche. La colonne **Tag défini** permet de consulter la manière dont le tag a été attribué.

Dans la barre d'outils, vous pouvez effectuer l'une des opérations suivantes :

- Attribuez un autre tag à l'appareil.
- Supprimez un tag déjà attribué.
- Affichez tous les tags de l'appareil qui existent sur le Serveur d'administration.

Vous ne pouvez pas afficher les tags attribués localement sur l'appareil.

Attribution manuelle d'un tag à un appareil

Pour attribuer un tag manuellement à un appareil, procédez comme suit :

1. Consultez les tags attribués à l'appareil auquel vous souhaitez attribuer un autre tag.
2. Cliquez sur **Ajouter**.
3. Dans la fenêtre qui s'ouvre, réalisez une des opérations suivantes :
   - Pour créer un tag et l'attribuer, sélectionnez **Créer un tag**, puis renseignez le nom du nouveau tag.
   - Pour sélectionner un tag existant, sélectionnez **Attribuer un tag existant**, puis sélectionnez le tag nécessaire dans la liste déroulante.
4. Cliquez sur le bouton **OK** pour appliquer les modifications.
5. Cliquez sur **Enregistrer** pour 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 **Gestion des ressources** → **Ressources (Appareils)**.
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 **OK**.

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 gérer 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 :

Exécutez une des actions suivantes :

- Dans le menu principal, accédez à **Gestion des ressources** → **Tags** → **Règles d'attribution automatique de tags**.
- Dans le menu principal, accédez à **Gestion des ressources** → **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 **Configurer les règles d'attribution automatique de tags**.

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. 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**.

4. Exécutez une des actions 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 **Enregistrer** pour 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 **Tags**, 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 la règle pour qu'elle se déclenche dans les conditions suivantes (vous pouvez sélectionner 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, l'architecture du système d'exploitation, et le gestionnaire de paquets.
   - **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 **Enregistrer** pour 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 le bouton **Supprimer**.
4. Dans la fenêtre qui s'ouvre, cliquez sur **OK**.

   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. Exécutez la commande suivante pour redémarrer le service de l'Agent d'administration :

   ```
   systemctl restart klnagent
   ```

   L'utilitaire klscflag attribue les tags définis à votre appareil.

4. Si vous souhaitez vous assurer que l'utilitaire klscflag a bien attribué les tags définis, [affichez les tags attribués à l'appareil](#).

Vous pouvez également [attribuer des tags d'appareil manuellement](#).

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

Nous ne recommandons pas d'activer le chiffrement dans VDI.

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 la section **Gestion des ressources** → **Ressources (Appareils)**.
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 de masse. 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** → **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 de masse

- 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 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 pour la plateforme requise.

Pour autoriser l'accès à un disque chiffré en mode hors ligne dans Kaspersky Endpoint Security for Windows, 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.

Transmission des clés de chiffrement entre les Serveurs d'administration

Si la fonctionnalité de chiffrement des données est activée sur un appareil administré, la clé de chiffrement est stockée sur le Serveur d'administration. La clé de chiffrement est utilisée pour accéder aux données chiffrées et pour administrer la stratégie de chiffrement.

La clé de chiffrement doit être transmise à un autre Serveur d'administration dans les cas suivants :

- Vous reconfigurez l'Agent d'administration sur un appareil administré pour affecter l'appareil à un autre Serveur d'administration. Si cet appareil contient des données chiffrées, la clé de chiffrement doit être transmise au Serveur d'administration cible. Sinon, les données ne peuvent pas être déchiffrées.

- Vous chiffrez un disque amovible connecté à un appareil D1 administré par le Serveur d'administration S1, puis vous connectez ce disque amovible à un appareil D2 administré par le Serveur d'administration S2. Pour accéder aux données sur le disque amovible, la clé de chiffrement doit être transmise du Serveur d'administration S1 au Serveur d'administration S2.

- Vous chiffrez un fichier sur un appareil D1 administré par le Serveur d'administration S1, puis vous essayez d'accéder au fichier sur un appareil D2 administré par le Serveur d'administration S2. Pour accéder au fichier, la clé de chiffrement doit être transmise du Serveur d'administration S1 au Serveur d'administration S2.

Vous pouvez transmettre des clés de chiffrement des manières suivantes :

- Automatiquement, en activant l'option **&Utiliser la hiérarchie des Serveurs d'administration pour obtenir des clés de chiffrement** dans les propriétés de deux Serveurs d'administration entre lesquels une clé de chiffrement doit être transmise. Si cette option est désactivée pour l'un des Serveurs d'administration, la transmission automatique des clés de chiffrement n'est pas possible.

  Lorsque vous activez l'option **&Utiliser la hiérarchie des Serveurs d'administration pour obtenir des clés de chiffrement** dans un Serveurs d'administration, le Serveur d'administration envoie toutes les clés de chiffrement stockées dans son stockage au Serveur d'administration principal (le cas échéant) d'un niveau supérieur dans la hiérarchie.

  Lorsque vous essayez d'accéder à des données chiffrées, le Serveur d'administration recherche d'abord la clé de chiffrement dans son propre stockage. Si l'option **&Utiliser la hiérarchie des Serveurs d'administration pour obtenir des clés de chiffrement** est activée et que la clé de chiffrement requise n'a pas été trouvée dans le stockage, le Serveur d'administration envoie également une demande aux Serveurs d'administration principaux (le cas échéant) de lui fournir la clé de chiffrement requise. La demande sera envoyée à tous les Serveurs d'administration principaux jusqu'au serveur situé au niveau le plus élevé de la hiérarchie.

- Manuellement d'un Serveur d'administration à un autre en exportant et en important le fichier contenant les clés de chiffrement.

  L'exportation et l'importation des clés de chiffrement sont des actions incluses dans la fonctionnalité Gestion des clés de chiffrement. Pour exécuter ces actions, configurez les privilèges d'accès à la fonctionnalité pour les utilisateurs de Kaspersky Security Center Linux comme suit :

  - Accordez le privilège d'accès **Lire** à la fonction de gestion des clés de chiffrement à l'utilisateur qui exporte les clés de chiffrement depuis le Serveur d'administration secondaire.

  - Accordez le privilège d'accès **Écrire** à la fonction de gestion des clés de chiffrement à l'utilisateur qui importe les clés de chiffrement sur le Serveur d'administration cible.

Pour activer la transmission automatique des clés de chiffrement entre les Serveurs d'administration au sein de la hiérarchie, procédez comme suit :

1. Accédez aux propriétés du Serveur d'administration requis :

   a. Dans le menu principal, sélectionnez une section (à l'exception de **Place de marché**, **Navigation dans la console** et **Paramètres**), puis, en haut de la page, cliquez sur le bouton **Afficher la hiérarchie**.

   b. Dans le panneau de navigation qui s'ouvre, placez le curseur de la souris sur le nom du Serveur d'administration requis, puis cliquez sur l'icône des paramètres (⚙).

   Vous pouvez également cliquer sur le nom du Serveur d'administration, puis, une fois que le nom s'affiche dans le menu principal, cliquer dessus dans le menu principal pour ouvrir la fenêtre des propriétés du serveur.

2. Dans la fenêtre des propriétés qui s'ouvre, sélectionnez la section **Algorithme de chiffrement**.

3. Activez l'option **&Utiliser la hiérarchie des Serveurs d'administration pour obtenir des clés de chiffrement**.

4. Cliquez sur **Enregistrer** pour appliquer les modifications.

Les clés de chiffrement seront transmises aux Serveurs d'administration principaux (le cas échéant) lors de la prochaine synchronisation (le battement de cœur). Ce Serveur d'administration fournira également, sur demande, une clé de chiffrement de son stockage à un Serveur d'administration secondaire.

Pour transmettre manuellement les clés de chiffrement entre les Serveur d'administration :

1. Accédez aux propriétés du Serveur d'administration à partir duquel vous souhaitez exporter les clés de chiffrement :

   a. Dans le menu principal, sélectionnez une section (à l'exception de **Place de marché**, **Navigation dans la console** et **Paramètres**), puis, en haut de la page, cliquez sur le bouton **Afficher la hiérarchie**.

   b. Dans le panneau de navigation qui s'ouvre, placez le curseur de la souris sur le nom du Serveur d'administration requis, puis cliquez sur l'icône des paramètres (⚙).

   Vous pouvez également cliquer sur le nom du Serveur d'administration, puis, une fois que le nom s'affiche dans le menu principal, cliquer dessus dans le menu principal pour ouvrir la fenêtre des propriétés du serveur.

2. Dans la fenêtre des propriétés qui s'ouvre, sélectionnez la section **Algorithme de chiffrement**.

3. Cliquez sur **Exporter des clés de chiffrement**.

   Assurez-vous que l'utilisateur qui exporte les clés de chiffrement depuis le Serveur dispose du privilège d'accès **Lire** pour la fonction de gestion des clés de chiffrement.

4. Dans la fenêtre **Exporter les clés de chiffrement à partir du Serveur d'administration ?** :

   a. Spécifiez un mot de passe pour protéger le fichier contre tout accès non autorisé.

   b. Spécifiez où vous souhaitez enregistrer le fichier.

   N'oubliez pas le mot de passe. Un mot de passe oublié ne peut pas être récupéré. Si le mot de passe est perdu, vous devez répéter la procédure d'exportation. Par conséquent, prenez note du mot de passe et conservez-le à portée de main.

5. Transmettez le fichier à un autre Serveur d'administration, par exemple, via un dossier partagé ou un lecteur amovible.

6. Accédez aux propriétés du Serveur d'administration vers lequel vous souhaitez importer les clés de chiffrement.

7. Dans la fenêtre des propriétés, sélectionnez la section **Algorithme de chiffrement**.

8. Cliquez sur **Importer des clés de chiffrement**.

   Assurez-vous que l'utilisateur qui importe les clés de chiffrement depuis le Serveur dispose du privilège d'accès **Écrire** pour la fonction de gestion des clés de chiffrement.

9. Sélectionnez le fichier contenant les clés de chiffrement.

10. Indiquez le mot de passe.

11. Cliquez sur le bouton **OK**.

Les clés de chiffrement sont transmises au Serveur d'administration cible.

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 étapes de l'assistant. Dans la fenêtre **Nouvelle tâche** de l'Assistant d'ajout de tâche, sélectionnez l'application **Kaspersky Security Center 16.2** 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 de la 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.

Évitement des conflits entre plusieurs Serveurs d'administration

Si le réseau compte plus d'un Serveur d'administration, ils peuvent voir les mêmes appareils clients. Cela peut entraîner, par exemple, l'installation par le Serveur d'administration d'une application déjà installée par un autre Serveur d'administration, et d'autres conflits. Pour empêcher l'installation d'une application sur un appareil administré par un autre Serveur d'administration, vous devez activer l'option **Installer uniquement sur les appareils administrés via &ce Serveur d'administration** dans les propriétés de la tâche *Installation à distance d'une application*.

Si vous activez l'option **Installer uniquement sur les appareils administrés via &ce Serveur d'administration**, puis que vous exécutez la tâche *Installation à distance d'une application*, une vérification est effectuée afin de déterminer si les appareils sont administrés par un autre Serveur d'administration. Pour les appareils administrés par un autre Serveur d'administration, la valeur de l'attribut **Administrés par un autre Serveur d'administration** est définie sur `true`. La tâche *Installation à distance d'une application* ne sera pas appliquée à ces appareils.

Les valeurs de l'attribut **Administrés par un autre Serveur d'administration** s'affichent dans la colonne **Administrés par un autre Serveur d'administration** dans la liste des appareils administrés et la liste des appareils non définis.

Vous pouvez également utiliser la propriété **Administrés par un autre Serveur d'administration** en tant que critère aux fins suivantes :

- Affichage des appareils administrés
- Sélections d'appareils
- Règles de déplacement des appareils
- Règles d'attribution automatique de tags

Pour réinitialiser l'attribut Administrés par un autre Serveur d'administration :

1. Dans le menu principal de Kaspersky Security Center Web Console, accédez à **Découverte et déploiement** → **Appareils non définis**.
2. Sélectionnez l'appareil requis, puis cliquez sur le bouton **Supprimer l'attribut Administré par un autre Serveur d'administration**.

L'attribut **Administrés par un autre Serveur d'administration** est réinitialisé.

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 "<passerelle ip ou nom>" -svt STRING_T -ss "|ss_type = \"SS_SETTINGS\";"`

     Ici, le paramètre `<passerelle ip ou nom>` 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.

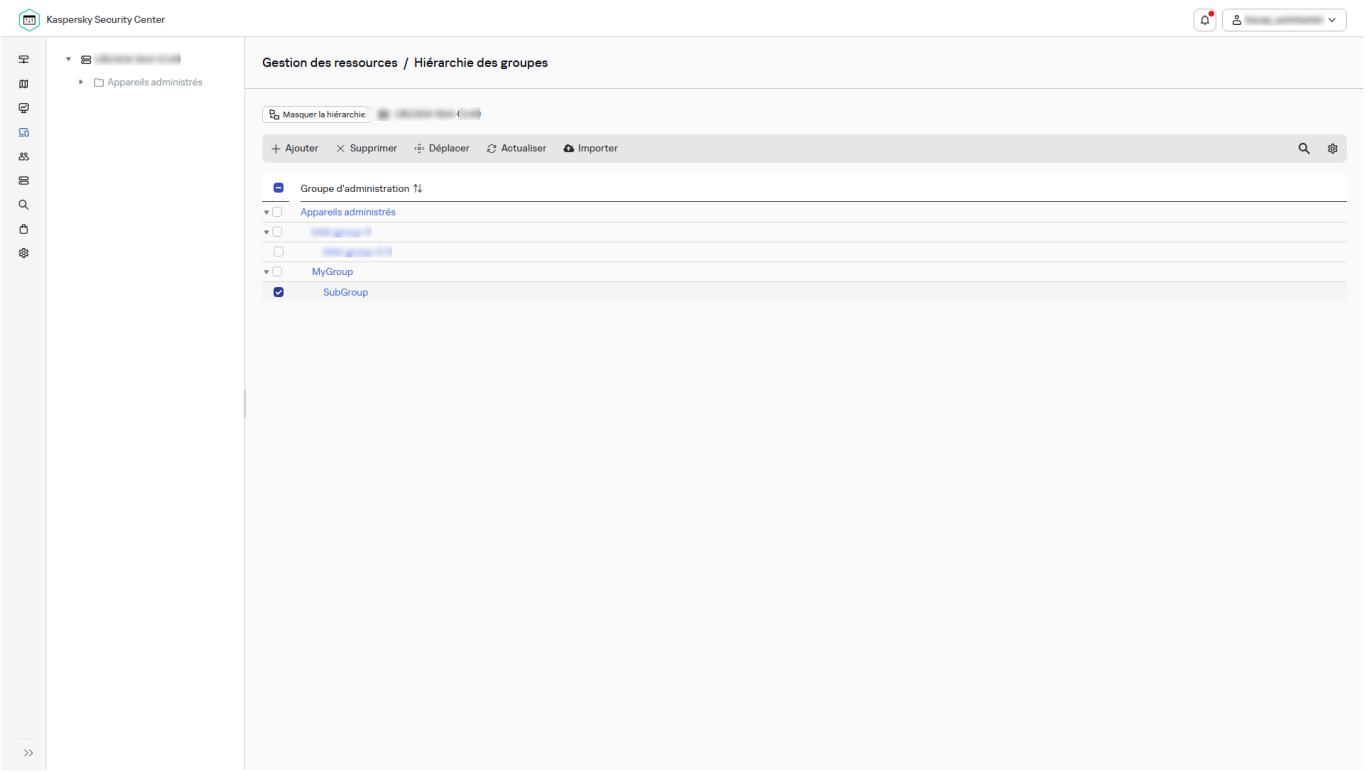
Pour voir ou configurer les actions lorsque les appareils du groupe sont inactifs :

1. Dans le menu principal, accédez à **Gestion des ressources** → **Hiérarchie des groupes**.

2. Accédez aux propriétés du groupe d'administration requis de l'une des manières suivantes :

   - Cliquez sur le nom du groupe d'administration.

   - Cliquez sur le bouton **Afficher la hiérarchie** en haut de la page. Dans le panneau de navigation qui s'ouvre, placez le curseur de la souris sur le nom du groupe requis, puis cliquez sur l'icône des paramètres (⚙).



Hiérarchie du groupe d'administration

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.

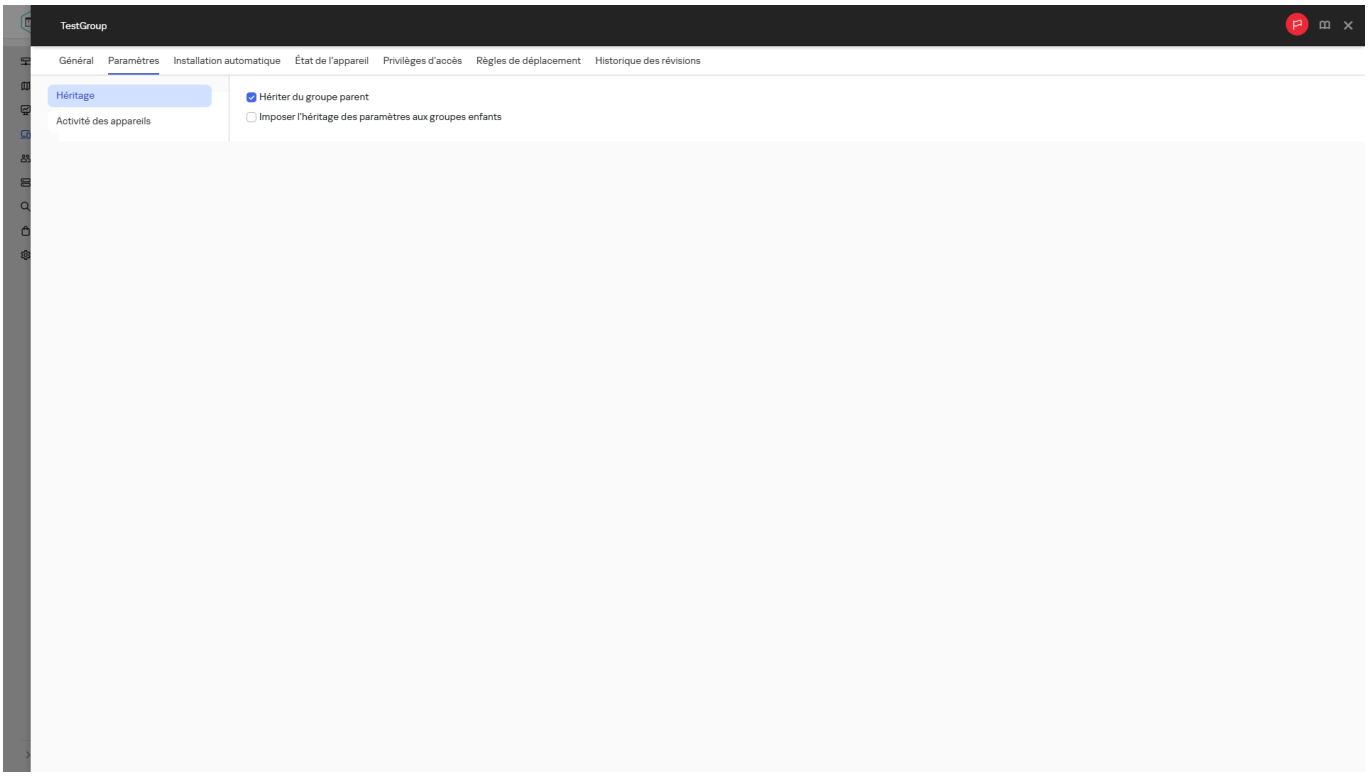
  Cette option est disponible uniquement si le groupe d'administration possède un groupe parent.

  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.



Propriétés des groupes d'administration

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)**

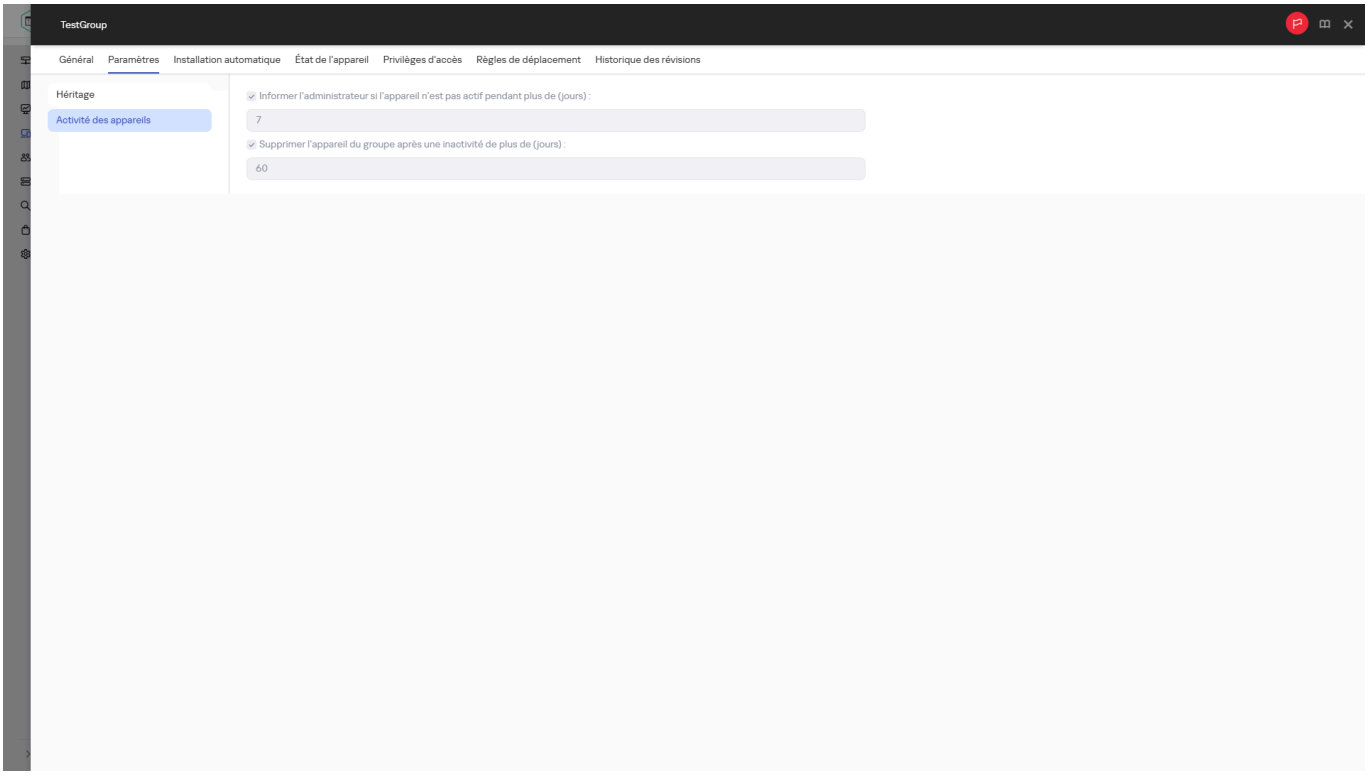
  Quand cette option est activée, l'administrateur reçoit des notifications sur les appareils inactifs. Vous pouvez définir la période à l'issue de laquelle l'événement **L'appareil est resté inactif sur le réseau depuis longtemps** est créé. Par défaut, la valeur de cet intervalle est de 7 jours.

  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.



Propriétés des groupes d'administration

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 **Gestion des ressources** → **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 **Gestion des ressources** → **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 ap&plications 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.

Accès à distance aux appareils administrés

Kaspersky Security Center Linux vous permet d'établir une connexion à distance aux appareils administrés. L'administrateur peut obtenir à l'appareil administré à l'aide de l'Agent d'administration installé sur l'appareil. La connexion à distance à l'appareil client à l'aide de l'Agent d'administration est même possible dans le cas si les ports TCP et UDP de l'appareil client ne sont pas accessibles. Après la connexion à l'appareil, l'administrateur obtient l'accès complet aux informations sur cet appareil et peut administrer les applications installées sur celui-ci.

Les méthodes d'établissement d'une connexion à distance dépendent de la plateforme utilisée sur l'appareil avec Kaspersky Security Center Web Console. Kaspersky Security Center Web Console peut être installé sur un appareil autre que le Serveur d'administration, sur un appareil Windows ou Linux.

Depuis la Kaspersky Security Center Web Console installée sur un appareil Linux, vous pouvez établir les connexions suivantes :

- Vers un appareil administré basé sur Linux en utilisant :
  - La connexion au bureau à distance (RDP).
  - Virtual Network Computing (VNC).
- Vers un appareil administré basé sur Windows en utilisant :
  - La connexion au bureau à distance (RDP).
  - Virtual Network Computing (VNC).

Depuis la Kaspersky Security Center Web Console installée sur un appareil Windows, vous pouvez établir les connexions suivantes :

- Vers un appareil administré basé sur Linux en utilisant :
  - La connexion au bureau à distance (RDP).
  - Virtual Network Computing (VNC).
- Vers un appareil administré basé sur Windows en utilisant :
  - La connexion au bureau à distance (RDP).
  - Partage du bureau Windows (WSD).

La connexion à distance aux appareils administrés n'est pas prise en charge lors de l'accès à Kaspersky Security Center Web Console depuis un appareil fonctionnant sous Microsoft Windows sur l'architecture ARM.

Pour établir une connexion à distance à un appareil, vous devez disposer des éléments suivants :

- utilitaire klsctunnel

  L'utilitaire Kaspersky est utilisé pour tunneliser la connexion entre un appareil administré et le Serveur d'administration.

  Kaspersky Security Center Linux permet d'établir des connexions TPC en tunnel depuis la Kaspersky Security Center Web Console via le Serveur d'administration et puis via l'Agent d'administration vers le port défini sur l'appareil administré. Le tunnel est utilisé pour connecter une application cliente qui se trouve sur un appareil doté de Kaspersky Security Center Web Console au port TCP sur l'appareil administré si la connexion directe de l'appareil avec Kaspersky Security Center Web Console et l'appareil n'est pas possible.

La connexion en tunnel de l'appareil client à distance avec le Serveur d'administration est nécessaire si le port de connexion au Serveur d'administration est inaccessible sur l'appareil. Le port sur l'appareil peut être inaccessible dans les cas suivants :

- L'appareil à distance est connecté au réseau local avec le mécanisme NAT utilisé.
- L'appareil à distance fait partie du réseau local du Serveur d'administration, mais son port est fermé par un pare-feu.

L'utilitaire peut être téléchargé lorsqu'une connexion à distance est établie via Kaspersky Security Center Web Console ou manuellement à partir du site Internet de Kaspersky.

L'utilitaire klsctunnel est installé sur l'appareil du Serveur d'administration et utilisé pour tous les types de connexions à distance (RDP, VNC, WDS).

- Client RDP ou VNC

  Le client RDP ou VNC est installé sur l'appareil du Serveur d'administration. Ce client vous permet d'obtenir un accès à distance à l'appareil administré en utilisant l'adresse et le port de la connexion locale fournis par l'utilitaire klsctunnel.

  La connexion RDP à la session en cours sur le poste de travail distant de l'utilisateur s'établit sans notification. Une fois l'administrateur connecté à la session, l'utilisateur de l'appareil sera déconnecté sans notification.

- Partage du bureau Windows (uniquement pour les appareils administrés sous Windows)

  Cette fonction vous permet de vous connecter à la session existante sur l'appareil client sans déconnecter l'utilisateur travaillant dans cette session. Dans ce cas, l'administrateur et l'utilisateur de la session sur l'appareil ont un accès collectif au bureau.

  Lors de la connexion à la séance existante du bureau à distance, l'utilisateur de cette séance sur l'appareil recevra une demande de connexion en provenance de l'administrateur. Les informations sur le processus de l'utilisation à distance de l'appareil et sur les résultats de cette utilisation ne sont pas conservées dans les rapports de Kaspersky Security Center Linux.

  L'administrateur peut configurer l'audit des actions sur l'appareil client distant. Lors de l'audit, l'application enregistre les informations relatives aux fichiers que l'administrateur a ouverts et/ou modifiés sur l'appareil client.

Accès à distance depuis un appareil Linux avec Kaspersky Security Center Web Console vers un appareil administré basé sur Linux

Prérequis

Avant de démarrer, assurez-vous que vous avez :

- Sur l'appareil administré tournant sous Linux, l'Agent d'administration version 15.3 ou ultérieure est installé.
- Sur l'appareil administré tournant sous Linux, le serveur RDP est installé (si vous vous connectez à l'appareil administré à l'aide de Connexion Bureau à distance).
- Sur l'appareil administré tournant sous Linux, le serveur VNC est installé (si vous vous connectez à l'appareil administré à l'aide de Virtual Network Computing).

- Le port pour le tunneling des connexions RDP est ouvert (l'option **Ouvrir le port pour tunnelliser les connexions RDP** est activée dans la section **Ports de connexion** de la fenêtre des propriétés du Serveur d'administration).

- L'administrateur dispose du droit **Démarrer des sessions RDP** pour établir des connexions RDP (si vous vous connectez à l'appareil administré à l'aide de la connexion Bureau à distance).

- L'administrateur a le droit **Lancer le tunneling** pour établir la connexion tunnel pour VNC (si vous vous connectez à l'appareil administré à l'aide de Virtual Network Computing).

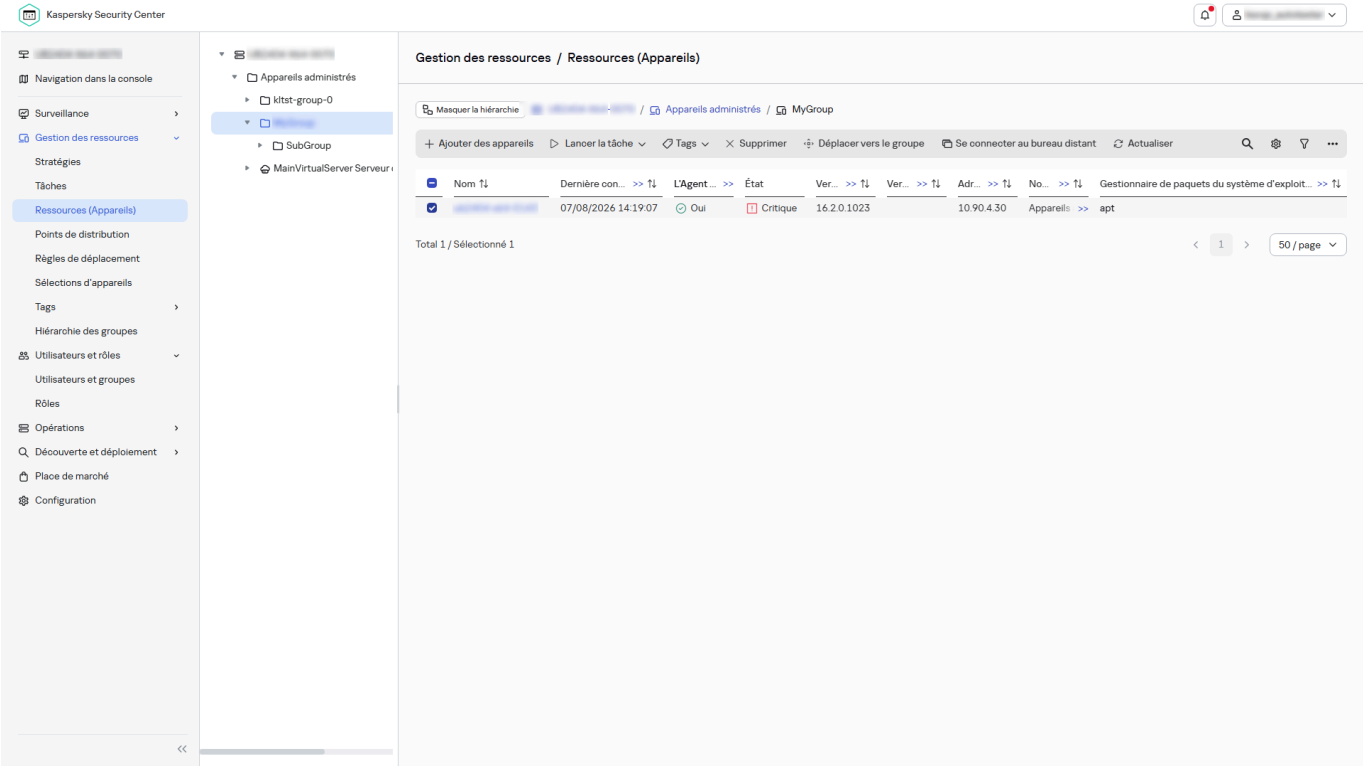
Pour vous connecter à un appareil administré basé sur Linux en utilisant RDP ou VNC via Kaspersky Security Center Web Console ouvert sur un appareil basé sur Linux, procédez comme suit :

1. Dans le menu principal, accédez à la section **Gestion des ressources** → **Ressources (Appareils)** ou ouvrez une sélection d'appareils.

2. Cochez la case en regard de l'appareil administré auquel vous souhaitez vous connecter à distance, puis cliquez sur le bouton **Se connecter au bureau distant**.

   La fenêtre **Se connecter au bureau distant** s'ouvre.

   Si vous sélectionnez plusieurs appareils, un appareil mobile ou un appareil exécutant macOS, le bouton **Se connecter au bureau distant** sera désactivé.



La liste des appareils administrés

3. Téléchargez l'utilitaire klsctunnel en cliquant sur le bouton **Télécharger**, puis exécutez-le.

Lors du téléchargement de l'utilitaire, tenez compte des éléments suivants :

- Pour obtenir une version à jour de l'utilitaire klsctunnel, assurez-vous que le Serveur d'administration a accès aux serveurs de mise à jour Kaspersky.

  Vous pouvez exécuter la tâche *Télécharger les mises à jour vers le Stockage du Serveur d'administration* et sélectionner les serveurs de mise à jour Kaspersky comme source de mises à jour. Si la tâche se termine correctement, le Serveur d'administration a accès aux serveurs de mise à jour Kaspersky.

- Si le fichier utilitaire n'est pas disponible au téléchargement, un message d'erreur s'affiche. Dans ce cas, téléchargez l'utilitaire manuellement, puis placez-le sur l'appareil du Serveur d'administration dans le répertoire /var/opt/kaspersky/klnagent_srv.

4. Dans la fenêtre **Se connecter au bureau distant**, spécifiez le port de connexion. Le numéro de port par défaut est 3389.

5. Générez un blob de texte avec des paramètres de connexion codés en cliquant sur le bouton **Générer un blob**, puis copiez et collez le texte dans le champ correspondant de l'utilitaire klsctunnel.

   Un blob contient les paramètres requis pour établir une connexion entre le Serveur d'administration et l'appareil administré. Un blob est valide pendant 3 minutes. Si celui-ci a expiré, générez-en un nouveau.

6. Dans l'utilitaire klsctunnel, si vous utilisez un serveur proxy, spécifiez les paramètres de connexion au serveur proxy.

   L'utilitaire klsctunnel affiche l'adresse et le port de la connexion locale d'un client d'accès à distance.

   L'utilitaire permet à l'administrateur de fermer la connexion au tunnel. Si la connexion au tunnel est fermée, la connexion actuelle au bureau à distance est interrompue.

7. Exécutez un client d'accès à distance (RDP ou VNC) et connectez-le à l'appareil administré à l'aide de l'adresse et du port fournis par l'utilitaire klsctunnel.

La connexion avec l'appareil administré est établie. Le bureau est disponible dans la fenêtre du client d'accès à distance.

Accès à distance depuis un appareil Linux avec Kaspersky Security Center Web Console vers un appareil administré basé sur Windows

La connexion au bureau à distance (RDP).

Prérequis

Avant de démarrer, assurez-vous que vous avez :

- Une connexion à distance est autorisée dans les paramètres du système d'exploitation de l'appareil administré.

- Sur l'appareil administré tournant sous Windows, l'Agent d'administration version 13.0 ou ultérieure est installé.

- L'administrateur dispose du droit **Démarrer des sessions RDP** pour établir des connexions RDP.

- Le port pour le tunneling des connexions RDP est ouvert (l'option **Ouvrir le port pour tunnelliser les connexions RDP** est activée dans la section **Ports de connexion** de la fenêtre des propriétés du Serveur d'administration).

Pour vous connecter à un appareil administré basé sur Windows en utilisant RDP via Kaspersky Security Center Web Console ouvert sur un appareil basé sur Linux, procédez comme suit :

1. Dans le menu principal, accédez à la section **Gestion des ressources** → **Ressources (Appareils)** ou ouvrez une sélection d'appareils.

2. Cochez la case en regard de l'appareil administré auquel vous souhaitez vous connecter à distance, puis cliquez sur le bouton **Se connecter au bureau distant**.

   La fenêtre **Se connecter au bureau distant** s'ouvre.

   Si vous sélectionnez plusieurs appareils, un appareil mobile ou un appareil exécutant macOS, le bouton **Se connecter au bureau distant** sera désactivé.

3. Dans la fenêtre **Se connecter au bureau distant**, sélectionnez le type de connexion **RDP**.

4. Si une connexion à distance n'est pas autorisée dans les paramètres du système d'exploitation de l'appareil administré, autorisez la connexion à distance de manière centralisée en cliquant sur le bouton **Modifier les paramètres**.

   Si les paramètres sont appliqués correctement, une notification s'affiche. De plus, sur l'appareil administré, dans la section **Paramètres** → **Système** → **Bureau à distance**, l'option **Activer le Bureau à distance** est activée.

   Si la connexion à distance est autorisée dans les paramètres du système d'exploitation de l'appareil administré, le bouton **Modifier les paramètres** ne s'affiche pas.

5. Téléchargez l'utilitaire klsctunnel en cliquant sur le bouton **Télécharger**, puis exécutez-le.

   Lors du téléchargement de l'utilitaire, tenez compte des éléments suivants :

   - Pour obtenir une version à jour de l'utilitaire klsctunnel, assurez-vous que le Serveur d'administration a accès aux serveurs de mise à jour Kaspersky.

     Vous pouvez exécuter la tâche *Télécharger les mises à jour vers le Stockage du Serveur d'administration* et sélectionner les serveurs de mise à jour Kaspersky comme source de mises à jour. Si la tâche se termine correctement, le Serveur d'administration a accès aux serveurs de mise à jour Kaspersky.

   - Si le fichier utilitaire n'est pas disponible au téléchargement, un message d'erreur s'affiche. Dans ce cas, téléchargez l'utilitaire manuellement, puis placez-le sur l'appareil du Serveur d'administration dans le répertoire /var/opt/kaspersky/klnagent_srv.

6. Générez un blob de texte avec des paramètres de connexion codés en cliquant sur le bouton **Générer un blob**, puis copiez et collez le texte dans le champ correspondant de l'utilitaire klsctunnel.

   Un blob contient les paramètres requis pour établir une connexion entre le Serveur d'administration et l'appareil administré. Un blob est valide pendant 3 minutes. Si celui-ci a expiré, générez-en un nouveau.

7. Dans l'utilitaire klsctunnel, si vous utilisez un serveur proxy, spécifiez les paramètres de connexion au serveur proxy.

   L'utilitaire klsctunnel affiche l'adresse et le port de la connexion à l'appareil distant.

L'utilitaire permet à l'administrateur de fermer la connexion au tunnel. Si la connexion au tunnel est fermée, la connexion actuelle au bureau à distance est interrompue.

8. Exécutez un client RDP et connectez-le à l'appareil administré à l'aide de l'adresse et du port fournis par l'utilitaire klsctunnel.

La connexion à l'appareil administré est établie. Le bureau est accessible dans la fenêtre du client RDP.

La connexion à la session en cours sur le poste de travail distant de l'utilisateur s'établit sans notification. Une fois l'administrateur connecté à la session, l'utilisateur de l'appareil sera déconnecté sans notification.

Virtual Network Computing system (VNC)

Prérequis

Avant de démarrer, assurez-vous que vous avez :

- Sur l'appareil administré tournant sous Windows, l'Agent d'administration version 13.0 ou ultérieure est installé.
- Le serveur VNC est installé sur l'appareil administré exécutant Windows.
- L'administrateur dispose du droit **Lancer le tunneling** pour établir la connexion tunnel pour VNC.
- Le port pour le tunneling des connexions RDP est ouvert (l'option **Ouvrir le port pour tunnelliser les connexions RDP** est activée dans la section **Ports de connexion** de la fenêtre des propriétés du Serveur d'administration).

Pour vous connecter à un appareil administré basé sur Windows en utilisant VNC via Kaspersky Security Center Web Console ouvert sur un appareil basé sur Linux, procédez comme suit :

1. Dans le menu principal, accédez à la section **Gestion des ressources** → **Ressources (Appareils)** ou ouvrez une sélection d'appareils.
2. Cochez la case en regard de l'appareil administré auquel vous souhaitez vous connecter à distance, puis cliquez sur le bouton **Se connecter au bureau distant**.

   La fenêtre **Se connecter au bureau distant** s'ouvre.

   Si vous sélectionnez plusieurs appareils, un appareil mobile ou un appareil exécutant macOS, le bouton **Se connecter au bureau distant** sera désactivé.
3. Dans la fenêtre **Se connecter au bureau distant**, sélectionnez le type de connexion **VNC**.
4. Téléchargez l'utilitaire klsctunnel en cliquant sur le bouton **Télécharger**, puis exécutez-le.

   Si le fichier utilitaire n'est pas disponible au téléchargement, un message d'erreur s'affiche. Dans ce cas, téléchargez l'utilitaire manuellement.
5. Dans la fenêtre **Se connecter au bureau distant**, spécifiez le port de connexion VNC. Le numéro de port par défaut est 5900.

6. Générez un blob de texte avec des paramètres de connexion codés en cliquant sur le bouton **Générer un blob**, puis copiez et collez le texte dans le champ correspondant de l'utilitaire klsctunnel.

   Un blob contient les paramètres requis pour établir une connexion entre le Serveur d'administration et l'appareil administré. Un blob est valide pendant 3 minutes. Si celui-ci a expiré, générez-en un nouveau.

7. Dans l'utilitaire klsctunnel, si vous utilisez un serveur proxy, spécifiez les paramètres de connexion au serveur proxy.

   L'utilitaire klsctunnel affiche l'adresse et le port de la connexion locale du client VNC.

   L'utilitaire permet à l'utilisateur distant de fermer la connexion au tunnel. Si la connexion au tunnel est fermée, la connexion actuelle au bureau à distance est interrompue.

8. Exécutez un client VNC et connectez-le à l'appareil administré à l'aide de l'adresse et du port fournis par l'utilitaire klsctunnel.

La connexion à l'appareil administré est établie. Le bureau est accessible dans la fenêtre du client VNC.

Accès à distance depuis un appareil Windows avec Kaspersky Security Center Web Console vers un appareil administré basé sur Linux

La connexion au bureau à distance (RDP).

Prérequis

Avant de démarrer, assurez-vous que vous avez :

- Le serveur RDP est installé sur l'appareil administré exécutant Linux.
- Sur l'appareil administré tournant sous Linux, l'Agent d'administration version 15.3 ou ultérieure est installé.
- L'administrateur dispose du droit **Démarrer des sessions RDP** pour établir des connexions RDP.
- Le port pour le tunneling des connexions RDP est ouvert (l'option **Ouvrir le port pour tunnelliser les connexions RDP** est activée dans la section **Ports de connexion** de la fenêtre des propriétés du Serveur d'administration).

Pour vous connecter à un appareil administré basé sur Linux en utilisant RDP via Kaspersky Security Center Web Console ouvert sur un appareil basé sur Windows, procédez comme suit :

1. Dans le menu principal, accédez à la section **Gestion des ressources** → **Ressources (Appareils)** ou ouvrez une sélection d'appareils.

2. Cochez la case en regard de l'appareil administré auquel vous souhaitez vous connecter à distance, puis cliquez sur le bouton **Se connecter au bureau distant**.

   La fenêtre **Se connecter au bureau distant** s'ouvre.

   Si vous sélectionnez plusieurs appareils, un appareil mobile ou un appareil exécutant macOS, le bouton **Se connecter au bureau distant** sera désactivé.

3. Dans la fenêtre **Se connecter au bureau distant**, sélectionnez le type de connexion **RDP**.

4. Téléchargez l'utilitaire klsctunnel en cliquant sur le bouton **Télécharger**, puis exécutez-le.

   Lors du téléchargement de l'utilitaire, tenez compte des éléments suivants :

   - Pour obtenir une version à jour de l'utilitaire klsctunnel, assurez-vous que le Serveur d'administration a accès aux serveurs de mise à jour Kaspersky.

     Vous pouvez exécuter la tâche *Télécharger les mises à jour vers le Stockage du Serveur d'administration* et sélectionner les serveurs de mise à jour Kaspersky comme source de mises à jour. Si la tâche se termine correctement, le Serveur d'administration a accès aux serveurs de mise à jour Kaspersky.

   - Si le fichier utilitaire n'est pas disponible au téléchargement, un message d'erreur s'affiche. Dans ce cas, téléchargez l'utilitaire manuellement, puis placez-le sur l'appareil du Serveur d'administration dans le répertoire /var/opt/kaspersky/klnagent_srv.

5. Générez un blob de texte avec des paramètres de connexion codés en cliquant sur le bouton **Générer un blob**, puis copiez et collez le texte dans le champ correspondant de l'utilitaire klsctunnel.

   Un blob contient les paramètres requis pour établir une connexion entre le Serveur d'administration et l'appareil administré. Un blob est valide pendant 3 minutes. Si celui-ci a expiré, générez-en un nouveau.

6. Dans l'utilitaire klsctunnel, si vous utilisez un serveur proxy, spécifiez les paramètres de connexion au serveur proxy.

   Pour ce faire, cochez la case **Utiliser un serveur proxy**, puis spécifiez les paramètres de connexion.

7. Cliquez sur **Ouvrir le port**.

   La fenêtre Connexion Bureau à distance s'ouvre.

8. Indiquez les informations d'identification du compte à partir duquel vous êtes actuellement connecté à Kaspersky Security Center Web Console, puis connectez-vous à l'appareil administré.

   L'utilitaire klsctunnel affiche l'adresse et le port de la connexion à l'appareil distant.

   L'utilitaire permet à l'administrateur de fermer la connexion au tunnel. Si la connexion au tunnel est fermée, la connexion actuelle au bureau à distance est interrompue.

Lorsque la connexion à l'appareil client est établie, le bureau de l'appareil client est accessible dans la fenêtre Connexion Bureau à distance de Microsoft Windows.

La connexion à la session en cours sur le poste de travail distant de l'utilisateur s'établit sans notification. Une fois l'administrateur connecté à la session, l'utilisateur de l'appareil sera déconnecté sans notification.

Virtual Network Computing system (VNC)

Prérequis

Avant de démarrer, assurez-vous que vous avez :

- Sur l'appareil administré tournant sous Linux, l'Agent d'administration version 15.3 ou ultérieure est installé.

- Le serveur VNC est installé sur l'appareil administré exécutant Linux.

- L'administrateur dispose du droit **Lancer le tunneling** pour établir la connexion tunnel pour VNC.

- Le port pour le tunneling des connexions RDP est ouvert (l'option **Ouvrir le port pour tunnelliser les connexions RDP** est activée dans la section **Ports de connexion** de la fenêtre des propriétés du Serveur d'administration).

Pour vous connecter à un appareil administré basé sur Linux en utilisant VNC via Kaspersky Security Center Web Console ouvert sur un appareil basé sur Windows, procédez comme suit :

1. Dans le menu principal, accédez à la section **Gestion des ressources** → **Ressources (Appareils)** ou ouvrez une sélection d'appareils.

2. Cochez la case en regard de l'appareil administré auquel vous souhaitez vous connecter à distance, puis cliquez sur le bouton **Se connecter au bureau distant**.

   La fenêtre **Se connecter au bureau distant** s'ouvre.

   Si vous sélectionnez plusieurs appareils, un appareil mobile ou un appareil exécutant macOS, le bouton **Se connecter au bureau distant** sera désactivé.

3. Dans la fenêtre **Se connecter au bureau distant**, sélectionnez le type de connexion **VNC**.

4. Téléchargez l'utilitaire klsctunnel en cliquant sur le bouton **Télécharger**, puis exécutez-le.

   Si le fichier utilitaire n'est pas disponible au téléchargement, un message d'erreur s'affiche. Dans ce cas, téléchargez l'utilitaire manuellement.

5. Dans la fenêtre **Se connecter au bureau distant**, spécifiez le port de connexion VNC. Le numéro de port par défaut est 5900.

6. Générez un blob de texte avec des paramètres de connexion codés en cliquant sur le bouton **Générer un blob**, puis copiez et collez le texte dans le champ correspondant de l'utilitaire klsctunnel.

   Un blob contient les paramètres requis pour établir une connexion entre le Serveur d'administration et l'appareil administré. Un blob est valide pendant 3 minutes. Si celui-ci a expiré, générez-en un nouveau.

7. Dans l'utilitaire klsctunnel, si vous utilisez un serveur proxy, spécifiez les paramètres de connexion au serveur proxy.

   Pour ce faire, cochez la case **Utiliser un serveur proxy**, puis spécifiez les paramètres de connexion.

8. Cliquez sur **Ouvrir le port**.

   L'utilitaire klsctunnel affiche l'adresse et le port de la connexion locale du client VNC.

   L'utilitaire permet à l'utilisateur distant de fermer la connexion au tunnel. Si la connexion au tunnel est fermée, la connexion actuelle au bureau à distance est interrompue.

9. Exécutez un client VNC et connectez-le à l'appareil administré à l'aide de l'adresse et du port fournis par l'utilitaire klsctunnel.

La connexion à l'appareil administré est établie. Le bureau est accessible dans la fenêtre du client VNC.

Accès à distance depuis un appareil Windows avec Kaspersky Security Center Web Console vers un appareil administré basé sur Windows

La connexion au bureau à distance (RDP).

Prérequis

Avant de démarrer, assurez-vous que vous avez :

- Sur l'appareil administré tournant sous Windows, l'Agent d'administration version 13.0 ou ultérieure est installé.
- L'administrateur dispose du droit **Démarrer des sessions RDP** pour établir des connexions RDP.
- Le port pour le tunneling des connexions RDP est ouvert (l'option **Ouvrir le port pour tunnelliser les connexions RDP** est activée dans la section **Ports de connexion** de la fenêtre des propriétés du Serveur d'administration).
- Une connexion à distance est autorisée dans les paramètres du système d'exploitation de l'appareil administré.

Pour vous connecter à un appareil administré basé sur Windows en utilisant RDP via Kaspersky Security Center Web Console ouvert sur un appareil basé sur Windows, procédez comme suit :

1. Dans le menu principal, accédez à la section **Gestion des ressources** → **Ressources (Appareils)** ou ouvrez une sélection d'appareils.
2. Cochez la case en regard de l'appareil administré auquel vous souhaitez vous connecter à distance, puis cliquez sur le bouton **Se connecter au bureau distant**.

   La fenêtre **Se connecter au bureau distant** s'ouvre.

   Si vous sélectionnez plusieurs appareils, un appareil mobile ou un appareil exécutant macOS, le bouton **Se connecter au bureau distant** sera désactivé.
3. Dans la fenêtre **Se connecter au bureau distant**, sélectionnez le type de connexion **Connexion bureau distant**.
4. Si une connexion à distance n'est pas autorisée dans les paramètres du système d'exploitation de l'appareil administré, autorisez la connexion à distance de manière centralisée en cliquant sur le bouton **Modifier les paramètres**.

   Si les paramètres sont appliqués correctement, une notification s'affiche. De plus, sur l'appareil administré, dans la section **Paramètres** → **Système** → **Bureau à distance**, l'option **Activer le Bureau à distance** est activée.

   Si la connexion à distance est autorisée dans les paramètres du système d'exploitation de l'appareil administré, le bouton **Modifier les paramètres** ne s'affiche pas.
5. Téléchargez l'utilitaire klsctunnel en cliquant sur le bouton **Télécharger**, puis exécutez-le.

Lors du téléchargement de l'utilitaire, tenez compte des éléments suivants :

- Pour obtenir une version à jour de l'utilitaire klsctunnel, assurez-vous que le Serveur d'administration a accès aux serveurs de mise à jour Kaspersky.

  Vous pouvez exécuter la tâche *Télécharger les mises à jour vers le Stockage du Serveur d'administration* et sélectionner les serveurs de mise à jour Kaspersky comme source de mises à jour. Si la tâche se termine correctement, le Serveur d'administration a accès aux serveurs de mise à jour Kaspersky.

- Si le fichier utilitaire n'est pas disponible au téléchargement, un message d'erreur s'affiche. Dans ce cas, téléchargez l'utilitaire manuellement, puis placez-le sur l'appareil du Serveur d'administration dans le répertoire /var/opt/kaspersky/klnagent_srv.

6. Générez un blob de texte avec des paramètres de connexion codés en cliquant sur le bouton **Générer un blob**, puis copiez et collez le texte dans le champ correspondant de l'utilitaire klsctunnel.

   Un blob contient les paramètres requis pour établir une connexion entre le Serveur d'administration et l'appareil administré. Un blob est valide pendant 3 minutes. Si celui-ci a expiré, générez-en un nouveau.

7. Dans l'utilitaire klsctunnel, si vous utilisez un serveur proxy, spécifiez les paramètres de connexion au serveur proxy.

   Pour ce faire, cochez la case **Utiliser un serveur proxy**, puis spécifiez les paramètres de connexion.

8. Cliquez sur **Ouvrir le port**.

   La fenêtre Connexion Bureau à distance s'ouvre.

9. Indiquez les informations d'identification du compte à partir duquel vous êtes actuellement connecté à Kaspersky Security Center Web Console, puis connectez-vous à l'appareil administré.

   L'utilitaire klsctunnel affiche l'adresse et le port de la connexion à l'appareil distant.

   L'utilitaire permet à l'administrateur de fermer la connexion au tunnel. Si la connexion au tunnel est fermée, la connexion actuelle au bureau à distance est interrompue.

Lorsque la connexion à l'appareil client est établie, le bureau de l'appareil client est accessible dans la fenêtre Connexion Bureau à distance de Microsoft Windows.

La connexion à la session en cours sur le poste de travail distant de l'utilisateur s'établit sans notification. Une fois l'administrateur connecté à la session, l'utilisateur de l'appareil sera déconnecté sans notification.

Partage du bureau Windows (WSD).

Prérequis

Avant de démarrer, assurez-vous que vous avez :

- Sur l'appareil administré tournant sous Windows, l'Agent d'administration version 13.0 ou ultérieure est installé.
- L'administrateur dispose du droit **Se Connecter aux sessions RDP existantes** pour établir la connexion WDS.
- La licence de Gestion des vulnérabilités et des correctifs est disponible.

- Microsoft Windows Vista ou une version plus récente est installée sur le poste de travail de l'administrateur. Le type du système d'exploitation de l'appareil hébergeant le Serveur d'administration ne représente pas une restriction pour la connexion à l'aide de Partage du bureau Windows.

  Vérifiez si la fonctionnalité de partage de bureau Windows est incluse dans votre édition Windows et assurez-vous qu'il existe une clé CLSID\{32BE5ED2-5C86-480F-A914-0FF8885A1B3F} dans le registre Windows.

- Microsoft Windows Vista ou une version plus récente est installée sur l'appareil client.

Pour vous connecter à un appareil administré basé sur Windows en utilisant VNC via Kaspersky Security Center Web Console ouvert sur un appareil basé sur Windows, procédez comme suit :

1. Dans le menu principal, accédez à la section **Gestion des ressources** → **Ressources (Appareils)** ou ouvrez une sélection d'appareils.

2. Cochez la case en regard de l'appareil administré auquel vous souhaitez vous connecter à distance, puis cliquez sur le bouton **Se connecter au bureau distant**.

   La fenêtre **Se connecter au bureau distant** s'ouvre.

   Si vous sélectionnez plusieurs appareils, un appareil mobile ou un appareil exécutant macOS, le bouton **Se connecter au bureau distant** sera désactivé.

3. Dans la fenêtre **Se connecter au bureau distant**, sélectionnez le type de connexion **Partage du bureau Windows**.

   Si la licence Gestion des vulnérabilités et des correctifs n'est pas disponible, un message d'erreur s'affiche.

4. Téléchargez l'utilitaire klsctunnel en cliquant sur le bouton **Télécharger**, puis exécutez-le.

   Si le fichier utilitaire n'est pas disponible au téléchargement, un message d'erreur s'affiche. Dans ce cas, téléchargez l'utilitaire manuellement.

5. Dans la liste des sessions utilisateur disponibles et actives sur l'appareil sélectionné, sélectionnez la session à laquelle vous souhaitez vous connecter.

   L'utilisateur distant doit autoriser la connexion. Si l'utilisateur distant refuse de se connecter ou s'il n'autorise pas la connexion pendant le délai d'expiration, un message d'erreur s'affiche.

6. Générez un blob de texte avec des paramètres de connexion codés en cliquant sur le bouton **Générer un blob**, puis copiez et collez le texte dans le champ correspondant de l'utilitaire klsctunnel.

   Un blob contient les paramètres requis pour établir une connexion entre le Serveur d'administration et l'appareil administré. Un blob est valide pendant 3 minutes. Si celui-ci a expiré, générez-en un nouveau.

7. Dans l'utilitaire klsctunnel, si vous utilisez un serveur proxy, spécifiez les paramètres de connexion au serveur proxy.

   Pour ce faire, cochez la case **Utiliser un serveur proxy**, puis spécifiez les paramètres de connexion.

8. Cliquez sur **Ouvrir le port**.

   L'utilitaire klsctunnel affiche l'adresse et le port de la connexion locale du client VNC.

   L'utilitaire permet à l'utilisateur distant de fermer la connexion au tunnel. Si la connexion au tunnel est fermée, la connexion actuelle au bureau à distance est interrompue.

Le partage du bureau démarre dans une nouvelle fenêtre. Si vous souhaitez interagir avec l'appareil, cliquez sur l'icône du menu ( ) dans le coin supérieur gauche de la fenêtre, puis sélectionnez **Mode interactif**.

Administration des appareils mobiles

L'administration de la protection des appareils mobiles via la Kaspersky Security Center est confiée à la Fonction Administration des appareils mobiles. Vous devez ajouter une clé de licence sur chaque appareil mobile pour activer l'application de protection. Si vous avez l'intention d'administrer les appareils mobiles qui appartiennent aux employés de votre organisation, activez et configurez l'Administration des appareils mobiles.

L'administration des appareils mobiles vous permet d'administrer les appareils Android et iOS des employés. La protection est assurée par l'application Kaspersky Endpoint Security for Android et le système d'administration des appareils iOS installés sur les appareils mobiles. Ces applications mobiles assurent la protection des appareils mobiles contre les menaces Web, les virus et les autres programmes qui présentent des menaces. Pour assurer une administration centralisée via Kaspersky Security Center Web Console, vous devez installer les plug-ins d'administration Web suivants sur l'appareil sur lequel Kaspersky Security Center Web Console est installé :

- Kaspersky Mobile Devices Protection and Management

  Le plug-in Kaspersky Mobile Devices Protection and Management permet d'administrer les appareils fonctionnant sous Android et iOS dans Kaspersky Security Center Web Console.

- Paramètres du serveur MDM iOS

  Le plug-in de paramétrage du serveur MDM iOS vous permet de configurer les paramètres du serveur MDM iOS utilisé pour connecter les appareils iOS au Serveur d'administration et gérer les appareils iOS.

Pour obtenir plus d'informations sur le déploiement de la protection et l'administration des appareils mobiles, consultez l'aide de Kaspersky Security for Mobile et l'aide de Kaspersky Secure Mobility Management.

Utilisation de Firebase Cloud Messaging

Pour garantir la diffusion en temps opportun des commandes aux appareils Android, Kaspersky Security Center Linux utilise le mécanisme des notifications push. Les notifications push entre les appareils Android et le Serveur d'administration sont échangées à l'aide de Firebase Cloud Messaging (ci-après dénommé FCM). Kaspersky Security Center Linux Web Console permet d'indiquer les paramètres du service Firebase Cloud Messaging pour connecter les appareils Android à ce service.

Pour obtenir les paramètres de Firebase Cloud Messaging, vous devez avoir un compte utilisateur Google.

Pour activer FCM, procédez comme suit :

1. Dans la fenêtre principale de Kaspersky Security Center Web Console, sélectionnez **Gestion des ressources** → **Mobile** → **Devices**.

2. Ouvrez le menu à trois points (⋮) et sélectionnez **Forced Android device synchronization**.

3. Dans le champ **Firebase project number**, indiquez l'identificateur de l'expéditeur de FCM.

4. Dans le champ **Private key**, sélectionnez le fichier de clé privée.

   Lors de la synchronisation suivantes avec le Serveur d'administration, les appareils Android seront connectés au service Firebase Cloud Messaging.

Lorsque vous passez à un autre projet Firebase, vous devez attendre 10 minutes que FCM reprenne.

Le service FCM fonctionne sur les plages d'adresses suivantes :

- Du côté de l'appareil Android, il faut octroyer l'accès aux ports 443 (HTTPS), 5228 (HTTPS), 5229 (HTTPS), 5230 (HTTPS) des adresses suivantes :
  - google.com
  - fcm.googleapis.com
  - oauth2.googleapis.com
  - android.apis.google.com
  - ou sur toutes les adresses IP de la liste " Google ASN 15169 "
- Du côté du Serveur d'administration, il faut octroyer l'accès sur le port 443 (HTTPS) des adresses suivantes :
  - fcm.googleapis.com
  - ou sur toutes les adresses IP de la liste " Google ASN 15169 "

Si les paramètres du serveur proxy ont été définis dans les propriétés du Serveur d'administration de Kaspersky Security Center Web Console, ils seront utilisés pour l'interaction avec FCM.

Configuration de FCM : obtention de l'identificateur de l'expéditeur et du fichier de clé privée

Pour configurer FCM, procédez comme suit :

1. S'inscrire sur le portail Google.
2. Accéder à la console Firebase.
3. Exécutez une des actions suivantes :
   - Pour créer un projet, cliquez sur **Créer un projet** et suivez les instructions à l'écran.
   - Ouvrez un projet existant.
4. Cliquez sur l'icône en forme d'engrenage et choisissez **Paramètres du projet**.

   La fenêtre **Paramètres du projet** s'ouvre.

5. Sélectionnez l'onglet **Messagerie Cloud**.

6. Récupérez l'identificateur de l'expéditeur dans le champ **Identificateur de l'expéditeur** dans la section **API de Firebase Cloud Messaging (V1)**.

7. Sélectionnez l'onglet **Comptes de services** et cliquez sur **Générer une nouvelle clé privée**.

8. Dans la fenêtre qui s'ouvre, cliquez sur **Générer une clé** pour générer et télécharger un fichier de clé privée.

Firebase Cloud Messaging est maintenant configuré.

Intégration avec l'infrastructure à clé publique

Vous pouvez intégrer l'émission de certificats avec l'autorité de certification (AC) de Microsoft via l'infrastructure à clé publique (ICP). L'intégration à l'ICP est destinée à simplifier l'émission de certificats d'utilisateur de domaine par le Serveur d'administration. Suite à cette intégration, l'émission des certificats est automatique.

Pour obtenir des informations détaillées sur la configuration de l'intégration à l'ICP pour l'émission des certificats, consultez l'aide de Kaspersky Secure Mobility Management.

Vous pouvez effectuer l'intégration de l'ICP avec des paramètres particuliers et assigner à l'ICP le rôle de source de certificats pour des types particuliers de certificats. Les paramètres d'intégration de l'ICP vous permettent de définir le modèle individuel par défaut pour tous les types de certificats.

Les particularités de l'utilisation de l'intégration de l'ICP pour l'émission de certificats :

- L'intégration de l'ICP est désactivée par défaut. Pour en savoir plus sur l'activation de l'ICP et la configuration de ses paramètres, consultez l'aide de Kaspersky Secure Mobility Management.

- Les certificats sont émis à l'aide de l'Agent d'administration pour Windows. Cela assure l'intégration entre le Serveur d'administration et l'autorité de certification de Microsoft. Étant donné que plusieurs appareils peuvent être installés avec l'Agent d'administration, vous pouvez préciser l'appareil qui se connectera à l'autorité de certification de Microsoft dans les **Issuance rules**. Cet appareil doit disposer d'un certificat de l'Agent d'enregistrement (EA) installé dans le stockage de certificats du compte à partir duquel l'intégration à l'ICP est effectuée. Le certificat est émis par l'administrateur de l'autorité de certification du domaine.

- Le compte à partir duquel l'intégration à l'ICP est effectuée doit être un utilisateur du domaine et disposer des droits de *connexion en tant que service*.

- Kaspersky Security Center Linux ne peut fonctionner qu'avec une seule intégration d'ICP (CA Microsoft) à la fois.

Administration des groupes d'administration

Cette section contient les informations sur le travail avec les groupes d'administration.

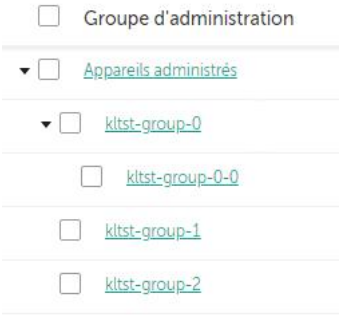
Avec les groupes d'administration, vous pouvez effectuer les actions suivantes :

- 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).

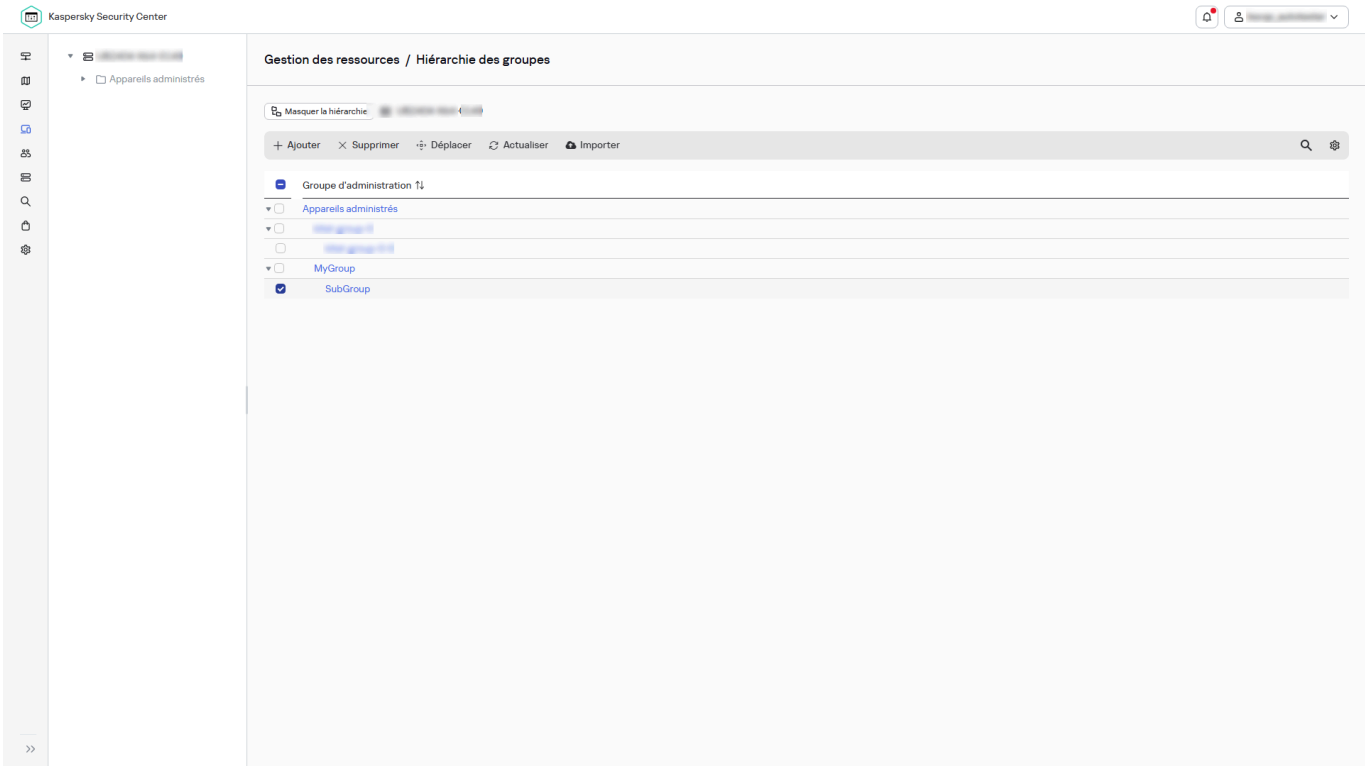


Consultation des hiérarchies des groupes d'administration

Pour créer un groupe d'administration, procédez comme suit :

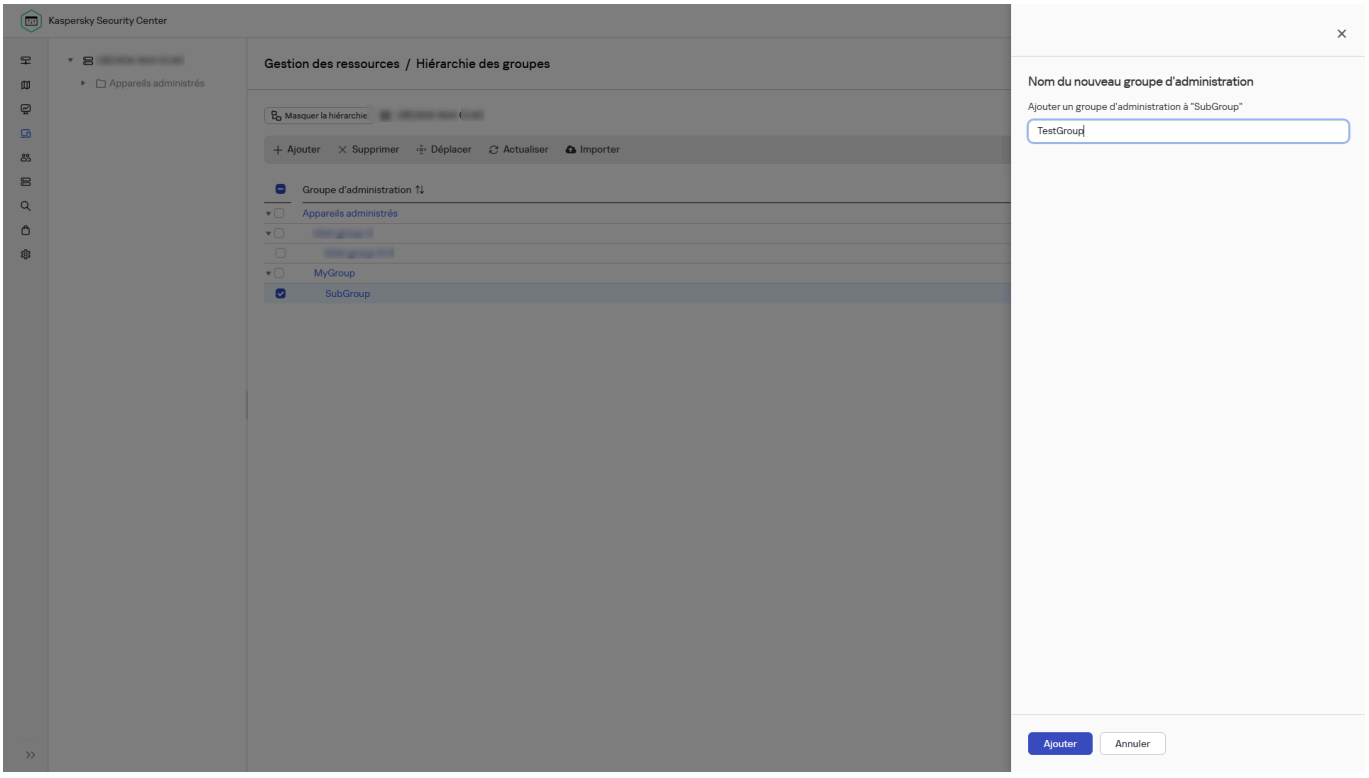
1. Dans le menu principal, accédez à **Gestion des ressources** → **Hiérarchie des groupes**.

2. Dans la structure du groupe d'administration, sélectionnez le groupe d'administration qui doit inclure le nouveau groupe d'administration.



3. Cliquez sur **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 **Gestion des ressources** → **Hiérarchie des groupes**.

2. Cliquez sur **Importer**.

   Finalement, l'Assistant de création de la structure des groupes d'administration se lance. Suivez les étapes 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 **Gestion des ressources** → **Hiérarchie des groupes**.

2. Accédez aux propriétés du groupe d'administration requis de l'une des manières suivantes :

   - Cliquez sur le nom du groupe d'administration.

   - Cliquez sur le bouton **Afficher la hiérarchie** en haut de la page. Dans le panneau de navigation qui s'ouvre, placez le curseur de la souris sur le nom du groupe requis, puis cliquez sur l'icône des paramètres (⚙).

   La fenêtre des propriétés du groupe d'administration s'ouvre.

3. Dans la fenêtre des propriétés, sélectionnez l'onglet **Installation automatique**.

4. 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 **Gestion des ressources** → **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 **Gestion des ressources** → **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.

Si vous souhaitez installer l'Agent d'administration sur des appareils qui utilisent le système d'exploitation RED OS 7.3.4 ou une version ultérieure ou MSVSPHERE 9.2 ou une version ultérieure, installez le paquet libxcrypt-compat pour assurer le bon fonctionnement de l'Agent d'administration.

4. **Création et configuration 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 de stratégie par défaut. Vous pouvez également modifier les paramètres par défaut de la stratégie à tout moment selon vos besoins.

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 :

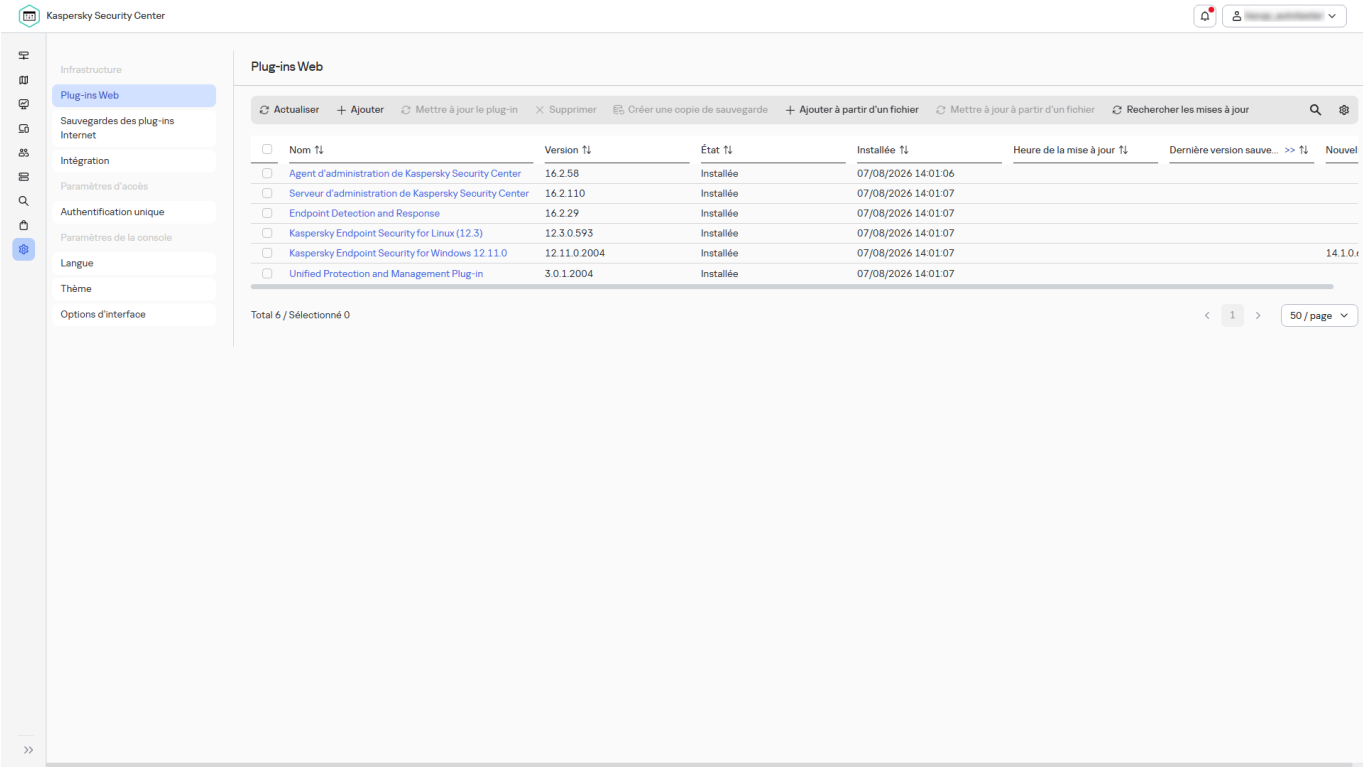
- Toutes les stratégies et les tâches requises pour les applications sont créées.
- Les programmes de tâches sont configurés en fonction de vos besoins.
- Les applications sélectionnées sont déployé ou son déploiement est programmé sur les appareils clients sélectionnés.

Obtention des plug-ins d'administration pour les applications de Kaspersky

Pour déployer une application Kaspersky, par exemple Kaspersky Endpoint Security for Linux ou Kaspersky Endpoint Security for Windows, vous devez ajouter et installer le plug-in Internet 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**.



La liste des plug-ins Internet installés

2. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Ajouter**.

   Une liste des plug-ins disponibles s'affiche.

3. Dans la liste des plug-ins disponibles, sélectionnez le plug-in que vous souhaitez télécharger (par exemple, Kaspersky Endpoint Security 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.

Paquets

Le paquet d'installation est un ensemble de fichiers créés pour l'installation à distance d'une application Kaspersky. 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.

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.

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.

Lors de la création de paquets d'installation pour installer l'application sur des appareils Windows, si vous recevez le message **Une erreur s'est produite. Veuillez réessayer le téléchargement** :

1. Créez l'indicateur RIUtilsArchiveDirUsed en exécutant la commande suivante :

   ```
   /opt/kaspersky/ksc64/sbin/klscflag -fset -pv klserver -n RIUtilsArchiveDirUsed -t d -v 1
   ```

2. Exécutez la commande suivante pour redémarrer le service du Serveur d'administration :

   ```
   systemctl restart kladminserver_srv.service
   ```

3. Téléchargez les modules supplémentaires « Fichiers pour l'installation à distance via Kaspersky Security Center » depuis le site Internet de Kaspersky.

   Les archives téléchargées portent les noms suivants :

   - ri_utils_win32.zip
   - ri_utils_arm64.zip

   Ne renommez pas les archives.

4. Placez les archives dans le répertoire /var/opt/kaspersky/klnagent_srv/1093/.working/ri_utils_archives.

Vous pouvez maintenant créer un paquet d'installation pour installer l'application sur des appareils Windows.

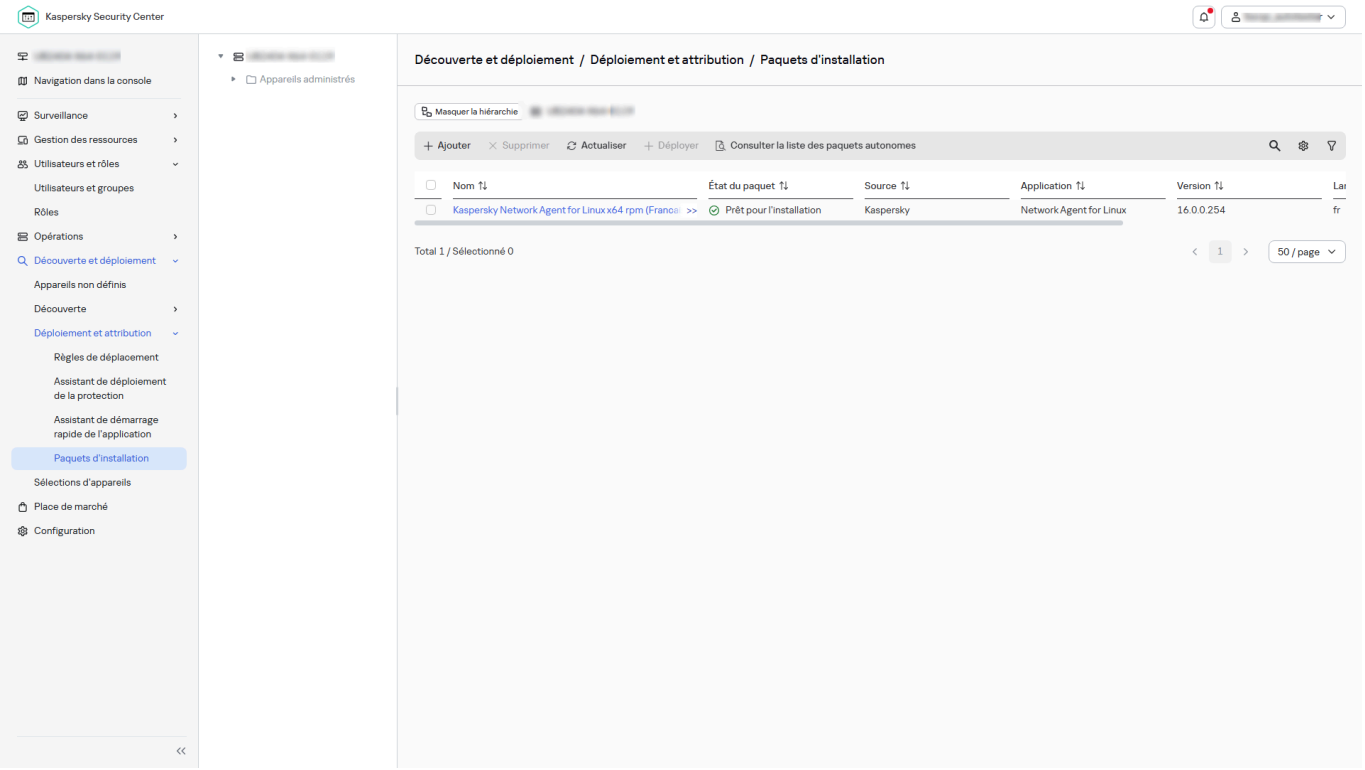
Pour télécharger et créer un paquet d'installation pour l'application Kaspersky, procédez comme suit :

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.

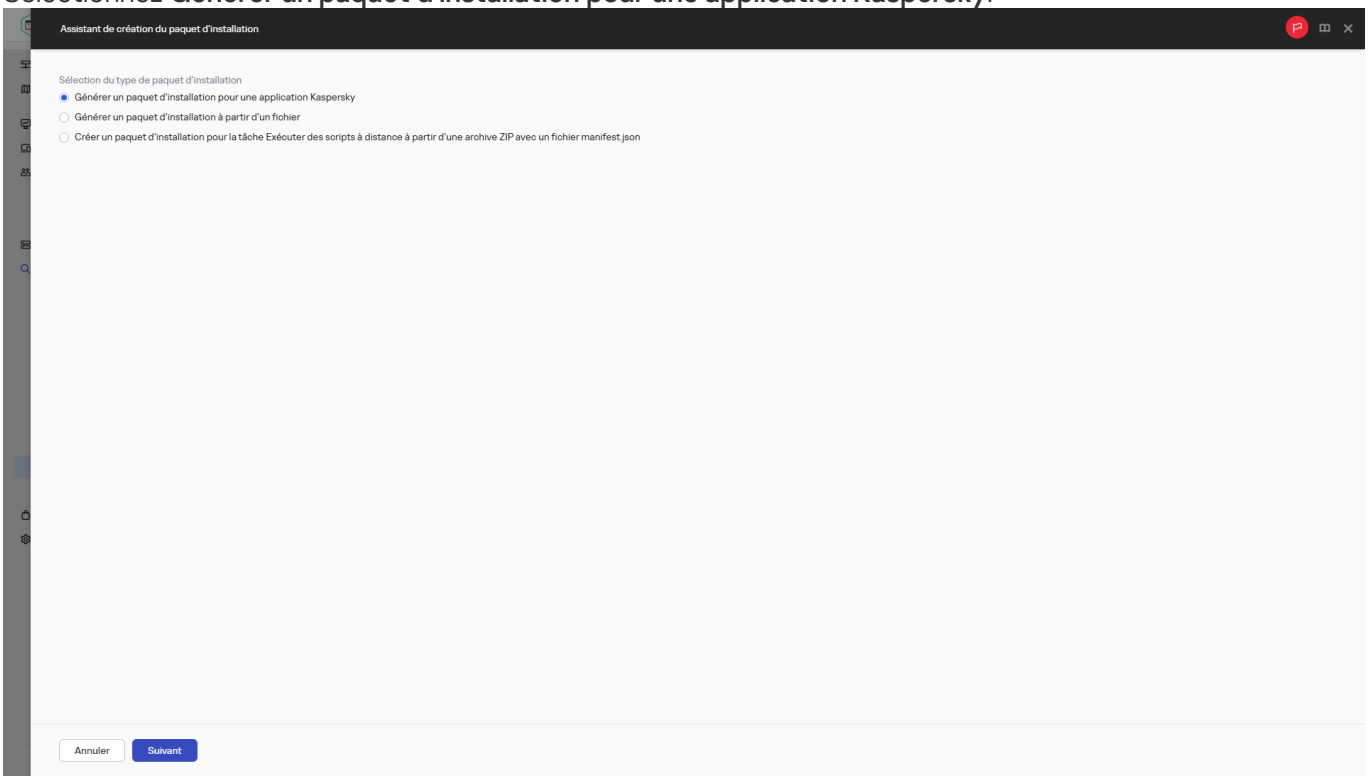


La liste des paquets d'installation

2. Cliquez sur **Ajouter**.

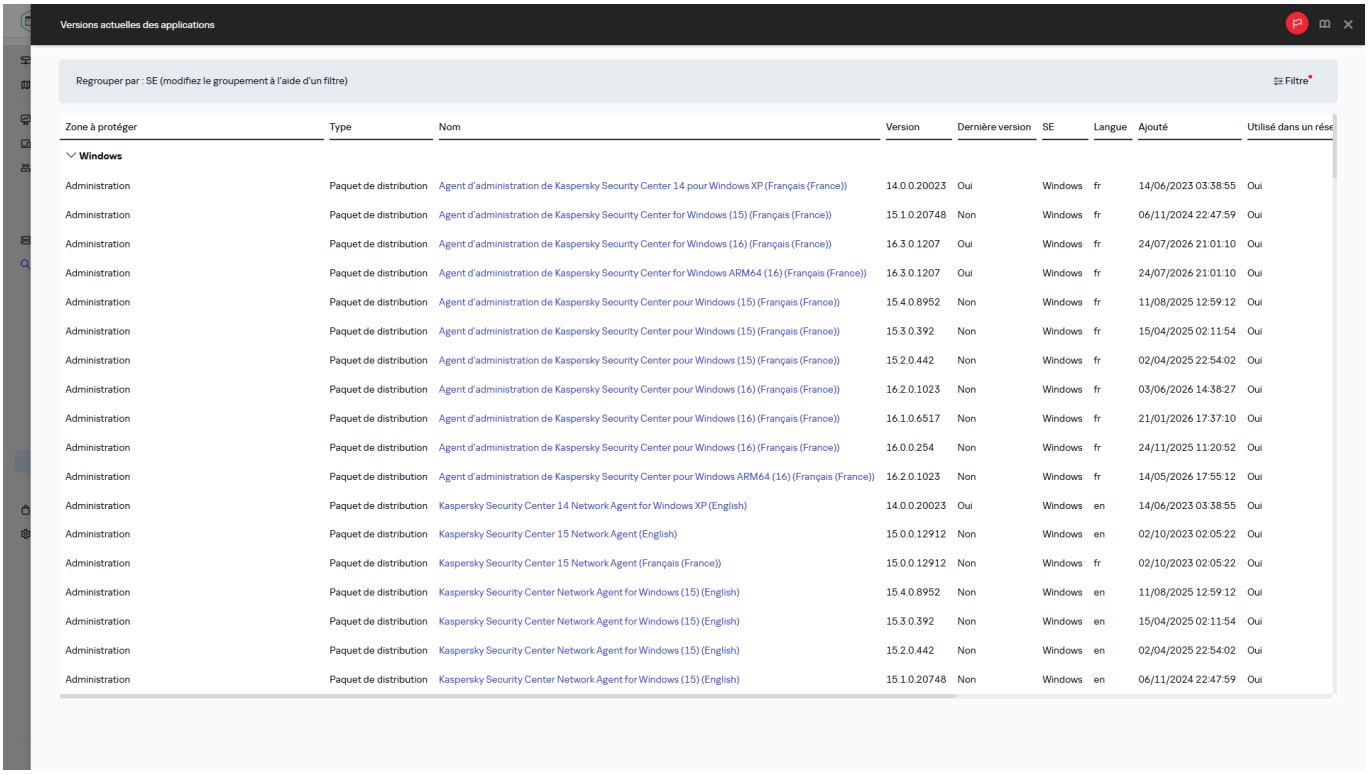
   L'Assistant de création du paquet d'installation se lance. Parcourez les étapes de l'assistant à l'aide du bouton **Suivant**.

3. Sélectionnez **Générer un paquet d'installation pour une application Kaspersky**.



Sélection du type de paquet d'installation

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. Par défaut, la liste n'affiche que les applications en anglais et dans la langue correspondant à la langue de l'interface. Pour afficher d'autres langues, cliquez sur **Filtrer** et configurez les paramètres du filtre.



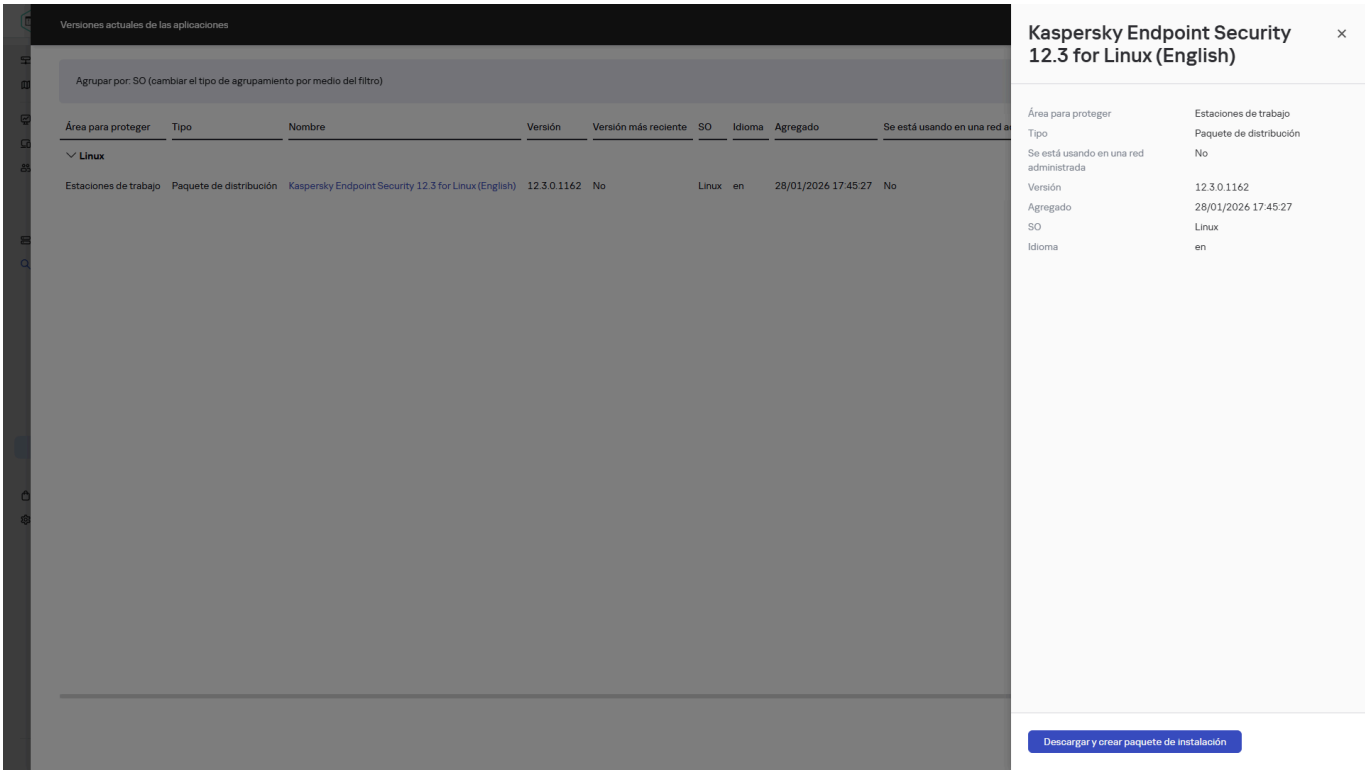
Zone à protéger	Type	Nom	Version	Dernière version	SE	Langue	Ajouté	Utilisé dans un rése
Windows								
Administration	Paquet de distribution	Agent d'administration de Kaspersky Security Center 14 pour Windows XP (Français (France))	14.0.0.20023	Oui	Windows	fr	14/06/2023 03:38:55	Oui
Administration	Paquet de distribution	Agent d'administration de Kaspersky Security Center for Windows (15) (Français (France))	15.1.0.20748	Non	Windows	fr	06/11/2024 22:47:59	Oui
Administration	Paquet de distribution	Agent d'administration de Kaspersky Security Center for Windows (16) (Français (France))	16.3.0.1207	Oui	Windows	fr	24/07/2026 21:01:10	Oui
Administration	Paquet de distribution	Agent d'administration de Kaspersky Security Center for Windows ARM64 (16) (Français (France))	16.3.0.1207	Oui	Windows	fr	24/07/2026 21:01:10	Oui
Administration	Paquet de distribution	Agent d'administration de Kaspersky Security Center pour Windows (15) (Français (France))	15.4.0.8952	Non	Windows	fr	11/08/2025 12:59:12	Oui
Administration	Paquet de distribution	Agent d'administration de Kaspersky Security Center pour Windows (15) (Français (France))	15.3.0.392	Non	Windows	fr	15/04/2025 02:11:54	Oui
Administration	Paquet de distribution	Agent d'administration de Kaspersky Security Center pour Windows (15) (Français (France))	15.2.0.442	Non	Windows	fr	02/04/2025 22:54:02	Oui
Administration	Paquet de distribution	Agent d'administration de Kaspersky Security Center pour Windows (16) (Français (France))	16.2.0.1023	Non	Windows	fr	03/06/2026 14:38:27	Oui
Administration	Paquet de distribution	Agent d'administration de Kaspersky Security Center pour Windows (16) (Français (France))	16.1.0.6517	Non	Windows	fr	21/01/2026 17:37:10	Oui
Administration	Paquet de distribution	Agent d'administration de Kaspersky Security Center pour Windows (16) (Français (France))	16.0.0.254	Non	Windows	fr	24/11/2025 11:20:52	Oui
Administration	Paquet de distribution	Agent d'administration de Kaspersky Security Center pour Windows ARM64 (16) (Français (France))	16.2.0.1023	Non	Windows	fr	14/05/2026 17:55:12	Oui
Administration	Paquet de distribution	Kaspersky Security Center 14 Network Agent for Windows XP (English)	14.0.0.20023	Oui	Windows	en	14/06/2023 03:38:55	Oui
Administration	Paquet de distribution	Kaspersky Security Center 15 Network Agent (English)	15.0.0.12912	Non	Windows	en	02/10/2023 02:05:22	Oui
Administration	Paquet de distribution	Kaspersky Security Center 15 Network Agent (Français (France))	15.0.0.12912	Non	Windows	fr	02/10/2023 02:05:22	Oui
Administration	Paquet de distribution	Kaspersky Security Center Network Agent for Windows (15) (English)	15.4.0.8952	Non	Windows	en	11/08/2025 12:59:12	Oui
Administration	Paquet de distribution	Kaspersky Security Center Network Agent for Windows (15) (English)	15.3.0.392	Non	Windows	en	15/04/2025 02:11:54	Oui
Administration	Paquet de distribution	Kaspersky Security Center Network Agent for Windows (15) (English)	15.2.0.442	Non	Windows	en	02/04/2025 22:54:02	Oui
Administration	Paquet de distribution	Kaspersky Security Center Network Agent for Windows (15) (English)	15.1.0.20748	Non	Windows	en	06/11/2024 22:47:59	Oui

La liste des paquets d'installation disponibles

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.



Téléchargement du paquet d'installation

5. Lisez les informations et cliquez sur le bouton **Télécharger et créer le paquet d'installation**.

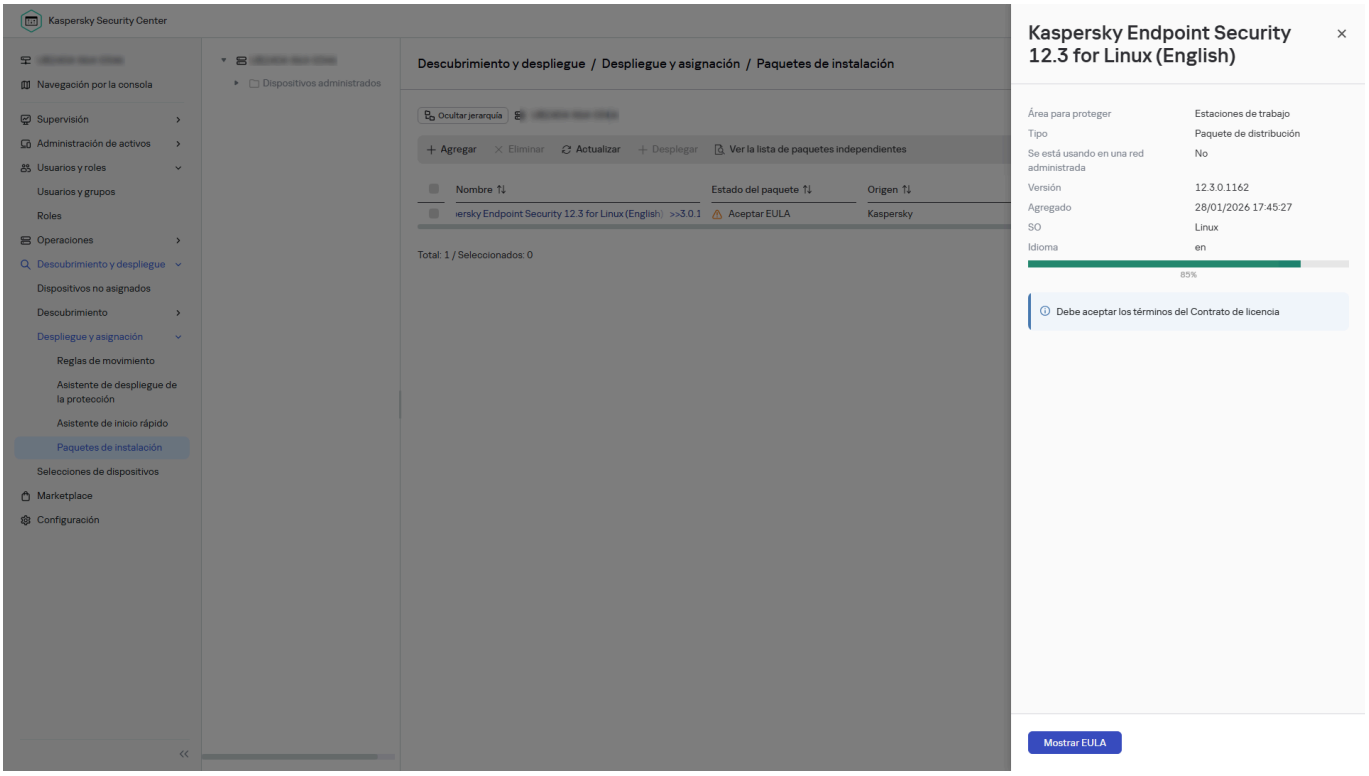
   Si un paquet de distribution ne peut pas être converti en un paquet d'installation, le bouton **Télécharger et créer le paquet d'installation** s'affiche à la place du bouton **Télécharger le paquet de distribution**.

Pour certaines applications de Kaspersky, le bouton **Afficher le CLUF** s'affiche avant ou pendant le téléchargement. Si c'est le cas, procédez comme suit :

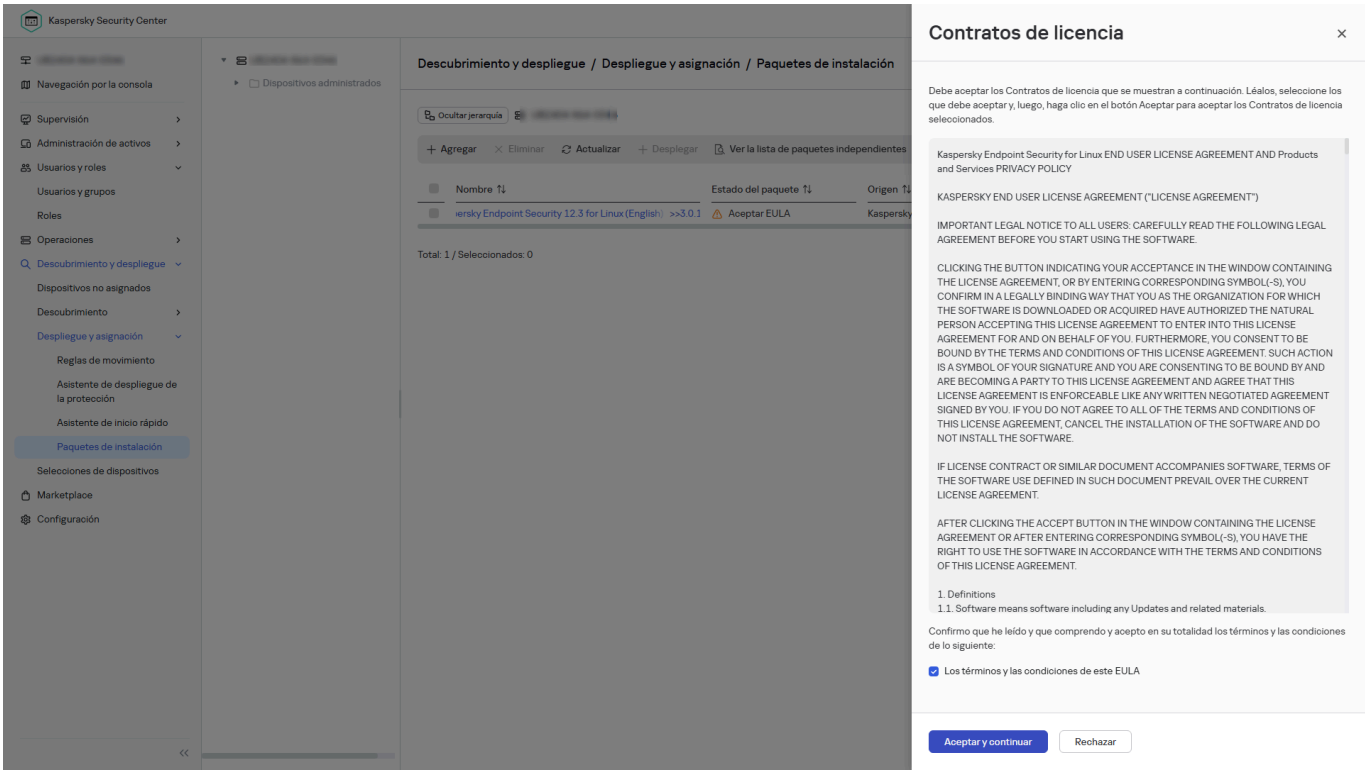
a. Cliquez sur le bouton **Afficher le CLUF** pour lire le contrat de licence utilisateur final (CLUF).

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.



Téléchargement du paquet d'installation



Acceptation du CLUF

Vous pouvez fermer la fenêtre de l'assistant. Dans ce cas, le processus de téléchargement se poursuivra en arrière-plan. Vous pouvez suivre l'état de téléchargement du paquet d'installation ainsi que filtrer et trier les statuts dans la colonne **État du paquet**.

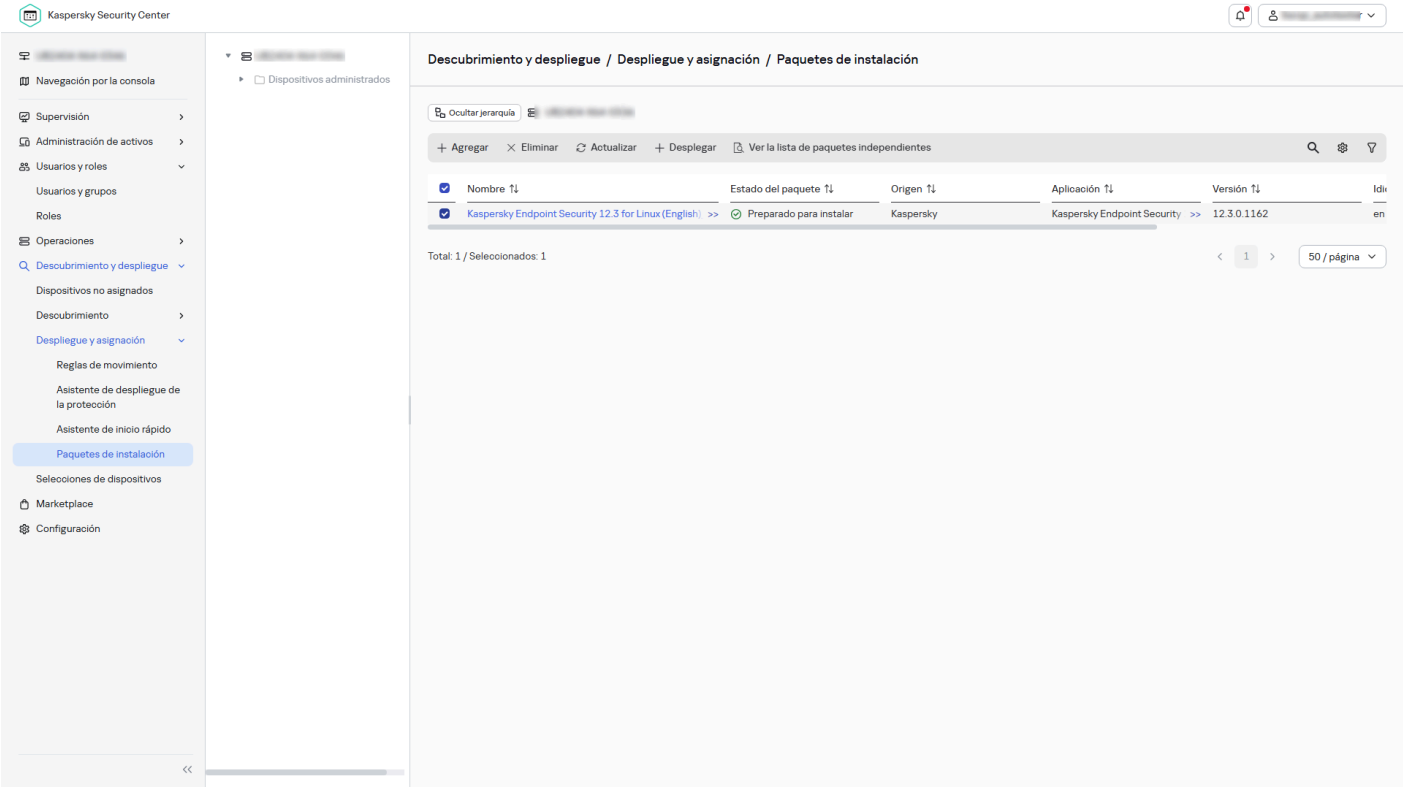
Si le processus de téléchargement s'arrête et que l'état du téléchargement passe à **Accepter le CLUF**, cliquez sur le nom du paquet d'installation et effectuez les étapes 5.a et 5.b.

Par défaut, les Paquets d'installation avec les statuts **En cours** et **Accepter le CLUF** sont placés au début de la liste.

> 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. 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.



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.

Si le Serveur d'administration a accès au stockage des paquets de distribution d'applications pour l'installation à distance, utilisez la tâche **Téléchargement des mises à jour sur le stockage du Serveur d'administration** pour télécharger les dépendances nécessaires à la création de paquets d'installation destinés à installer des applications sur les appareils Windows.

Si le Serveur d'administration n'a pas accès au stockage des paquets de distribution d'applications pour l'installation à distance :

1. Créez l'indicateur RIUtilsArchiveDirUsed en exécutant la commande suivante :

   ```
   /opt/kaspersky/ksc64/sbin/klscflag -fset -pv klserver -n RIUtilsArchiveDirUsed -t d -v 1
   ```

2. Exécutez la commande suivante pour redémarrer le service du Serveur d'administration :

   ```
   systemctl restart kladminserver_srv.service
   ```

3. Téléchargez les modules supplémentaires « Fichiers pour l'installation à distance via Kaspersky Security Center » depuis le site Internet de Kaspersky.

   Les archives téléchargées portent les noms suivants :

   - ri_utils_win32.zip
   - ri_utils_arm64.zip

   Ne renommez pas les archives.

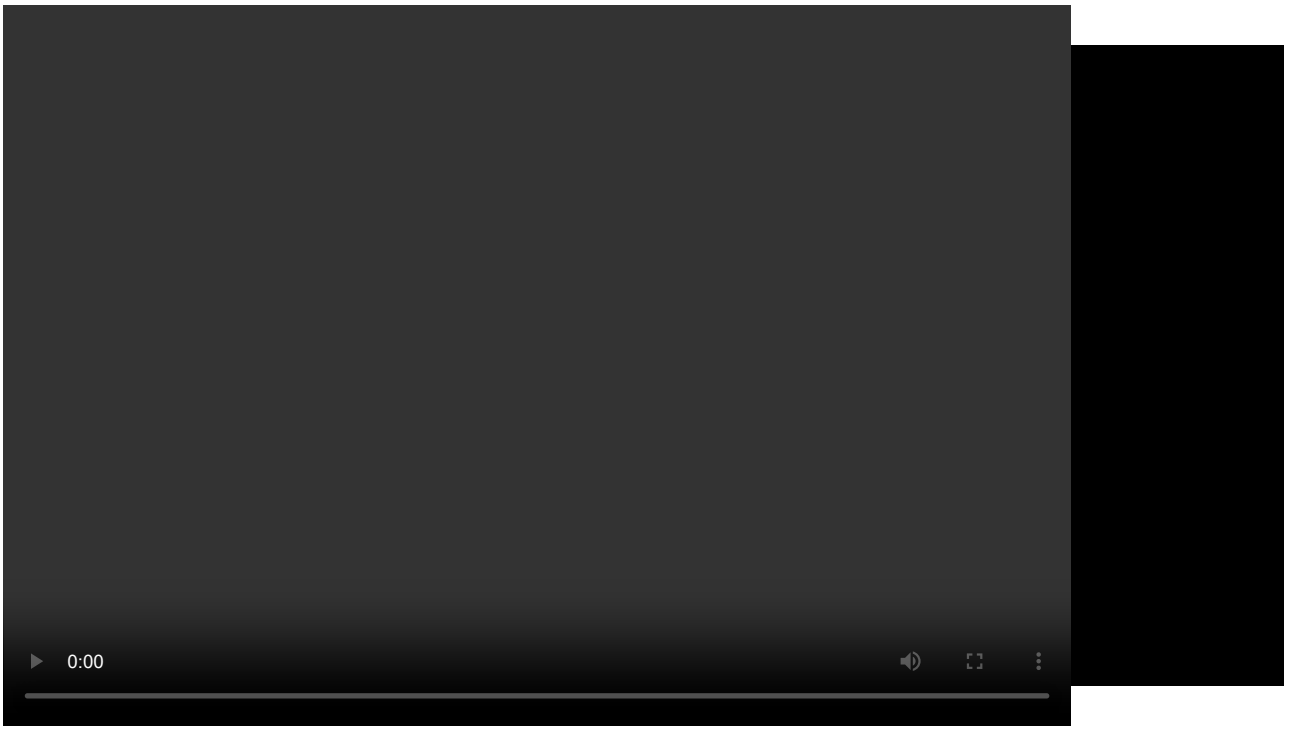
4. Placez les archives dans le répertoire /var/opt/kaspersky/klnagent_srv/1093/.working/ri_utils_archives.

   Dans le cas contraire, l'erreur suivante s'affiche lors de la création d'un paquet d'installation : **Utilitaires d'installation à distance pour win32 introuvables**.

Le Serveur d'administration dispose désormais des dépendances requises.

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.

Regardez la vidéo pour découvrir comment créer et déployer un paquet d'installation personnalisé pour Windows. La version texte de ce tutoriel, valable pour les appareils Windows et Linux, est disponible ci-dessous.



Création et déploiement d'un paquet d'installation personnalisé à partir d'un fichier pour Windows. Enregistrements vidéo

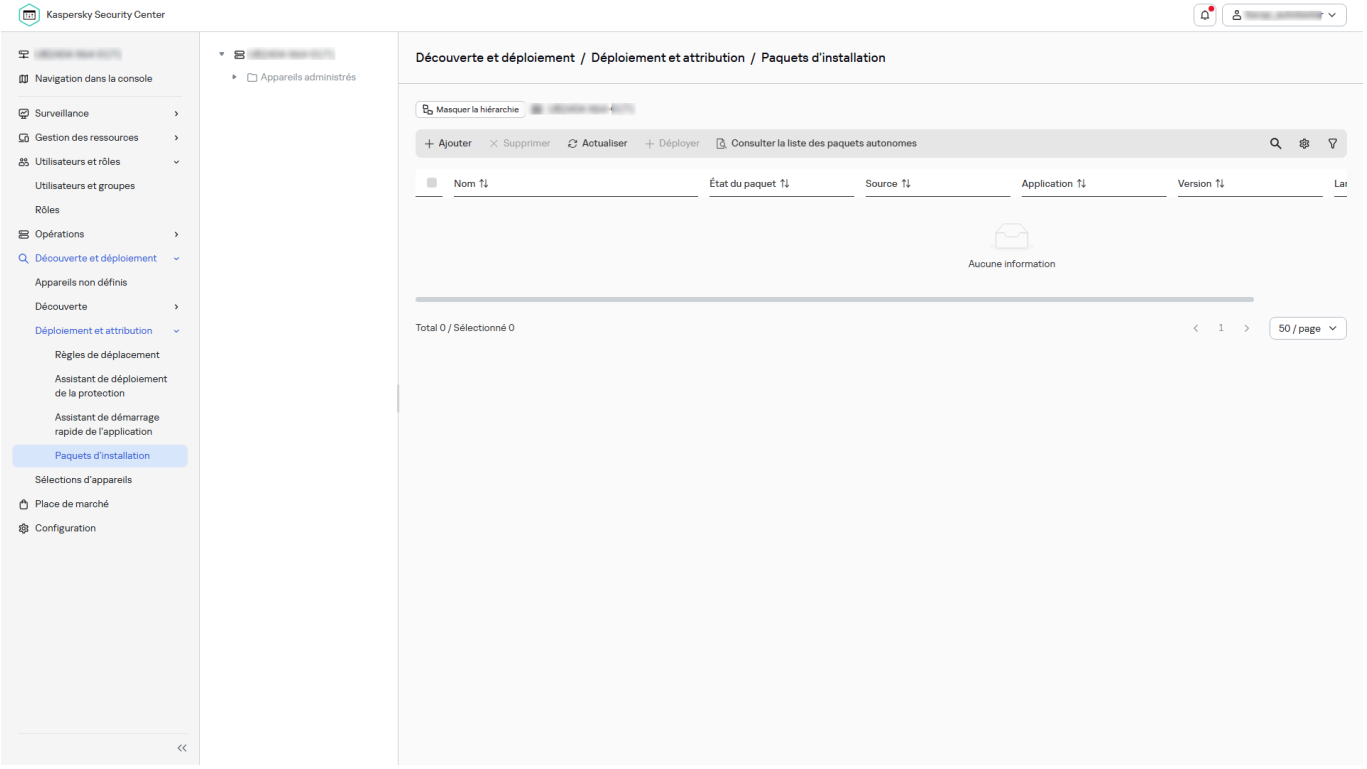
Pour créer le paquet d'installation personnalisé :

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.

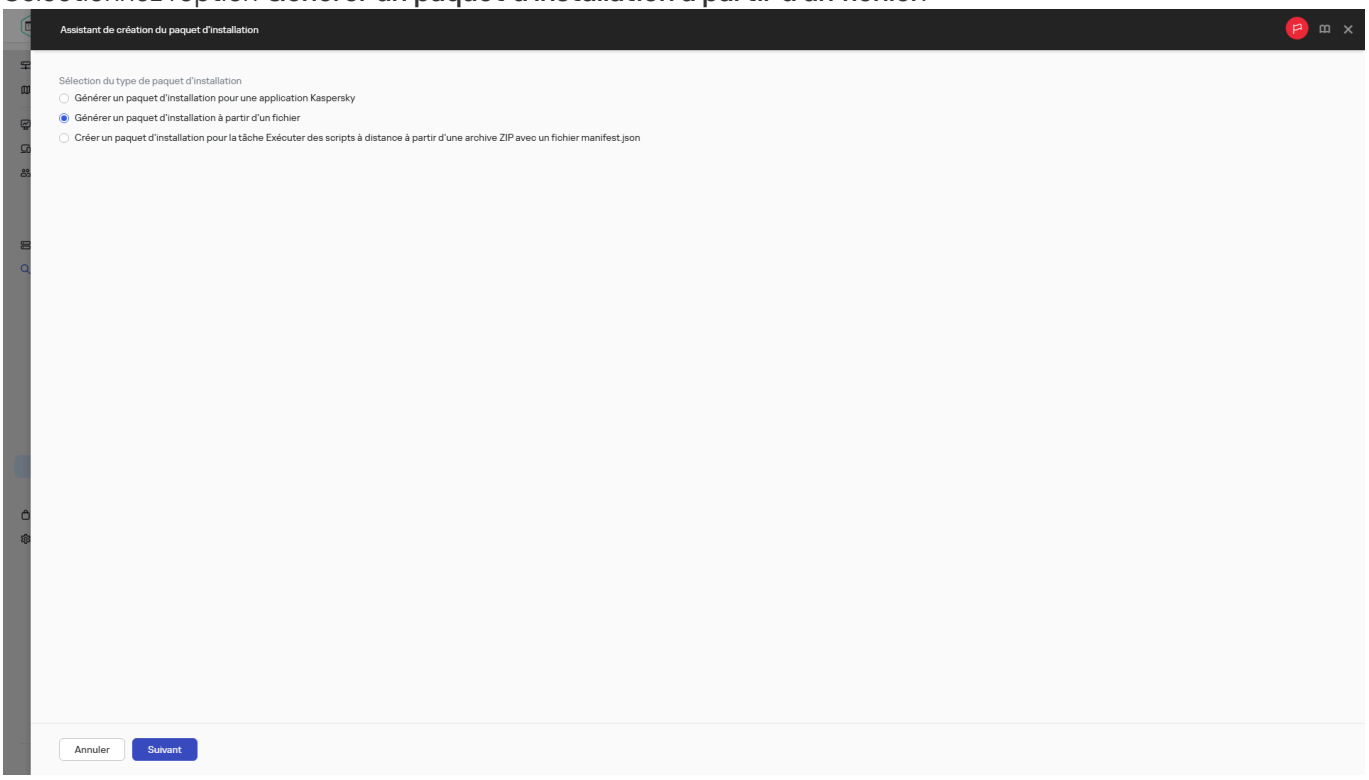


La liste des paquets d'installation

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**.



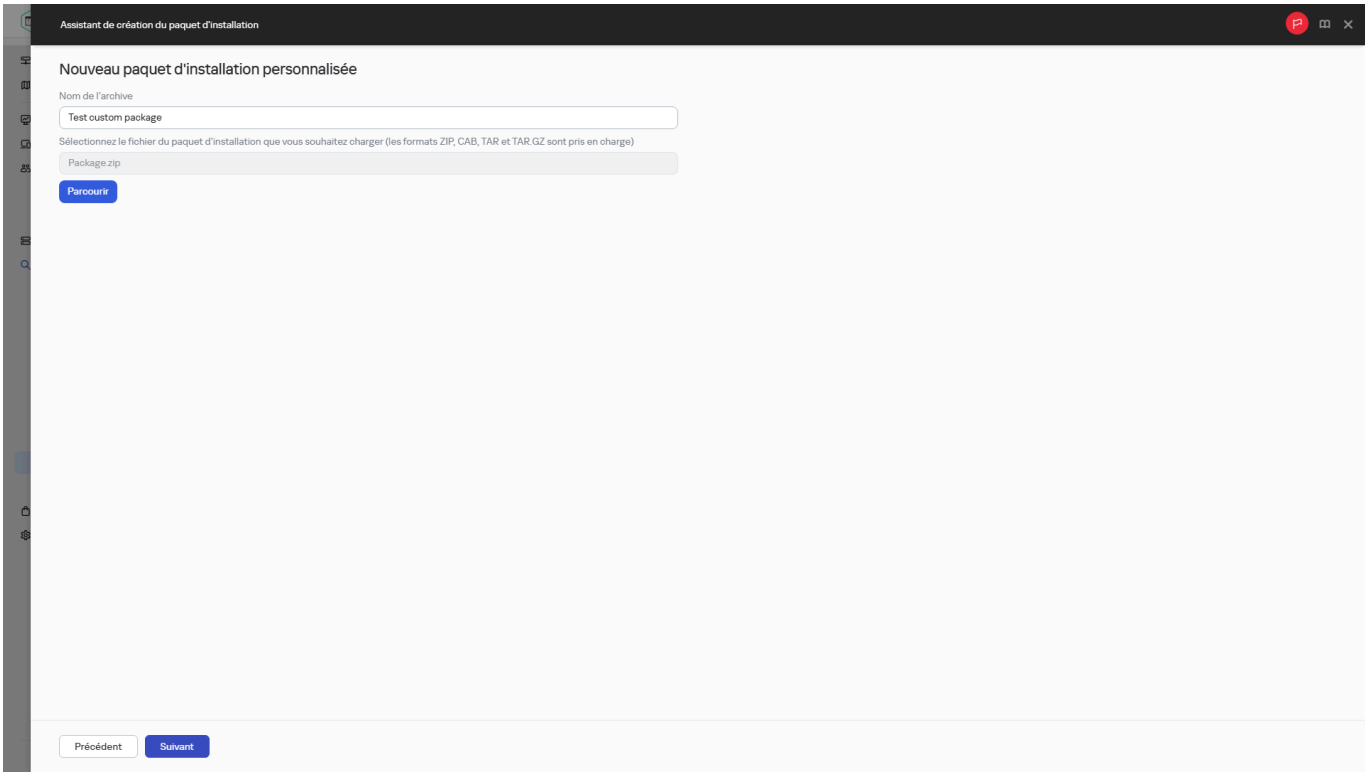
Sélection du type de paquet d'installation

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.



Spécification du fichier de paquet d'installation

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.

   Comment créer un paquet d'installation au format deb ou rpm

   1. Créez un script `.sh` à l'aide des commandes suivantes :

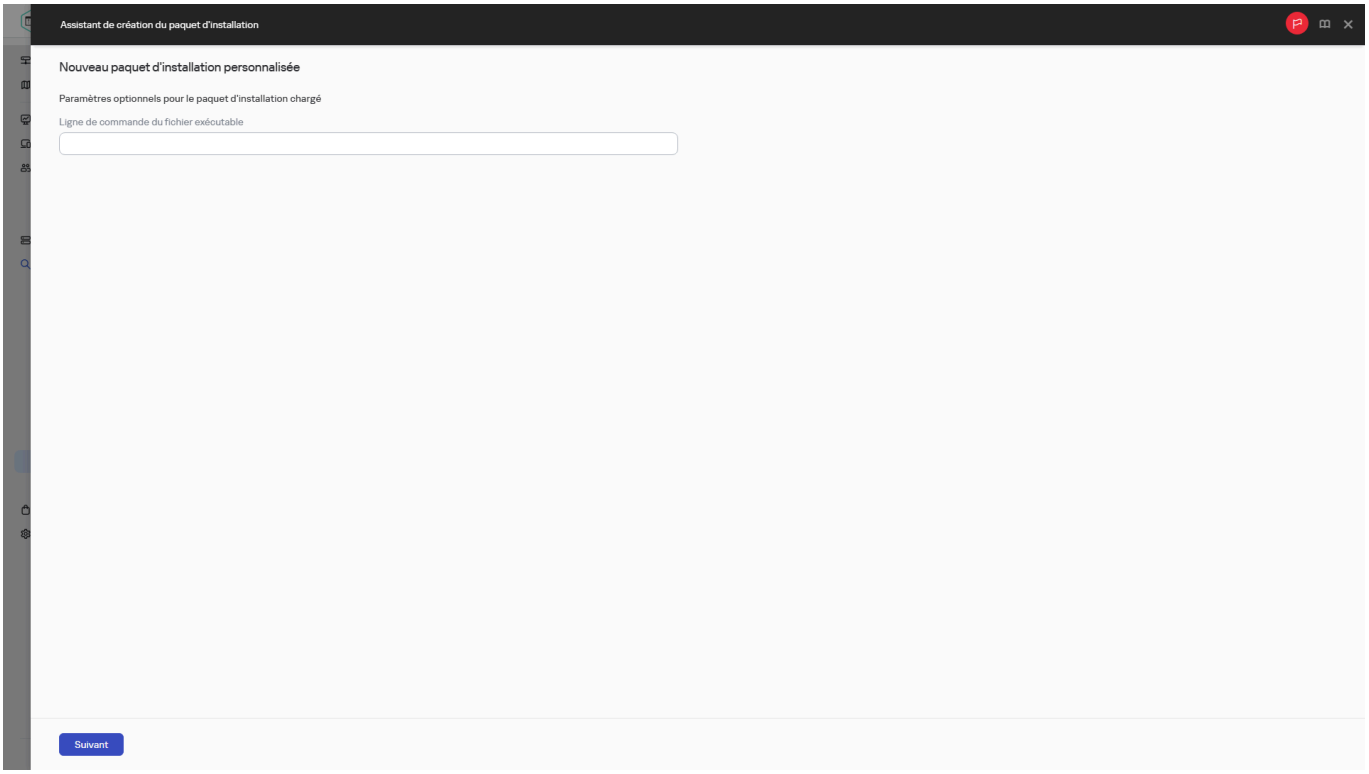
      ```
      #!/bin/sh
      script_dir="$(dirname "$0")"
      apt-get install --yes "$script_dir/<nom_du_paquet>.deb" </dev/null
      ```

      Le contenu du script et les commandes peuvent varier en fonction du format du paquet et d'autres détails. Vous pouvez adapter le script à votre configuration.

   2. Placez le script créé dans une archive avec le fichier `.deb` ou `.rpm`.

   3. Lors de la création du paquet d'installation, sélectionnez le script créé comme 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.



Spécification des paramètres de ligne de commande facultatifs

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.
  - **État du paquet**. État du téléchargement du paquet d'installation.
  - **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.

- **SE**. 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.

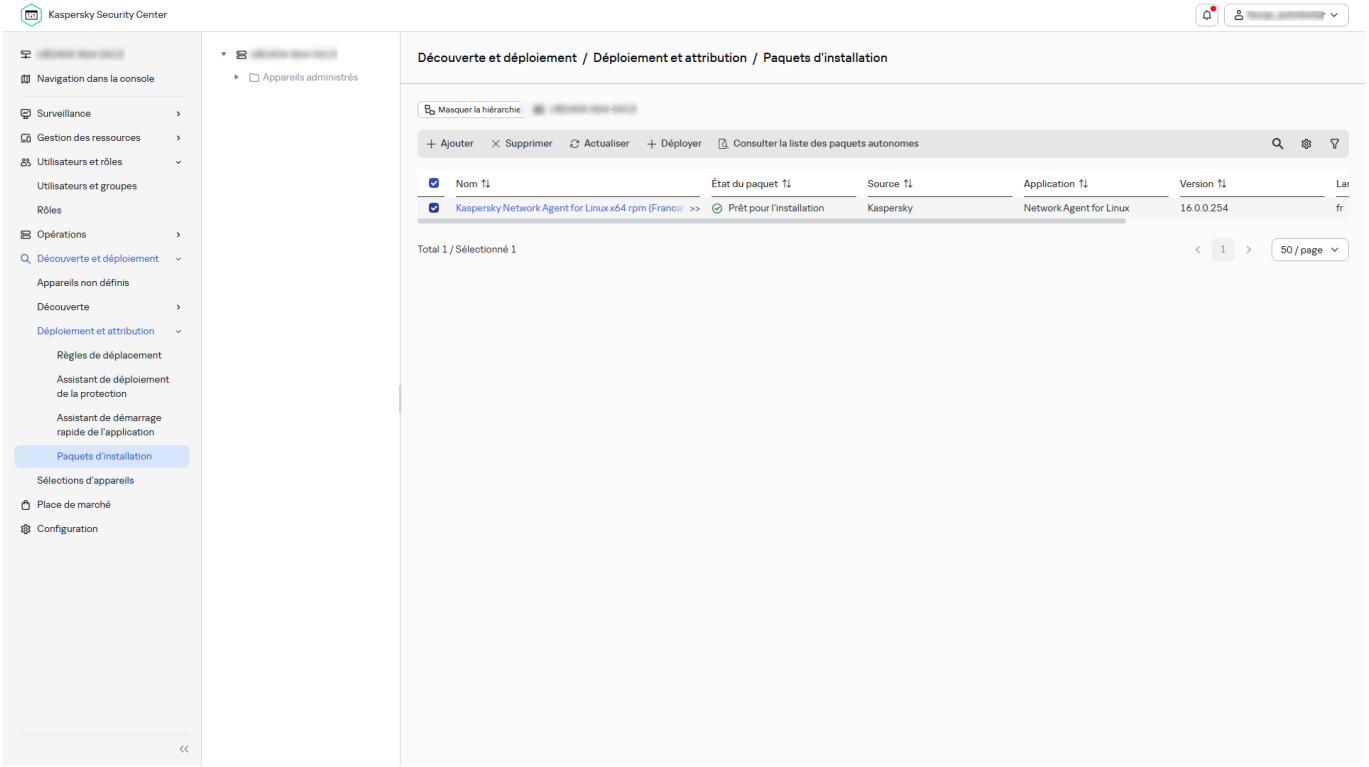
Pour créer un paquet d'installation autonome :

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.

   > Les informations relatives à la taille, au hachage du fichier et au chemin d'accès ne sont pas disponibles dans la liste des paquets d'installation pour le paquet autonome de l'Agent d'administration ou pour les paquets créés sur les Serveurs d'administration virtuels. Ces paquets autonomes sont générés au moment du téléchargement.

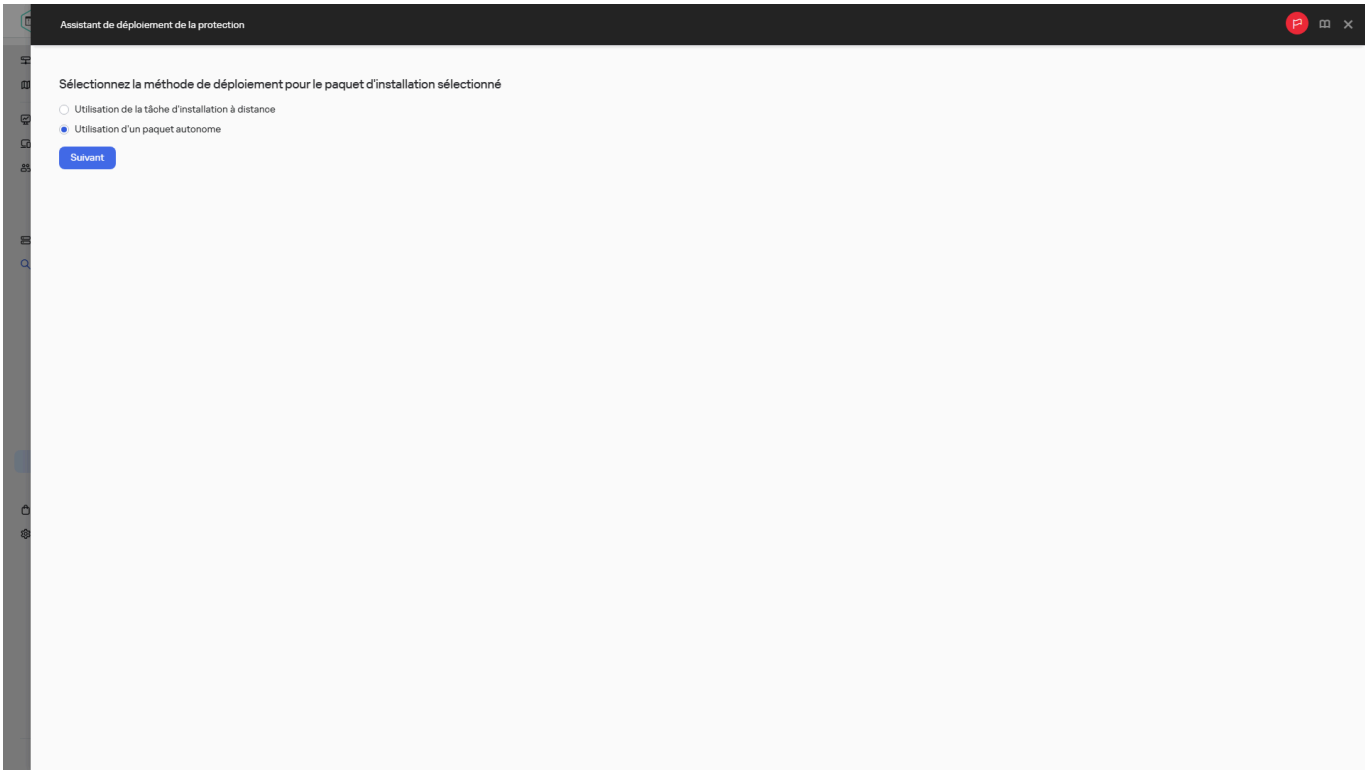
2. Dans la liste des paquets d'installation, sélectionnez le paquet d'installation de l'Agent d'administration et, au-dessus de la liste, cliquez sur le bouton **Déployer**.



La liste des paquets d'installation

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**.



Sélection de la méthode de déploiement pour le paquet d'installation

4. Assurez-vous que l'option **Installer l'Agent d'administration avec cette application** est activée si vous souhaitez installer l'Agent d'administration avec l'application sélectionnée.

L'option s'affiche en fonction de l'application pour laquelle vous créez un paquet d'installation autonome.

Cette option est activée par défaut. 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 dans un groupe d'administration après l'installation de l'Agent d'administration, laissez cette option activée.

   Si vous souhaitez déplacer les appareils clients vers un groupe d'administration après l'installation de l'Agent d'administration, sélectionnez l'option **Déplacer les appareils non définis dans ce groupe**, et spécifiez un groupe d'administration vers lequel vous souhaitez déplacer l'appareil client. Par défaut, l'appareil est déplacé vers le groupe **Appareils administrés**.

Sélection du groupe d'administration pour déplacer l'appareil client

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.

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 d'Agent d'administration 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, toutes les mises à jour et tous les correctifs pour le Serveur d'administration, l'Agent d'administration, Kaspersky Security Center Web Console et le Serveur MDM iOS téléchargés sont installés automatiquement.

  Si l'option est désactivée, les mises à jour et les correctifs téléchargés sont installés uniquement après que l'administrateur a modifié leur état pour qu'il soit *Approuvé*. Les mises à jour et les correctifs avec l'état *Non défini* ne sont pas installés.

  Cette option est activée par défaut.

- 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.

- **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 **Passerelle de connexion**, 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 **Machine virtuelle**, 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 les VM**

  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.

Si vous souhaitez que les utilisateurs soient automatiquement invités à s'enregistrer en tant que propriétaires d'appareils après l'installation de l'Agent d'administration sur des appareils Linux, activez l'option **Autoriser l'exécution de l'utilitaire d'enregistrement des utilisateurs après l'installation de l'Agent d'administration**.

Si cette option est activée, l'enregistrement de l'utilisateur en tant que propriétaire de l'appareil sera lancé après l'installation de l'Agent d'administration. Cette option est Inactif par défaut.

- 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.

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 peut être publié sur le Serveur Web interne (qui fait partie de Kaspersky Security Center Linux), si cela se justifie (l'accès à ce serveur Web depuis l'extérieur est configuré pour les utilisateurs des appareils) ou sur un serveur Web spécialement déployé qui fait partie de Kaspersky Security Center Web Console. Vous pouvez également copier les paquets autonomes sur un autre serveur Web.

Kaspersky Security Center Linux permet d'envoyer un lien aux utilisateurs sélectionnés par email. Ce lien mène au fichier du paquet autonome sur le serveur Web et le message invite le destinataire à lancer le fichier (en mode interactif ou en mode silencieux avec la clé " -s "). Le paquet d'installation autonome peut être joint au message électronique pour les utilisateurs des appareils qui n'ont pas accès au Serveur Web. L'administrateur peut 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 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 une application à l'aide d'un 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 requise, 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**.

   Finalement, l'Assistant de création du paquet d'installation autonome se lance. 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. À 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.

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.

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.

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 **Gestion des ressources** → **Tâches**.

   La liste des tâches s'affiche.

3. Cliquez sur **Ajouter**.

   Ceci permet de lancer l'assistant de création d'une tâche. Suivez les étapes de l'Assistant.

4. Sur la page **Paramètres de nouvelle tâche**, sélectionnez **Kaspersky Security Center** dans la liste déroulante **Application**. Ensuite, dans la liste déroulante **Type de tâche**, sélectionnez **Diffusion du paquet d'installation**, puis indiquez le nom de la tâche.

5. Sur la page **Zone d'action d'une 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. 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 terminée, les paquets d'installation sélectionnés sont copiés sur les Serveurs d'administration secondaires indiqués.

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.
- **Créé**. 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.
- **Hachage 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.

Les informations relatives à la taille, au hachage du fichier et au chemin d'accès ne sont pas disponibles dans la liste des paquets d'installation pour le paquet autonome de l'Agent d'administration ou pour les paquets créés sur les Serveurs d'administration virtuels. Ces paquets autonomes sont générés au moment du téléchargement.

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**.

Installation de l'Agent d'administration pour Linux

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.

Il existe les méthodes suivantes pour installer initialement l'Agent d'administration sur l'Appareil administré 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.

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.

Préparation de l'appareil fonctionnant sous le système d'exploitation Linux à l'installation de l'Agent d'administration

Avant l'installation de l'Agent d'administration sur un appareil Linux, il faut réaliser les étapes de préparation requises pour tout appareil Linux.

Pour préparer l'appareil fonctionnant sous le système d'exploitation Linux à l'installation à distance de l'Agent d'administration, procédez comme suit :

1. Assurez-vous que l'appareil sur lequel vous voulez installer l'Agent d'administration pour Linux fonctionne sur une des distributions Linux supportées.
2. Si vous souhaitez installer l'Agent d'administration sur AltOS en mode environnement logiciel fermé, désactivez ce mode jusqu'à la fin de l'installation.
3. Téléchargez le paquet d'installation de l'Agent d'administration via l'interface de l'application ou depuis le site Internet de Kaspersky.

Si vous devez installer Kaspersky Industrial CyberSecurity for Linux Nodes sur un appareil fonctionnant sous un système d'exploitation Linux avec la bibliothèque glibc 2.5, vous devez télécharger l'un des paquets d'installation suivants depuis le site Internet de Kaspersky :

- klnagent64_16.1.0-6517_amd64_glibc2.5.deb
- klnagent64-16.1.0-6517.x86_64_glibc2.5.rpm
- klnagent_16.1.0-6517_i386_glibc2.5.deb
- klnagent-16.1.0-6517.i386_glibc2.5.rpm

Ces paquets d'installation sont disponibles pour les systèmes d'exploitation suivants avec la bibliothèque glibc 2.5 :

- CentOS 5.2 32 bits / 64 bits
- CentOS 5.4 32 bits / 64 bits
- CentOS 6.4 32 bits/64 bits
- CentOS 6.6 32 bits/64 bits
- Astra Linux Special Edition RUSB.10015-01 (mise à jour opérationnelle 1.4) 64 bits

Vous devez posséder la licence Kaspersky Industrial CyberSecurity for Linux Nodes pour obtenir le paquet d'installation.

4. 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
   - utilitaire ps

5. 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. Assurez-vous que le port TCP 22 est ouvert et accessible sur un appareil sous Linux non défini.

Le port TCP 22 doit être disponible pour que l'installation de l'Agent d'administration pour Linux se déroule correctement.

c. Désactivez le mot de passe de la demande sudo pour le compte utilisateur utilisé pour la connexion à l'appareil.

d. Utilisez la commande `visudo` pour ouvrir le fichier de configuration sudoers.

Dans le fichier que vous avez ouvert, ajoutez la ligne suivante à la fin du fichier : `<username> ALL = (ALL) NOPASSWD: ALL`. Dans ce cas, `< username >` est le compte utilisateur qui sera utilisé pour la connexion à l'appareil via le protocole SSH. Si vous utilisez le système d'exploitation Astra Linux, ajoutez dans le fichier /etc/sudoers la dernière ligne avec le texte suivant : `%astra-admin ALL=(ALL:ALL) NOPASSWD: ALL`

e. Enregistrez le fichier sudoers et fermez-le.

f. 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`.

6. Si vous souhaitez installer l'Agent d'administration à distance sur les appareils exécutant le système d'exploitation avec le système d'initialisation systemd, ouvrez le fichier `/etc/systemd/logind.conf`, puis exécutez une des actions suivantes :

- Spécifiez `no` comme valeur pour le paramètre `KillUserProcesses` : `KillUserProcesses=no`.
- Pour le paramètre `KillExcludeUsers`, saisissez le nom d'utilisateur du compte sous lequel l'installation à distance doit être effectuée, par exemple, `KillExcludeUsers=root`.

Appareil cible Astra Linux

Si la machine cible exécute Astra Linux, ajoutez la chaîne `export PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin` dans le fichier `/home/< nom d'utilisateur >/.bashrc`, où `< nom d'utilisateur >` est le compte à utiliser pour la connexion de l'appareil via SSH.

Appareil cible OSnova

Si l'appareil cible fonctionne sous OSnova, procédez comme suit :

a. Ouvrez le fichier `/usr/lib/systemd/logind.conf/10-enable-kill-user-processes.conf`, puis commentez la ligne `#KillUserProcess=yes`.

b. Ouvrez le fichier `/usr/lib/NESS/pam-user-session`, puis commentez la ligne `#loginctl terminate-session "$XDG_SESSION_ID"`.

Pour appliquer le paramètre modifié, redémarrez l'appareil Linux ou exécutez la commande suivante :

```
sudo systemctl restart systemd-logind.service
```

7. 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.

8. 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.

9. Si vous souhaitez installer l'Agent d'administration sur des appareils fonctionnant sous Ubuntu Server ou Ubuntu Desktop version 10.04, effectuez des étapes complémentaires de préparation de ces appareils.

10. Si vous souhaitez installer Kaspersky Industrial CyberSecurity for Linux Nodes sur un appareil fonctionnant sous un système d'exploitation Linux avec glibc 2.5, suivez les étapes supplémentaires pour préparer les appareils cibles.

11. Si vous installez l'Agent d'administration sur AltOS en mode environnement logiciel fermé, réactivez ce mode.

12. 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.

L'appareil Linux est prêt pour l'installation de l'Agent d'administration. Vous pouvez installer l'Agent d'administration à distance, en mode interactif ou en mode silencieux.

Préparation d'un appareil exécutant SUSE Linux Enterprise Server 15 pour l'installation de l'Agent d'administration

Avant d'installer l'Agent d'administration sur un appareil exécutant SUSE Linux Enterprise Server 15, vous devez effectuer deux procédures de préparation : celle des instructions ci-dessous et les étapes générales de préparation pour tout appareil Linux.

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.

Une fois l'appareil Linux préparé, vous pouvez installer l'Agent d'administration à distance, en mode interactif ou en mode silencieux.

Préparation d'un appareil exécutant Astra Linux dans l'environnement logiciel fermé mode pour l'installation de l'Agent d'administration

Avant l'installation de l'Agent d'administration sur un appareil exécutant Astra Linux en mode environnement logiciel fermé, vous devez effectuer deux procédures de préparation : celle des instructions ci-dessous et les étapes générales de préparation pour tout appareil Linux.

> Exécutez les commandes fournies dans cette instruction sous un compte avec des privilèges root.

Pour préparer un appareil exécutant Astra Linux dans l'environnement logiciel fermé mode en vue de l'installation de l'Agent d'administration, procédez comme suit :

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

   ```
   DIGSIG_ELF_MODE=1
   ```

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

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

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

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

4. Placez la clé de l'application /opt/kaspersky/klnagent64/share/kaspersky_astra_pub_key.gpg dans le répertoire créé à l'étape précédente :

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

   > Si le kit de distribution 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.

L'appareil Linux est prêt pour l'installation de l'Agent d'administration. Vous pouvez installer l'Agent d'administration à distance, en mode interactif ou en mode silencieux.

Préparation de l'installation de l'Agent d'administration sur un système d'exploitation Linux équipé de glibc 2.5 (ancien système d'exploitation)

Avant d'installer l'Agent d'administration sur un appareil exécutant un système d'exploitation Linux avec glibc 2.5 (ancien système d'exploitation), vous devez effectuer deux procédures de préparation, à savoir les étapes de préparation générales pour tout appareil Linux et la procédure décrite dans cet article.

Nous vous recommandons d'utiliser l'installation locale pour installer l'Agent d'administration sur le système d'exploitation Linux équipé de glibc 2.5 (ancien système d'exploitation). S'il est nécessaire d'utiliser une tâche d'installation à distance pour ce scénario, suivez les étapes supplémentaires décrites dans les instructions ci-dessous.

> Exécutez les commandes fournies dans cette procédure sous un compte avec des privilèges root.

Nous vous recommandons d'utiliser l'installation locale pour installer l'Agent d'administration sur le système d'exploitation Linux équipé de glibc 2.5 (ancien système d'exploitation). S'il est nécessaire d'utiliser une tâche d'installation à distance pour ce scénario, suivez les étapes supplémentaires décrites dans les instructions ci-dessous.

1. Sur l'appareil exécutant un système d'exploitation Linux avec glibc 2.5, effectuez les étapes de préparation communes pour tout appareil Linux.

2. Dans le fichier `/etc/sudoers`, supprimez la ligne `Defaults requiretty`.

3. Désactivez la liste d'autorisation des algorithmes de chiffrement valides pour les connexions SSH afin de pouvoir installer l'Agent d'administration sur l'appareil exécutant un système d'exploitation Linux avec glibc 2.5.

   Pour ce faire, sur l'appareil sur lequel le Serveur d'administration est installé ou sur un appareil faisant office de point de distribution dont la portée inclut l'appareil cible, exécutez la commande suivante dans la ligne de commande :

   ```
   klscflag -fset -pv ".core/.independent" -s "Transport" -n
   SSH_CLIENT_DISABLE_ALGS_PROTECT -t d -v 1
   ```

L'appareil Linux est prêt pour l'installation à distance de l'Agent d'administration.

La désactivation de la liste d'autorisation des algorithmes de chiffrement valides peut avoir une incidence sur la sécurité de la connexion SSH. Nous vous recommandons vivement de réactiver la liste d'autorisation des algorithmes de chiffrement valides immédiatement après l'installation de Agent d'administration. Pour réactiver la liste d'autorisation des algorithmes de chiffrement valides, exécutez la commande suivante :

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

Une fois que vous avez installé l'Agent d'administration et réactivé la liste d'autorisation des algorithmes de chiffrement valides, l'appareil fonctionnant sous un système d'exploitation Linux avec glibc 2.5 (ancien système d'exploitation) est désormais géré par le Serveur d'administration.

Préparation de l'installation de l'Agent d'administration sur un système d'exploitation Linux équipé d'OpenSSH version 6.4 (ancien système d'exploitation)

Avant d'installer l'Agent d'administration sur un appareil utilisant OpenSSH version 6.4 ou toute version antérieure (ancien système d'exploitation), vous devez effectuer deux procédures de préparation – les étapes de préparation générales pour tout appareil Linux et la procédure décrite dans cet article.

Nous vous recommandons d'utiliser l'installation locale pour installer l'Agent d'administration sur le système d'exploitation Linux équipé de glibc 2.5 (ancien système d'exploitation). S'il est nécessaire d'utiliser une tâche d'installation à distance pour ce scénario, suivez les étapes supplémentaires décrites dans les instructions ci-dessous.

Exécutez les commandes fournies dans cette instruction sous un compte avec des privilèges root.

Pour préparer un appareil qui utilise OpenSSH version 6.4 ou une version antérieure pour l'installation de l'Agent d'administration :

1. Sur l'appareil qui utilise OpenSSH version 6.4 ou une version antérieure, exécutez les étapes de préparation communes à tout appareil Linux.

2. Désactivez la liste d'autorisation des algorithmes de chiffrement valides pour les connexions SSH afin de pouvoir installer l'Agent d'administration sur l'appareil qui utilise OpenSSH version 6.4 ou toute version antérieure.

   Pour ce faire, sur l'appareil sur lequel le Serveur d'administration est installé ou sur un appareil faisant office de point de distribution dont la portée inclut l'appareil cible, exécutez la commande suivante dans la ligne de commande :

   ```
   klscflag -fset -pv ".core/.independent" -s "Transport" -n
   SSH_CLIENT_DISABLE_ALGS_PROTECT -t d -v 1
   ```

L'appareil Linux est prêt pour l'installation à distance de l'Agent d'administration.

La désactivation de la liste d'autorisation des algorithmes de chiffrement valides peut avoir une incidence sur la sécurité de la connexion SSH. Nous vous recommandons vivement de réactiver la liste d'autorisation des algorithmes de chiffrement valides immédiatement après l'installation de Agent d'administration. Pour réactiver la liste d'autorisation des algorithmes de chiffrement valides, exécutez la commande suivante :

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

Une fois que vous avez installé l'Agent d'administration et réactivé la liste d'autorisation des algorithmes de chiffrement valides, l'appareil fonctionnant sous un système d'exploitation Linux avec glibc 2.5 (ancien système d'exploitation) est désormais géré par le Serveur d'administration.

Installation à distance de l'Agent d'administration sur un appareil Linux

Avant l'installation de l'Agent d'administration sur l'appareil Linux, il faut réaliser les étapes préparatoires générales requises pour tous les appareils Linux.

Une fois la procédure générale terminée, vous pouvez suivre les instructions supplémentaires, propres à votre système d'exploitation :

- Préparation d'un appareil exécutant SUSE Linux Enterprise Server 15
- Préparation d'un appareil exécutant Astra Linux en mode environnement logiciel fermé
- Préparation d'un appareil exécutant UbuntuServer/Desktopversion 10.04 et 16.04
- Préparation d'un appareil fonctionnant sous le système d'exploitation Linux avec glibc 2.5

Pour installer l'Agent d'administration sur l'appareil localement, procédez comme suit :

1. Téléchargez et créez le paquet d'installation :

   a. Avant l'installation du paquet sur l'appareil, assurez-vous que les dépendances (les applications, les bibliothèques) liées au paquet en question sont installées.

      Vous pouvez indépendamment consulter les dépendances liées à chaque paquet en utilisant les utilitaires spécifiques à ce distributif Linux sur lequel le paquet sera installé. Vous pouvez consulter les informations relatives aux utilitaires dans la documentation de votre système d'exploitation.

   b. Pour la création du paquet d'installation à distance, utilisez les fichiers :

      - klnagent.kpd
      - akinstall.sh
      - Paquet .deb ou .rpm de l'Agent d'administration

2. Créez la tâche d'installation à distance de l'application avec les paramètres :

   - Dans la page **Paramètres** de l'assistant de création d'une tâche, cochez la case **En utilisant les ressources du système d'exploitation via le Serveur d'administration**. Décochez toutes les autres cases.
   - Dans la page **Sélection du compte utilisateur pour exécuter la tâche**, définissez les paramètres du compte utilisateur servant à connecter l'appareil via SSH.

3. Lancez la tâche d'installation à distance de l'application. Utilisez l'option de la commande `su` pour préserver l'environnement : `-m, -p, --preserve-environment`.

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.

Avant l'installation de l'Agent d'administration sur l'appareil Linux, il faut réaliser les étapes préparatoires générales requises pour tous les appareils Linux.

Une fois la procédure générale terminée, vous pouvez suivre les instructions supplémentaires, propres à votre système d'exploitation :

- Préparation d'un appareil exécutant SUSE Linux Enterprise Server 15
- Préparation d'un appareil exécutant Astra Linux en mode environnement logiciel fermé
- Préparation d'un appareil exécutant Ubuntu Server/Desktop version 10.04 et 16.04
- Préparation d'un appareil fonctionnant sous le système d'exploitation Linux avec glibc 2.5

Pour effectuer l'installation de l'Agent d'administration pour 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. Créez le fichier de réponse (au format TXT). Ajoutez au fichier de réponse une liste de variables au format VARIABLE_NAME=variable_value, chaque variable sur une ligne distincte.

   Pour assurer une utilisation correcte du fichier de réponse, vous devez y inclure un ensemble minimum des trois variables requises :

   - KLNAGENT_SERVER
   - KLNAGENT_AUTOINSTALL
   - EULA_ACCEPTED

   Vous pouvez également ajouter des variables facultatives pour utiliser des paramètres plus spécifiques de votre installation à distance. Le tableau suivant affiche toutes les variables pouvant être incluses dans le fichier de réponse :

   Variables du fichier de réponse utilisées comme paramètres de l'installation de l'Agent d'administration pour Linux en mode silencieux

   Variables du fichier de réponse utilisées comme paramètres de l'installation de l'Agent d'administration pour Linux en mode silencieux

Nom de la variable	Requis	Description	Valeurs possibles
KLNAGENT_SERVER	Oui	Contient le nom du Serveur d'administration présenté comme nom de domaine pleinement qualifié (FQDN) ou adresse IP.	Nom DNS ou adresse IP.

KLNAGENT_AUTOINSTALL	Oui	Définit si le mode d'installation silencieux est activé.	1 : le mode silencieux est activé ; l'utilisateur n'est invité à aucune action lors de l'installation. Autre : le mode silencieux est désactivé ; l'utilisateur peut être invité à effectuer des actions lors de l'installation.
EULA_ACCEPTED	Oui	Définit si l'utilisateur accepte le Contrat de licence utilisateur final (CLUF) de l'Agent d'administration ; lorsqu'il est manquant, il peut être interprété comme une non-acceptation du CLUF.	1 : je confirme que j'ai entièrement lu le présent Contrat de licence utilisateur final, que je le comprends et que j'accepte toutes ses conditions. Autre valeur ou valeur non définie : je refuse les conditions du Contrat de licence (l'installation n'aura pas lieu).
KLNAGENT_PROXY_USE	Non	Définit si la connexion avec le Serveur d'administration utilisera les paramètres du proxy. La valeur par défaut est égale à 0.	1 : les paramètres du proxy sont utilisés. Autre : les paramètres du proxy ne sont pas utilisés.
KLNAGENT_PROXY_ADDR	Non	Définit l'adresse du serveur proxy utilisé pour la connexion avec le Serveur d'administration.	Nom DNS ou adresse IP.
KLNAGENT_PROXY_LOGIN	Non	Définit le nom d'utilisateur utilisé pour établir la connexion au serveur proxy.	Tout nom d'utilisateur existant.
KLNAGENT_PROXY_PASSWORD	Non	Définit le mot de passe d'utilisateur utilisé pour établir la connexion au serveur proxy.	Tout jeu de caractères alphanumériques autorisé par le format du mot de passe dans le système d'exploitation.
KLNAGENT_VM_VDI	Non	Définit si l'Agent d'administration est installé sur une image pour la création de machines virtuelles dynamiques.	1 : l'Agent d'administration est installé sur une image, qui est ensuite utilisée pour la création de machines virtuelles dynamiques. Autre : aucune image n'est utilisée pendant l'installation.
KLNAGENT_VM_OPTIMIZE	Non	Définit si les paramètres de l'Agent d'administration sont optimaux pour l'hyperviseur.	1 : les paramètres locaux par défaut de l'Agent d'administration sont modifiés afin de permettre une utilisation optimisée sur l'hyperviseur.
KLNAGENT_TAGS	Non	Répertorie les balises attribuées à l'instance de l'Agent d'administration.	Un ou plusieurs noms de balises séparés par un point-virgule.
KLNAGENT_UDP_PORT	Non	Définit le port UDP utilisé par l'Agent d'administration. La valeur par défaut est égale à 15000.	Tout numéro de port existant.
KLNAGENT_PORT	Non	Définit le port non TLS utilisé par l'Agent d'administration. La valeur par défaut est égale à 14000.	Tout numéro de port existant.
KLNAGENT_SSLPORT	Non	Définit le port TLS utilisé par l'Agent d'administration. La valeur par défaut est égale à 13000.	Tout numéro de port existant.
KLNAGENT_USESSL	Non	Définit si le protocole TLS (Transport Layer Security ou Sécurité de la couche de transport) est utilisé pour établir la connexion.	1 (par défaut) : le protocole TLS est utilisé. Autre : le protocole TLS n'est pas utilisé.

KLNAGENT_GW_MODE	Non	Définit si la passerelle de connexion est utilisée.	1 (par défaut) : les paramètres actuels ne sont pas modifiés (au premier appel, aucune passerelle de connexion n'est définie). 2 : aucune passerelle de connexion n'est utilisée. 3 : une passerelle de connexion est utilisée. KLNAGENT_GW_ADDRESS est requis. 4 : l'instance de l'Agent d'administration est utilisée comme passerelle de connexion dans la zone démilitarisée (DMZ). Un certificat de serveur est requis.
KLNAGENT_GW_ADDRESS	Non	Définit l'adresse de la passerelle de connexion. La valeur n'est applicable que si KLNAGENT_GW_MODE=3.	Nom DNS ou adresse IP.
KLNAGENT_DEVICEOWNER_REGISTRATION_START	Non	Permet d'exécuter l'enregistrement de l'utilisateur en tant que propriétaire de l'appareil après l'installation de l'Agent d'administration. Si cette option est désactivée, l'enregistrement en tant que propriétaire de l'appareil n'est pas disponible pour l'utilisateur.	1 : l'enregistrement de l'utilisateur en tant que propriétaire de l'appareil sera lancé après l'installation de l'Agent d'administration. Autre : désactivé.
PTCH_ALLOW_APPLY_NONAPROVED_PATCHES	Non	Définit s'il faut installer automatiquement les mises à jour téléchargées pour l'Agent d'administration avec l'état *Non défini*.	true (par défaut) : les mises à jour sont installées automatiquement. false : les mises à jour ne sont pas installées automatiquement.

3. Installez l'Agent d'administration. La variable d'environnement KLAUTOANSWERS, qui spécifie le chemin d'accès au fichier de réponse, est transmise à la commande d'installation. Exécutez l'une des commandes suivantes :

   - Pour installer l'Agent d'administration à partir d'un paquet RPM sur un système d'exploitation 32 bits, exécutez la commande suivante :
     `sudo KLAUTOANSWERS=<chemin vers le fichier de réponse> yum install ./klnagent-<numéro de build>.i386.rpm`

   - Pour installer l'Agent d'administration à partir d'un paquet RPM sur un système d'exploitation 64 bits, exécutez la commande suivante :
     `sudo KLAUTOANSWERS=<chemin vers le fichier de réponse> yum install ./klnagent64-<numéro de build>.x86_64.rpm`

   - Pour installer l'Agent d'administration à partir d'un paquet RPM sur un système d'exploitation 64 bits pour l'architecture ARM, exécutez la commande suivante :
     `sudo KLAUTOANSWERS=<chemin vers le fichier de réponse> yum install ./klnagent64-<numéro de build>.aarch64.rpm`

   - Pour installer l'Agent d'administration à partir d'un paquet DEB sur un système d'exploitation 32 bits, exécutez la commande suivante :
     `sudo KLAUTOANSWERS=<chemin du fichier de réponse> apt install ./klnagent_<numéro de build>_i386.deb`

- Pour installer l'Agent d'administration à partir d'un paquet DEB dans un système d'exploitation 64 bits, exécutez la commande suivante :
  ```
  sudo KLAUTOANSWERS=< chemin vers le fichier de réponse > apt install
  ./klnagent64_< numéro de build >_amd64.deb
  ```

- Pour installer l'Agent d'administration à partir d'un paquet DEB sur un système d'exploitation 64 bits pour l'architecture ARM, exécutez la commande suivante :
  ```
  sudo KLAUTOANSWERS=< chemin vers le fichier de réponse > apt install
  ./klnagent64_< numéro de build >_arm64.deb
  ```

Selon la configuration du système d'exploitation, vous pouvez également utiliser les gestionnaires de paquets rpm, dpkg ou dnf pour installer l'Agent d'administration.

L'installation de l'Agent d'administration pour Linux démarre en mode silencieux ; l'utilisateur n'est invité à aucune action pendant le processus.

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.

Avant l'installation de l'Agent d'administration sur l'appareil Linux, il faut réaliser les étapes préparatoires générales requises pour tous les appareils Linux.

Une fois la procédure générale terminée, vous pouvez suivre les instructions supplémentaires, propres à votre système d'exploitation :

- Préparation d'un appareil exécutant SUSE Linux Enterprise Server 15
- Préparation d'un appareil exécutant Astra Linux en mode environnement logiciel fermé
- Préparation d'un appareil exécutant Ubuntu Server/Desktop version 10.04 et 16.04
- Préparation d'un appareil fonctionnant sous le système d'exploitation Linux avec glibc 2.5

Pour installer l'Agent d'administration en mode interactif, procédez comme suit :

1. Installez l'Agent d'administration. En fonction de votre distribution Linux, exécutez l'une des commandes suivantes :

   - Pour installer l'Agent d'administration à partir d'un paquet RPM dans le système d'exploitation 32 bits :
     ```
     # yum -i klnagent-< numéro de build >.i386.rpm
     ```

   - Pour installer l'Agent d'administration à partir d'un paquet RPM dans le système d'exploitation 64 bits :
     ```
     # yum -i klnagent64-< numéro de build >.x86_64.rpm
     ```

   - Pour installer l'Agent d'administration à partir d'un paquet RPM dans le système d'exploitation 64 bits pour architecture Arm :
     ```
     # yum -i klnagent64-< numéro de build >.aarch64.rpm
     ```

- Pour installer l'Agent d'administration à partir d'un paquet DEB dans le système d'exploitation 32 bits :

  ```
  # apt install ./klnagent_<numéro de build>_i386.deb
  ```

- Pour installer l'Agent d'administration à partir d'un paquet DEB dans le système d'exploitation 64 bits :

  ```
  # apt install ./klnagent64_<numéro de build>_amd64.deb
  ```

- Pour installer l'Agent d'administration à partir d'un paquet DEB dans le système d'exploitation 64 bits pour architecture Arm :

  ```
  # apt install ./klnagent64_<numéro de build>_arm64.deb
  ```

2. Configurez l'Agent d'administration :

   ```
   # /opt/kaspersky/klnagent64/lib/bin/setup/postinstall.pl
   ```

3. Lisez le Contrat de licence utilisateur final. 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 par défaut est 14000.

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

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.

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 de l'Agent d'administration pour Windows

Vous pouvez également utiliser le programme d'installation de l'Agent d'administration sur les appareils Windows d'une organisation pour les gérer à l'aide du Serveur d'administration.

Sous Microsoft Windows XP, un Agent d'administration peut ne pas effectuer correctement les opérations suivantes : télécharger les mises à jour directement à partir des serveurs de Kaspersky (comme point de distribution) ; fonctionner comme proxy KSN (comme point de distribution) et détecter les vulnérabilités tierces (si la gestion des vulnérabilités et des correctifs est utilisée).

Avant d'installer l'Agent d'administration sur un appareil fonctionnant sous Microsoft Windows sur l'architecture ARM, assurez-vous qu'aucun Agent d'administration pour Microsoft Windows x86-64 n'est déjà installé. Sinon, l'installation échouera.

Il existe les méthodes suivantes pour installer initialement l'Agent d'administration sur l'appareil administré par Windows :

- En exécutant la tâche d'installation à distance sur le point de distribution Windows.

  Avant de procéder à une installation à distance sur un appareil Windows non défini, un point de distribution Windows vérifie automatiquement le port UDP 137 afin de déterminer le type de système d'exploitation de l'appareil cible. Si le port UDP 137 n'est pas disponible, le point de distribution tente de se connecter au port TCP 445 sur l'appareil cible, ce qui est nécessaire pour effectuer l'installation.

- 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 les paramètres configurés.

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** pour démarrer l'Assistant d'installation de l'Agent d'administration. Suivez les étapes 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 les VM**.

      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.

Si vous souhaitez mettre à niveau l'Agent d'administration à l'aide du programme d'installation de Windows, exécutez la commande suivante :

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
REINSTALL=ALL REINSTALLMODE=vomus /norestart
```

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 de référence, arrêtez le service de l'Agent d'administration et exécutez 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.

- Assurez-vous que l'utilitaire klmover est exécuté avec la clé `-dupfix` avant le premier lancement du service de l'Agent d'administration sur les appareils cibles. Cette opération est obligatoire et doit être effectuée lors du premier lancement 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 suivante dans la ligne de commande Linux :

   ```
   ./klmover -cloningmode 1
   ```

   L'Agent d'administration passe au mode de clonage du disque.
3. Pour connaître l'état actuel du mode de clonage du disque, saisissez la commande suivante dans l'invite de commande :

   ```
   ./klmover -cloningmode
   ```

   La fenêtre de l'utilitaire affiche les informations qui indiquent sur le mode de clonage du disque est activé ou non.

4. Pour désactiver le mode de clonage du disque, saisissez la commande suivante dans la ligne de commande de l'utilitaire :

```
./klmover -cloningmode 0
```

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.	• 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.

Propriété MSI	Description	Valeurs possibles
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 : indiquer un certificat existant. Si cette option est sélectionnée, la propriété CERTFILE doit être définie.
CERTFILE	Chemin d'accès au certificat	Valeur de chaîne.
VMVDI	Activer le mode dynamique pour Virtual Desktop Infrastructure (VDI)	• 1 : activer. • 0 : ne pas activer. • Aucune valeur : ne pas activer.
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.

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 de la 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.

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.

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 **Gestion des ressources** → **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 de la liste**

  Vous pouvez définir les noms DNS, les adresses IP, ainsi que les plages d'adresses IP auxquels il convient d'affecter la tâche.

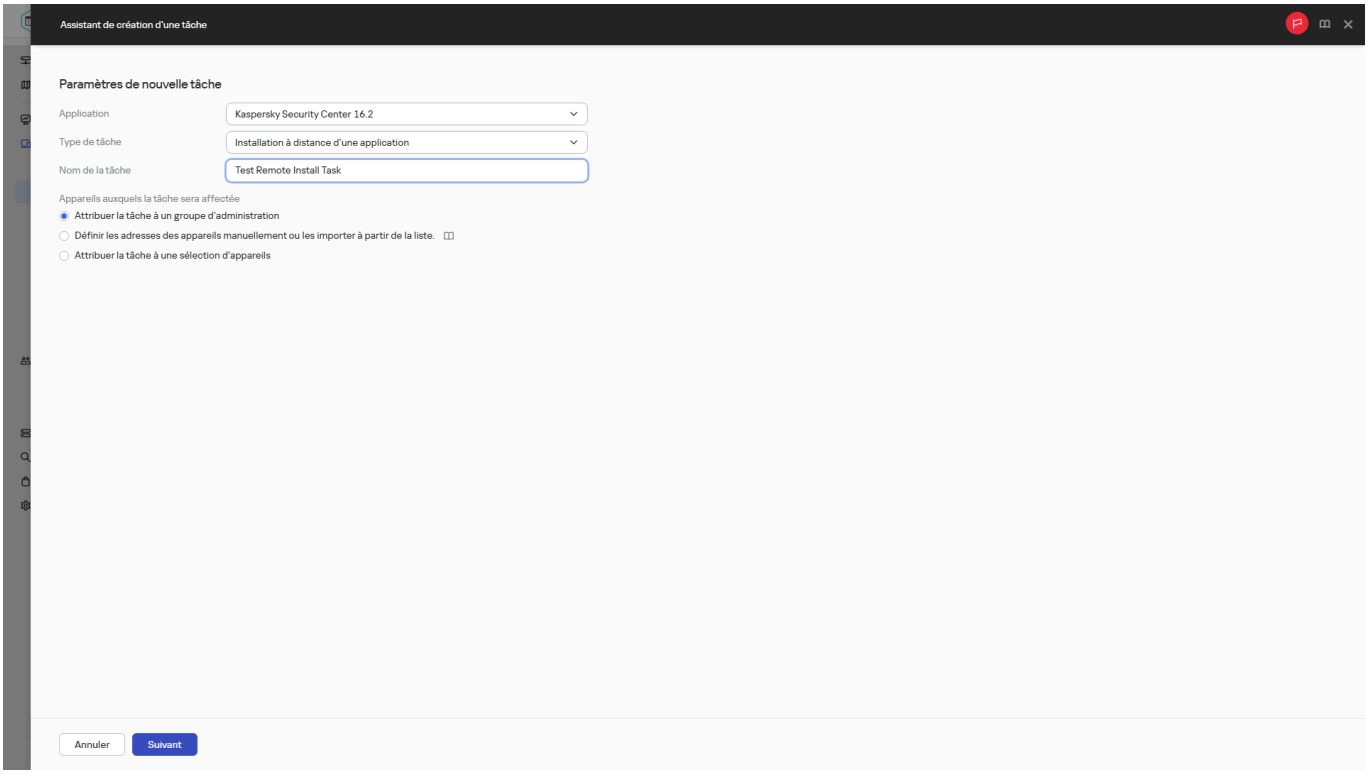
  Vous pourriez utiliser cette option pour exécuter une tâche pour un sous-réseau défini. Par exemple, vous pourriez souhaiter installer une certaine application sur les appareils des comptables ou analyser des appareils dans un sous-réseau qui est probablement infecté.

- **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.



Création de la tâche Installation à distance d'une application

5. À l'étape Zone d' **Zone d'action d'une 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 **Sélectionnez le 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 :

     - **Utilisation de 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 la case est cochée, les paquets d'installation sont fournis aux appareils clients à l'aide des mécanismes du système d'exploitation via un point 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*.

- Si vous passez d'une application Kaspersky à une autre et que votre application actuelle est protégée par un mot de passe, saisissez le mot de passe dans le champ **Mot de passe pour désinstaller l'application Kaspersky actuelle**. Notez que lors de la migration, votre application Kaspersky actuelle sera désinstallée.

  Le champ **Mot de passe pour désinstaller l'application Kaspersky actuelle** n'est accessible que si vous avez sélectionné l'option **Utilisation de l'Agent d'administration** dans le groupe de paramètres **Forcer le téléchargement du paquet d'installation**.

  Vous pouvez utiliser le mot de passe de désinstallation uniquement pour le scénario de migration de Kaspersky Security for Windows Server vers Kaspersky Endpoint Security for Windows lors de l'installation de Kaspersky Endpoint Security for Windows à l'aide de la tâche Installation à distance de l'application. L'utilisation du mot de passe de désinstallation lors de l'installation d'autres modules peut entraîner des erreurs d'installation.

Pour mener à bien la migration, assurez-vous que les conditions préalables suivantes sont remplies :

- Vous utilisez l'Agent d'administration de Kaspersky Security Center 14.2 for Windows ou une version ultérieure.
- Vous installez l'application sur les appareils fonctionnant sous Windows.

- Configurez les paramètres supplémentaires :
  - **Ne pas réinstaller l'application si elle est déjà installée**

    Si l'option est activée, l'application sélectionnée n'est pas installé à nouveau, si l'appareil client en est déjà équipé.

    Si l'option est désactivée, l'application sera malgré tout installée.

    Cette option est activée par défaut.

  - **Vérifier le type de système d'exploitation avant le téléchargement**

    Avant de transmettre les fichiers aux appareils clients, Kaspersky Security Center 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.

    Lorsque vous installez à distance l'Agent d'administration sur des appareils non définis, Kaspersky Security Center Linux ou un point de distribution détermine automatiquement le type de système d'exploitation de l'appareil, quel que soit le paramètre **Vérifier le type de système d'exploitation avant le téléchargement**.

  - **Réparer l'installation du paquet d'installation dans les stratégies de groupe d'Active Directory**

    Si l'option est activée, le paquet d'installation s'installera à l'aide des stratégies de groupes Active Directory.

    L'option est disponible si le paquet d'installation de l'Agent d'administration est sélectionné.

    Cette option est Inactif par défaut.

  - **Demander aux utilisateurs de fermer les applications en cours d'exécution**

    Les applications en cours d'exécution peuvent empêcher le redémarrage de l'appareil client. Par exemple, si un document est en train d'être modifié dans un logiciel de traitement de texte et qu'il n'est pas enregistré, l'application n'autorise pas le redémarrage de l'appareil.

    Quand cette option est activée, l'arrêt forcé de ces applications sur un appareil verrouillé doit avoir lieu avant de pouvoir redémarrer l'appareil. Les utilisateurs pourraient perdre toute modification qui n'a pas été enregistrée à ce moment.

    Si cette option est désactivée, un appareil verrouillé n'est pas redémarré. L'état de la tâche sur cet appareil indique qu'il faut redémarrer l'appareil. Les utilisateurs doivent quitter manuellement toutes les applications en cours d'exécution sur les appareils verrouillés, puis redémarrer ces appareils.

    Cette option est Inactif par défaut.

- Sélectionnez les appareils sur lesquels vous souhaitez installer l'application :
  - **Installer sur tous les appareils**

    L'application est installée même sur les appareils administrés par d'autres Serveurs d'administration.

    Par défaut, cette option est sélectionnée. Vous n'avez pas à modifier ce paramètre si vous n'avez qu'un seul Serveur d'administration sur votre réseau.

  - **Installer uniquement sur les appareils administrés via &ce Serveur d'administration**

    L'application est installée uniquement sur les appareils administrés par ce Serveur d'administration. Sélectionnez cette option si vous avez plus d'un Serveur d'administration dans votre réseau et que vous souhaitez évitez les conflits entre eux.

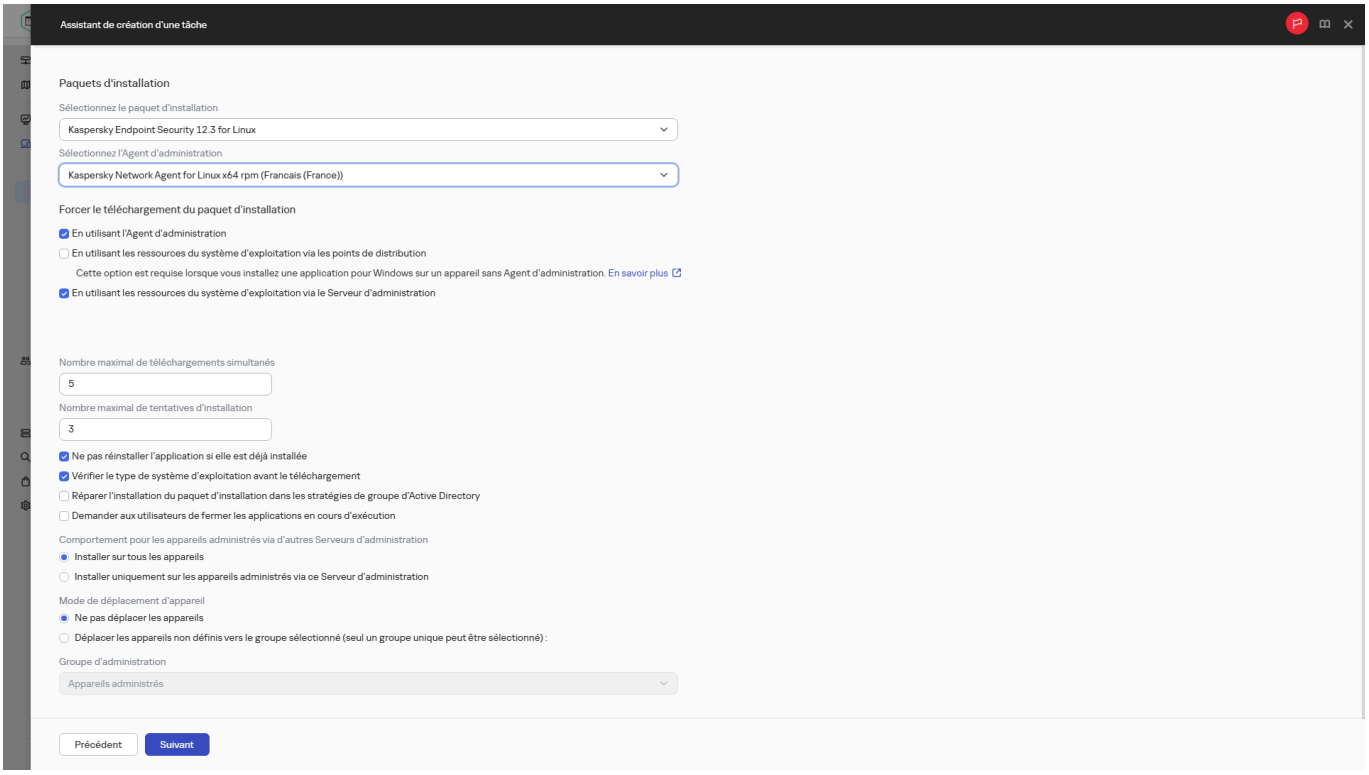
- Spécifiez si les appareils doivent être déplacés vers un groupe d'administration après l'installation :
  - **Ne pas déplacer les appareils**

    Les appareils demeurent dans les groupes où ils se trouvent. Les appareils qui n'ont été placés dans aucun groupe restent non définis.

  - **Déplacer les appareils non définis vers le groupe sélectionné (seul un groupe unique peut être sélectionné)**

    Les appareils sont déplacés vers le groupe d'administration que vous avez sélectionné.

Notez que l'option **Ne pas déplacer les appareils** est sélectionnée par défaut. Pour des raisons de sécurité, envisagez de déplacer les appareils manuellement.



Spécification des paramètres de la tâche

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 à distance des applications sur les appareils macOS

Pour installer des applications sur des appareils exécutant macOS à l'aide de la tâche de programme d'installation à distance, procédez comme suit :

1. Créez une archive constituée d'un paquet d'installation et d'un script d'installation .sh.

2. Dans l'assistant de création d'une tâche, désactivez l'option **Vérifier le type de système d'exploitation avant le téléchargement**.

Vous pouvez également utiliser la tâche **Exécuter des scripts à distance**. L'article suivant décrit la procédure à suivre pour configurer les fichiers pour cette tâche : Installation à distance d'applications sur les appareils à l'aide de la tâche Exécuter des scripts à distance.

Installation des applications sur les Serveurs d'administration secondaires

Si vous disposez de la version 15.4 ou d'une version ultérieure du Serveur d'administration, vous pouvez installer des applications sur un Serveur d'administration secondaire uniquement si celui-ci fonctionne avec la version 15.4 ou une version ultérieure.

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.

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**. 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). 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.

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 est appliquée aux appareils à l'aide des identifiants du compte sous lequel le Serveur d'administration est exécuté. Il est important de préciser qu'il s'agit du compte utilisé pour accéder au partage admin$, et non du compte sous lequel s'exécute la tâche d'installation à distance. L'installation s'effectue sous le compte LocalSystem.

Les appareils peuvent être désignés explicitement (via une liste) soit via la sélection du groupe d'administration de Kaspersky Security Center 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 de partage des accès et de sécurité est défini sur *Classique – 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 /var/opt/kaspersky/KSC_Backups* soit plusieurs fois supérieur au volume total des distributions des applications installées.

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.

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 <nom_de_l'appareil>` pour vous connecter à distance à l'appareil macOS. Dans le volet **Partage**, vous pouvez utiliser l'option **Autoriser l'accès à** pour définir l'étendue des utilisateurs autorisés à accéder à l'appareil macOS.

   b. Désactivez le mot de passe de la demande sudo pour le compte utilisateur utilisé pour la connexion à l'appareil.

      Utilisez la commande `sudo visudo` dans Terminal pour ouvrir le fichier de configuration sudoers. Dans le fichier que vous avez ouvert, dans l'entrée `Spécification des privilèges de l'utilisateur`, indiquez ce qui suit : `username ALL = (ALL) NOPASSWD: ALL`. Dans ce cas, `username` représente le compte utilisateur qui sera utilisé pour établir la connexion à l'appareil à l'aide du protocole SSH.

   c. Enregistrez le fichier sudoers et fermez-le.

   d. Connectez-vous à nouveau à l'appareil via SSH et vérifiez que le service Sudo ne requiert pas de mot de passe à l'aide de la commande `sudo whoami`.
3. Téléchargez et créez le paquet d'installation :
   a. Téléchargez le paquet d'installation de l'Agent d'administration à l'aide de l'une des méthodes suivantes :
      - À l'aide de l'interface de l'application
      - En téléchargeant la version appropriée de l'Agent d'administration depuis le site Internet du Support technique à l'adresse https://support.kaspersky.com/fr/.
      - 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.

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.

Nous vous déconseillons d'activer le chiffrement des disques sur les machines virtuelles dynamiques.

Prise en charge de la copie des machines virtuelles

Copier une machine virtuelle dotée de l'Agent d'administration ou la créer au départ d'un modèle doté de l'Agent d'administration est similaire au déploiement par prise d'une image du disque dur et copie de celui-ci. Pour cette raison, en général, lors de la copie de machines virtuelles, il faut réaliser les mêmes actions que lors du déploiement de l'Agent d'administration par copie d'une image du disque.

Cependant, dans les deux cas décrits ci-après, l'Agent d'administration détecte la copie automatiquement. Il n'est dès lors pas nécessaire d'exécuter les actions complexes décrites dans la section " Déploiement par prise d'image et copie d'image du disque dur de l'appareil " :

- Lors de l'installation de l'Agent d'administration, l'option **Activer le mode dynamique pour VDI** a été sélectionnée : après chaque redémarrage du système d'exploitation, cette machine virtuelle est considérée comme un nouvel appareil, qu'elle ait été copiée ou non.
- Utilisation d'un des hyperviseurs suivants : VMware™, HyperV® ou Xen® : l'Agent d'administration détermine l'opération de copie de la machine virtuelle à l'aide de la modification des indicateurs de la configuration matérielle virtuelle.

L'analyse des modifications de la configuration matérielle virtuelle n'est pas absolument sûre. Avant d'utiliser largement cette méthode, il faut d'abord confirmer son fonctionnement sur un nombre restreint de machines virtuelles pour la version de l'hyperviseur utilisée par l'entreprise.

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 **Gestion des ressources** → **Tâches**.
2. Cliquez sur le nom de la tâche d'installation à distance pour laquelle vous souhaitez spécifier les paramètres propres à Unix.

   La fenêtre de propriétés de la tâche s'affiche.
3. Accédez à **Paramètres de l'application** → **Paramètres propres à Unix**.

4. Définissez les paramètres suivants :

- **Définir un mot de passe pour le compte root (uniquement pour le déploiement via SSH)**

  Si la commande `sudo` ne peut pas être utilisée sur l'appareil cible sans indiquer le mot de passe, sélectionnez cette option, puis indiquez le mot de passe du compte root. Kaspersky Security Center 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.

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.

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 **Gestion des ressources** → **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

Pour supprimer des applications incompatibles à l'aide d'une tâche, utilisez la *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 **À la fin 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

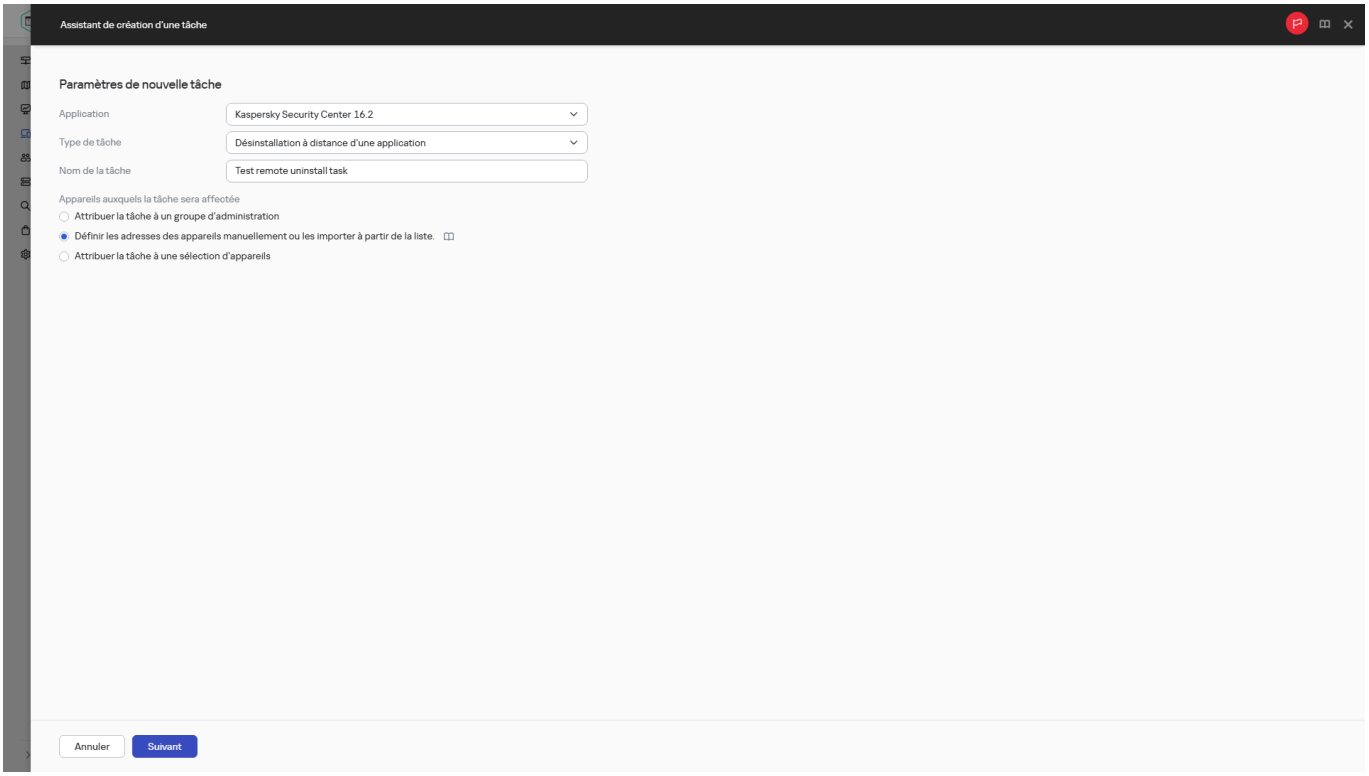
Vous pouvez supprimer des applications ou des mises à jour logicielles sur les appareils administrés qui exécutent Linux à distance uniquement à l'aide de l'Agent d'administration.

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 **Gestion des ressources** → **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.

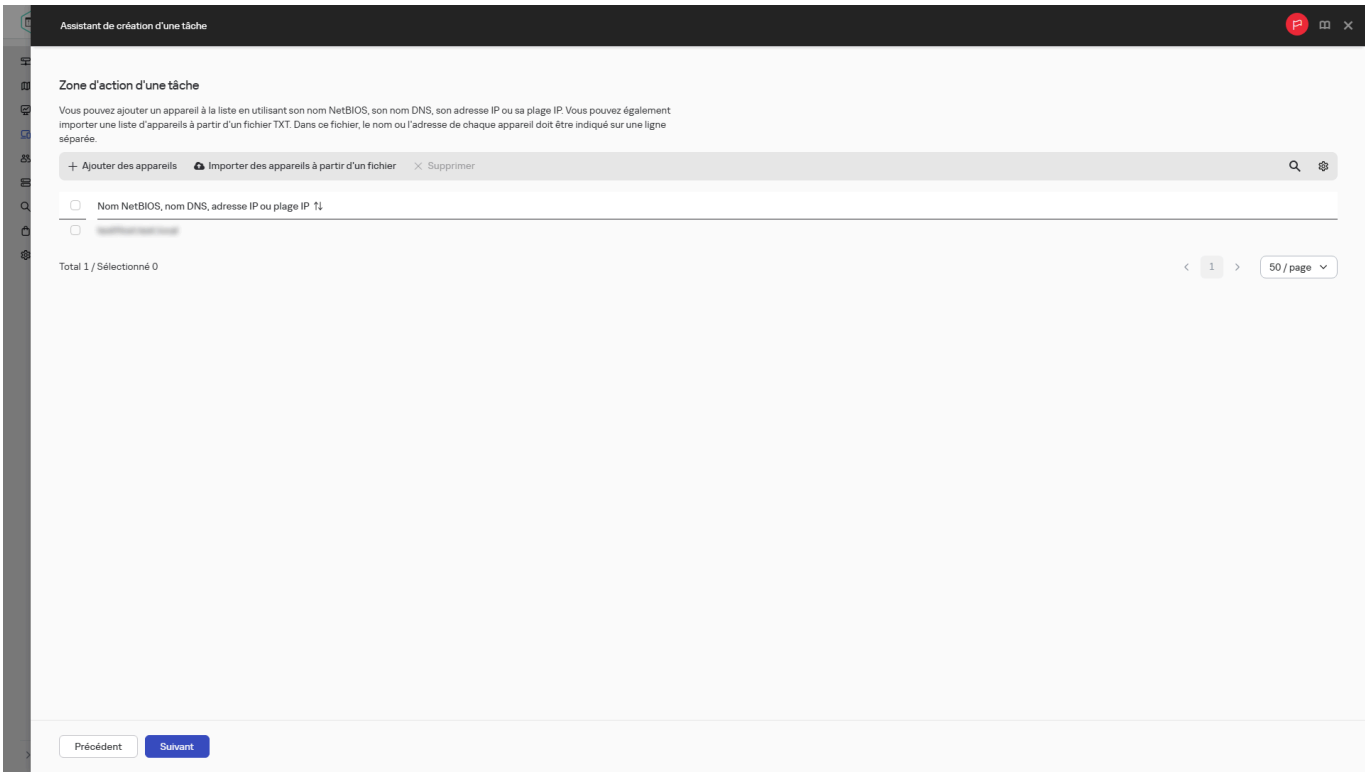
Le nom de la tâche ne peut pas contenir plus de 100 symboles et contenir de symboles spéciaux ("*<>?\:|).



Création de la tâche Désinstallation à distance d'une application

6. Sélectionnez les appareils auxquels les tâches seront affectées.

   Accédez à l'étape suivante de l'Assistant.



Spécification de la zone de la tâche

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 incompatible**

  Une liste des applications incompatibles avec les applications de sécurité Kaspersky ou Kaspersky Security Center Linux s'affiche. Cochez les cases en regard de l'application que vous souhaitez supprimer.

- **Supprimer une application depuis le registre des applications**

  Par défaut, les Agents d'administration envoient au Serveur d'administration des informations à propos des applications installées sur les appareils administrés. La liste des applications installées est stockée dans le registre des applications.

  Pour sélectionner une application dans le registre des applications :

  a. Cliquez sur le champ **Application à désinstaller**, puis sélectionnez l'application que vous souhaitez supprimer.

  Si vous sélectionnez l'Agent d'administration de Kaspersky Security Center, lorsque vous exécutez la tâche, l'état *Terminé avec succès* indique que le processus de suppression a démarré. Si l'Agent d'administration de Kaspersky Security Center est supprimé, l'état ne change pas. Si la tâche échoue, l'état passe à *Échec*.

  b. Précisez les options de désinstallation :

  - **Mode de désinstallation**

    Sélectionnez la manière dont vous souhaitez supprimer l'application :

    - **Définir automatiquement la commande de désinstallation**

      Si l'application dispose d'une commande de désinstallation définie par le fournisseur de l'application, Kaspersky Security Center 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 fait partie du 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 l'application sur un appareil administré dans la limite du nombre d'exécutions du programme d'installation défini par le paramètre, Kaspersky Security Center Linux cesse de distribuer l'utilitaire de désinstallation à cet appareil administré et ne lance 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.

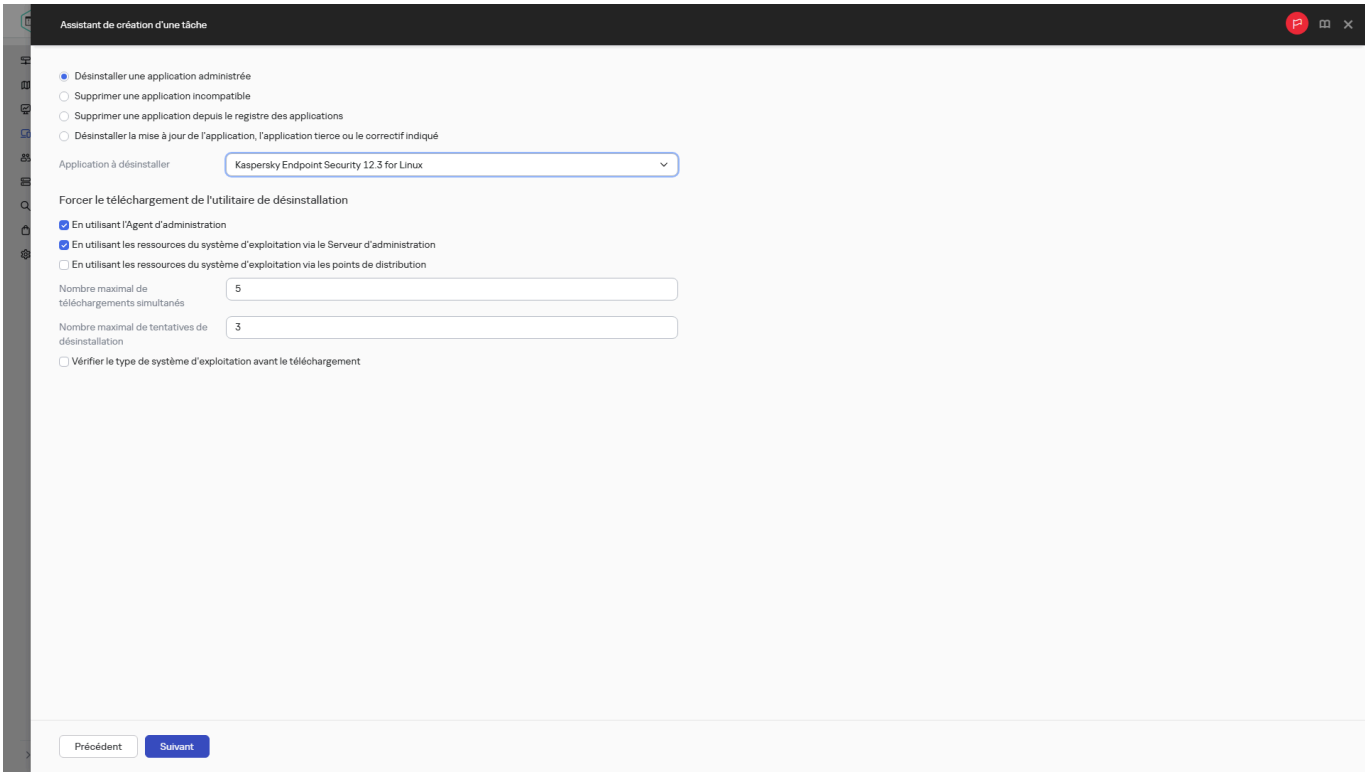
  Si le nombre de tentatives paramétré est dépassé et que l'appareil est prêt pour la désinstallation de l'application, vous pouvez augmenter la valeur du paramètre **Nombre maximal de tentatives de désinstallation** et lancer la tâche de désinstallation de l'application. Sinon, vous pouvez aussi créer 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.

Lorsque vous installez à distance l'Agent d'administration sur des appareils non définis, Kaspersky Security Center Linux ou un point de distribution détermine automatiquement le type de système d'exploitation de l'appareil, quel que soit le paramètre **Vérifier le type de système d'exploitation avant le téléchargement**.

Accédez à l'étape suivante de l'Assistant.



Spécification des paramètres de la tâche

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 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. Si, à l'étape **Fin de la création de la tâche** de l'Assistant, vous activez l'option **Ouvrir les détails de la tâche à la fin de la création**, vous pouvez modifier les paramètres par défaut de la tâche.

    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.

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 **Gestion des ressources** → **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 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.

Création de la tâche Exécuter des scripts à distance

Vous pouvez créer une tâche *Exécuter des scripts à distance* pour exécuter un paquet d'installation sur un appareil client et pour installer une application à distance.

Un paquet d'installation contient une archive ZIP avec un ensemble de scripts à exécuter sur les appareils clients, ainsi qu'un fichier manifest.json. Apprenez-en plus à propos de la création de ce type de paquet d'installation dans cet article.

Cette tâche doit être démarrée uniquement sur les appareils dotés de l'Agent d'administration pour Linux.

Pour démarrer une tâche Exécuter des scripts à distance, procédez comme suit :

1. Accédez à l'**Assistant de création d'une tâche** et sélectionnez le type de tâche **Exécuter des scripts à distance**.

2. Saisissez le nom de la tâche et sélectionnez les appareils auxquels la tâche sera affectée. Cliquez sur **Suivant**.

3. Sélectionnez un paquet d'installation basé sur une archive ZIP avec un fichier manifest.json pour une exécution à distance.

   Si vous ne souhaitez pas ré-exécuter la tâche sur les appareils où elle est déjà terminée, activez l'option **Ne pas lancer cette tâche sur des appareils sur lesquels elle a déjà été effectuée**.

4. Sélectionnez un compte pour exécuter la tâche.

   Si vous sélectionnez le compte par défaut, la tâche sera exécutée par l'Agent d'administration (compte root).

   Vous ne pouvez pas modifier le compte qui lui est attribué lorsque la tâche *Exécuter des scripts à distance* démarre. Pour modifier le compte utilisateur auquel la tâche est attribuée, il faut arrêter la tâche dans les paramètres de la tâche et la créer de nouveau avec les bons détails du compte.

5. Si vous souhaitez modifier les paramètres de la tâche par défaut, activez l'option **Ouvrir les détails de la tâche à la fin de la création** sur la page **Fin de la création de la tâche**. Si vous n'activez pas cette tâche, la tâche est créée selon les paramètres par défaut. Vous pourrez modifier ces paramètres par défaut plus tard, à tout moment.

6. Cliquez sur le bouton **Terminer**.

   La tâche *Exécuter des scripts à distance* est créée et s'affiche dans la liste des tâches.

Après avoir reçu des données de la tâche *Exécuter des scripts à distance*, l'Agent d'administration restreint l'accès aux données reçues pour tous les utilisateurs, sauf pour l'administrateur et pour l'utilisateur spécifié dans les paramètres de la tâche.

Création d'un paquet d'installation sur la base d'un fichier manifeste

Pour créer un paquet d'installation sur la base d'un fichier manifeste, procédez comme suit :

1. Exécutez une des actions suivantes :

   - Dans le menu principal, accédez à **Découverte et déploiement** → **Déploiement et attribution** → **Paquets d'installation**.
   - Dans le menu principal, accédez à **Opérations** → **Stockages** → **Paquets d'installation**.

   Une liste des paquets d'installation disponibles sur le Serveur d'administration s'affiche.

2. Cliquez sur **Ajouter**.

   L'Assistant de création du paquet d'installation se lance. Parcourez les étapes de l'Assistant à l'aide du bouton **Suivant**.

3. Sélectionnez **Créer un paquet d'installation pour la tâche Exécuter des scripts à distance à partir d'une archive ZIP avec un fichier manifest.json**.

4. Définissez le nom du paquet et cliquez sur le bouton **Parcourir**.

   Dans la fenêtre qui s'ouvre, choisissez un fichier pour créer le paquet d'installation.

5. Sélectionnez un fichier d'archive situé sur les disques disponibles. Découvrez comment préparer une archive pour cette tâche dans cet article.

   Le chargement du fichier sur le Serveur d'administration Kaspersky Security Center Linux commence.

   Le processus de création du paquet d'installation se lance.

   L'Assistant vous informe lorsque le processus est terminé.

   Si le paquet d'installation n'est pas créé, un message approprié s'affiche.

6. Cliquez sur le bouton **Terminer** pour fermer l'Assistant.

Le paquet d'installation que vous avez créé est téléchargé dans le sous-dossier Paquets du dossier partagé du Serveur d'administration. Après le téléchargement, le paquet d'installation apparaît dans la liste des paquets d'installation.

Dans la liste des paquets d'installation d'un Serveur d'administration, vous pouvez cliquer sur le lien portant le nom d'un paquet d'installation personnalisé pour :

- Afficher les propriétés suivantes d'un paquet d'installation :
  - **Nom.** Nom du paquet d'installation personnalisé.
  - **Source.** Nom du fournisseur de l'application.
  - **Version.** Version de l'application.
  - **Date de création.** Date de création du paquet d'installation.
  - **Date de modification.** Date de modification du paquet d'installation.
  - **Chemin.** Chemin d'accès au paquet d'installation personnalisé sur le Serveur d'administration.
- Modifiez le nom de l'archive et les paramètres de ligne de commande. Cette fonctionnalité n'est disponible que pour les paquets qui ne sont pas créés sur la base des applications Kaspersky.

Préparation d'une archive pour la tâche Exécuter des scripts à distance

L'archive pour la tâche *Exécuter des scripts à distance* basée sur un fichier manifest.json doit remplir les conditions suivantes :

- Format d'archive : ZIP.
- Taille totale : pas plus de 1 Go.
- Le nombre de fichiers et de dossiers dans l'archive est illimité.
- Le fichier manifeste de l'archive doit correspondre au schéma ci-dessous et être nommé manifest.json. Le schéma est validé uniquement lors de l'exécution de la tâche sur l'appareil.

  Schéma JSON du fichier manifeste et description des tableaux

  Schéma JSON

```
{
 "$schema": "http://json-schema.org/draft-07/schema#",
  "title": "Schema for execute scripts task",
   "type": "object",
    "properties": {
        "version": {
            "type": "integer",
            "enum": [1]
        },
        "actions":{
            "type": "array",
```

```
            "items": {
                "type": "object",
                "properties": {
                    "type": {
                        "type": "string",
                        "enum": ["execute"]
                    },
                    "path": {
                        "type": "string"
                    },
                    "args": {
                        "type": "string"
                    },
                    "results":{
                        "type": "array",
                        "items": {
                            "type": "object",
                            "properties": {
                                "code": {
                                    "type": "integer",
                                    "minimum": -255,
                                    "maximum": 255
                                },
                                "next":{
                                    "type": "string",
                                    "enum": ["break", "continue"]
                                }
                            },
                            "required": [
                                "code",
                                "next"
                            ]
                        }
                    },
                    "default_next":{
                        "type": "string",
                        "enum": ["break", "continue"]
                    }
                },
                "required": [
                    "type",
                    "path",
                    "default_next"
                ]
            }
        }
    },
    "required": [
        "version",
        "actions"
    ]
}
```

Exemple de fichier manifeste

```
{
  "version": 1,
  "actions": [
```

```
    {
      "type": "execute",
      "path": "scripts/run1.cmd",
      "args": "testArg",
      "results": [
        {
          "code": 0,
          "next": "continue"
        }
      ],
      "default_next": "break"
    },
    {
      "type": "execute",
      "path": "scripts/run2.cmd",
      "results": [
        {
          "code": 0,
          "next": "continue"
        }
      ],
      "default_next": "break"
    },
    {
      "type": "execute",
      "path": "scripts/run3.cmd",
      "results": [
        {
          "code": 0,
          "next": "continue"
        }
      ],
      "default_next": "break"
    }
  ]
}
```

- L'archive doit être structurée comme suit :

```
manifest.json
<file1>
<file2>
<folder1>/<file3>
<folder2>/<folder3>/<file4>
...
<fileX>
```

`manifest.json` est le fichier manifeste de la tâche.

`<file1>`, ..., `<fileX>` constituent l'ensemble des fichiers contenant les scripts à exécuter.

Installation à distance d'applications sur les appareils à l'aide de la tâche Exécuter des scripts à distance

La tâche *Exécuter des scripts à distance* peut être utilisée pour installer à distance une application sur un appareil client en créant un paquet d'installation personnalisé.

Découvrez comment préparer une archive pour cette tâche dans cet article.

Pour créer le paquet d'installation en vue de l'installation à distance d'une application sur un appareil client, les fichiers suivants doivent figurer dans l'archive à charger pour cette tâche :

- `<nom du paquet>`.deb
- **install.sh**

  ```
  sudo apt-get install <nom du paquet>.deb
  ```

- **manifest.json**

  ### Schéma JSON pour l'installation à distance d'une application

  ```
  {
    "version": 1,
    "actions": [
      {
        "type": "execute",
        "path": "install.sh",
        "args": "<saisissez les arguments, si nécessaire>",
        "results": [
          {
            "code": 0,
            "next": "continue"
          }
        ],
        "default_next": "break"
      }
    ]
  }
  ```

  ### Description des tableaux

  1. `version` : version du fichier manifeste et de la tâche.

     Pour le moment, la seule valeur acceptable est 1.

  2. Les éléments du tableau `actions` déterminent la composition et l'ordre des scripts exécutés dans la tâche.

     L'ordre d'exécution du script correspond à l'index (place) de l'élément dans le tableau.

  3. Pour chaque élément du tableau `actions`, les éléments suivants sont définis.

     a. `type` : type de la commande exécutable issue des scripts. Pour le moment, la valeur est toujours `execute`.

     b. `path` : chemin d'accès au fichier script dans l'archive.

c. `args` : arguments transmis au script dans le cadre de l'exécution de la commande.

d. `results` : tableau qui définit les actions supplémentaires en fonction du résultat de la tâche.

1. `code` : valeur qui retourne un script.

2. `next` : action à terminer ensuite. L'action `continue` lance l'exécution du script suivant (élément du tableau `actions`). L'action `break` arrête la tâche.

e. `default_next` : action si le script renvoie une valeur non contenue dans les `results`.

Au démarrage de la tâche *Exécuter des scripts à distance*, l'Agent d'administration charge le paquet d'installation avec l'application sur l'appareil client. Lorsque l'appareil client reçoit le paquet d'installation, l'Agent d'administration sur cet appareil analyse le fichier manifest.json et définit l'ordre d'exécution des scripts et des actions en fonction du résultat, puis démarre l'exécution.

Lorsque la tâche *Exécuter des scripts à distance* est terminée, l'application est installée sur l'appareil client.

Configuration des notifications et de la surveillance de la tâche Exécuter des scripts à distance

Vous pouvez configurer la surveillance, le comportement d'enregistrement des événements et les notifications pour la tâche *Exécuter des scripts à distance*.

Pour consulter l'état de la tâche Exécuter des scripts à distance, procédez comme suit :

1. Dans le menu principal, accédez à **Gestion des ressources** → **Tâches**.

   La liste des tâches s'affiche.

2. Sélectionnez la tâche et cliquez sur **Historique de l'appareil**.

   La progression de la tâche s'affiche.

Pour configurer le comportement d'enregistrement des événements, procédez comme suit :

1. Dans la liste des tâches, cliquez sur la tâche et accédez à l'onglet **Configuration**.

2. Dans la section **Notifications**, cliquez sur le bouton **Configuration**.

3. Choisissez une des options suivantes en fonction du comportement de l'application à l'issue de la tâche :

   - **Sauvegarder tous les événements**.

   - **Sauvegarder les événements relatifs au déroulement des tâches**.

   - **Sauvegarder uniquement le résultat de la tâche**.

     Les événements sont enregistrés dans l'**Historique de l'appareil** et le **Stockage d'événements**.

     Par défaut, seuls les résultats d'exécution de la tâche sont enregistrés.

Si vous sélectionnez **Sauvegarder tous les événements**, seuls les résultats d'exécution de la tâche seront enregistrés.

4. Si vous souhaitez conserver les événements dans la base de données du Serveur d'administration, dans le journal des événements sur le Serveur d'administration ou sur l'appareil, activez l'option correspondante.

Apprenez-en plus à propos de la configuration des notifications dans cet article.

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, 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 que Kaspersky Security Center continue de fonctionner, vous devez renouveler votre licence commerciale. Après l'expiration de la licence, vous ne pouvez plus utiliser l'application et devez la supprimer de l'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 fourni avec un fichier clé ou un code d'activation.

Le certificat de licence contient les informations suivantes sur la licence accordée :

- Identifiant de licence ou numéro de commande
- informations relatives à l'utilisateur qui reçoit la licence
- informations relatives à l'application qui peut être activée à l'aide de la licence
- restrictions associées au nombre d'unités concernées par la licence (par exemple, le nombre d'appareils sur lesquels l'application peut être utilisée avec la licence)
- date de début de la 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 peut fonctionner dans les modes suivants :

- **Fonctionnalité de base de la Console d'administration**

  Kaspersky Security Center fonctionne dans ce mode avant l'activation de l'application ou après l'expiration de la licence commerciale. Kaspersky Security Center avec la prise en charge de la fonctionnalité de base de la Console d'administration est livré parmi les applications de Kaspersky conçues pour la protection des réseaux de l'entreprise. Il peut également être téléchargé depuis le site Internet de Kaspersky.

- **Licence commerciale**

  Si vous avez besoin de fonctionnalités supplémentaires qui ne sont pas comprises dans les fonctionnalités de base de la Console d'administration, vous devez acheter une licence commerciale.

  Lors de l'ajout d'une clé de licence dans la fenêtre des propriétés du Serveur d'administration, assurez-vous d'ajouter une clé de licence qui vous permet d'utiliser Kaspersky Security Center Linux. Vous pouvez trouver ces informations sur le site Internet de Kaspersky. Chaque page Internet de solution contient la liste des applications incluses dans cette solution. Le Serveur d'administration peut accepter des clés de licence non prises en charge, par exemple une clé de licence pour Kaspersky Endpoint Security Cloud, mais ces clés de licence n'offrent pas de nouvelles fonctionnalités en plus des fonctionnalités de base de la Console d'administration.

Fonctionnalité ou propriété	Mode de fonctionnement de Kaspersky Security Center Linux	
	Licence manquante	Licence commerciale
Fonctionnalité de base de la Console d'administration Les fonctions suivantes sont disponibles : • Création des Serveurs d'administration virtuels pour administrer le réseau des offices à distance et des entreprises clientes. • Formation d'une hiérarchie des groupes d'administration pour administrer l'ensemble d'appareils comme un tout unique. • Installation à distance des applications. • Configuration centralisée des paramètres des applications installées sur les appareils clients. • Contrôle d'état de sécurité antivirus de l'entreprise. • Administration des rôles des utilisateurs. • Réception des statistiques et des rapports sur le fonctionnement des applications, ainsi que la réception des notifications sur les événements critiques. • Travail centralisé avec les fichiers placés en quarantaine ou dans la sauvegarde, et avec les fichiers dont le traitement est différé. • Administration du processus de chiffrement et de protection des données. • Consultation et modification manuelle de la liste du matériel détecté suite au sondage du réseau. • Consultation de la liste des images des systèmes d'exploitation accessibles à l'installation à distance.	✓	✓

Fonctionnalité ou propriété	Mode de fonctionnement de Kaspersky Security Center Linux	
	Licence manquante	Licence commerciale
Gestion des vulnérabilités et des correctifs : fonctionnalité de base Les tâches suivantes ne requièrent pas de licence commerciale : • Tâche *Recherche de vulnérabilités et de mises à jour requises* Grâce à cette tâche, Kaspersky Security Center Linux reçoit la liste des vulnérabilités détectées et des mises à jour requises pour les logiciels tiers installés sur les appareils administrés. • La tâche *Corriger les vulnérabilités* La tâche *Corriger les vulnérabilités* utilise les correctifs recommandés pour les logiciels Microsoft et les correctifs utilisateur pour les logiciels tiers. Pour utiliser cette tâche, vous devez spécifier manuellement les correctifs utilisateur pour les vulnérabilités dans les paramètres de la tâche.	✓	✓
Gestion des vulnérabilités et des correctifs : fonctionnalité avancée Vous pouvez définir les règles pour l'installation à distance automatique des mises à jour logicielles et la correction automatique des vulnérabilités.	—	✓
Administration des systèmes Les fonctions suivantes sont disponibles : • Permission à distance de la connexion aux appareils clients via un module de Microsoft® Windows® nommé Remote Desktop Connection. • Connexion à distance aux appareils clients à l'aide du Partage du bureau Windows.	—	✓
Exportation des événements dans les systèmes SIEM via le protocole Syslog Le protocole Syslog permet de transmettre n'importe quel événement survenu sur le Serveur d'administration de Kaspersky Security Center et dans les applications de Kaspersky installées sur les appareils administrés. Le protocole Syslog est un protocole standard d'enregistrement de messages. Vous pouvez l'utiliser pour exporter des événements vers n'importe quel système SIEM.	✓	✓
Agrégation des alertes et exécution des actions de réponse via Active Directory, KASAP et Kaspersky TIP Sandbox	—	✓

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.

Si le fichier clé a été accidentellement supprimé, vous pouvez le restaurer. Le fichier clé peut vous être utile pour vous inscrire sur Kaspersky CompanyAccount, par exemple.

Pour restaurer le fichier clé, vous devez effectuer l'une des opérations suivantes :

- Contactez le fournisseur de licences.
- Obtenez un fichier clé sur le site Internet de Kaspersky à partir du code d'activation disponible.

À propos de la collecte des données

Données fournies à des tiers

Le service Administration des appareils mobiles est utilisé lors de l'utilisation de la fonctionnalité d'administration des appareils mobiles du Logiciel afin de fournir en temps voulu des commandes aux appareils exécutant le système d'exploitation Android via le mécanisme de notification push. Si l'utilisateur a configuré l'utilisation du service Google Firebase Cloud Messaging, il accepte de fournir les informations suivantes au service Google Firebase Cloud Messaging en mode automatique :

- Identifiant de l'instance
- Identifiant du logiciel dans le service Google Firebase Cloud Messaging
- Version du logiciel installé
- Version complète du logiciel
- Version Google Play
- Nom de la distribution du logiciel
- Version du schéma pour les données fournies
- Version du système d'exploitation
- Identifiant du logiciel

Pour bloquer l'échange d'informations avec le service Google Firebase Cloud Messaging, l'Utilisateur doit rétablir les paramètres d'utilisation du service Google Firebase Cloud Messaging à leurs valeurs d'usine.

Le service Apple Push Notification Service (APNs) est utilisé lors de l'utilisation de la fonctionnalité d'administration des appareils mobiles du Logiciel afin de fournir en temps voulu des commandes aux appareils exécutant le système d'exploitation iOS via le mécanisme de notification push. Si l'Utilisateur a installé un certificat APNs sur un Serveur MDM iOS, créé un profil MDM iOS avec une série de paramètres pour la connexion des appareils mobiles iOS au Logiciel et installé ce profil sur ses appareils mobiles, l'Utilisateur accepte de fournir les informations suivantes à APNs en mode automatique :

- Jeton : jeton push de l'appareil. Le serveur utilise ce jeton lors de l'envoi de notifications push à l'appareil.
- PushMagic : chaîne qui doit être incluse dans la notification push. La valeur de chaîne est générée par l'appareil.

Données transférées à AO Kaspersky Lab

Si l'Utilisateur dispose de la fonctionnalité de Kaspersky Extended Detection and Response Optimum, Kaspersky Security Center Linux transfère les données dans les cas suivants :

- Pour attribuer une formation à un employé, Kaspersky Security Center Linux transfère les données suivantes à Kaspersky Automated Security Awareness Platform (KASAP) : adresse email de l'utilisateur, adresse email secondaire de l'utilisateur (le cas échéant), identifiant de l'utilisateur dans KASAP, identifiant du groupe de formation.

- Pour exécuter automatiquement un fichier à l'aide de Kaspersky Cloud Sandbox, l'application administrée transfère les fichiers placés en quarantaine depuis le Serveur d'administration à l'aide de l'Agent d'administration, puis vers Kaspersky Cloud Sandbox à l'aide de Kaspersky Security Center Web Console. Kaspersky Cloud Sandbox analyse le fichier ainsi que tous les fichiers susceptibles d'être créés pendant son exécution.

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
- Gestion des mises à jour pour Kaspersky et des applications tierces, recherche et correction des vulnérabilités
- Activation des applications de Kaspersky sur les appareils
- Administration des comptes utilisateurs
- Affichage des informations sur le fonctionnement des applications Kaspersky sur les appareils
- Affichage des rapports
- Intégration aux services de Kaspersky

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, Samba, FreeIPA et ALD Pro) ou l'analyse des intervalles IP. Le Serveur d'administration obtient des données indépendamment ou reçoit des données de l'Agent d'administration.

- Informations provenant des contrôleurs de domaine (Active Directory, Samba, FreeIPA et ALD Pro) 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, localisation réseau, adresse MAC, numéro de série, type de système d'exploitation, si l'appareil est une machine virtuelle avec le type d'hyperviseur et si l'appareil est une machine virtuelle dynamique dans le cadre de VDI.

  - Autres spécifications des appareils administrés et de leurs modules requis pour l'audit des appareils administrés et la prise de décision concernant l'application de mises à jour et de correctifs particuliers : 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.

- Données nécessaires à la connexion des appareils mobiles au Serveur d'administration : certificat, port de connexion mobile, adresse de connexion au Serveur d'administration. L'Utilisateur saisit les données dans Kaspersky Security Center Web Console.

- Détails des appareils mobiles transférés via le protocole mobile. Les données répertoriées ci-dessous sont transférées à partir de l'appareil mobile vers le Serveur d'administration :

  - Informations sur l'application : nom de l'application, version complète de l'application, date et heure d'installation de l'application, état de la protection en temps réel de l'appareil, identifiant de la session.

  - Informations sur les clés de licence utilisées par l'application : numéro de série et type de clé licence, état de la clé de licence, période de validité de la clé de licence en jours, dates de génération et d'expiration de la clé de licence, nom de l'entreprise à laquelle la licence a été fournie, informations supplémentaires en cas d'utilisation d'un abonnement (drapeau d'abonnement, date d'expiration et nombre de jours disponibles pour le renouvellement de l'abonnement, adresse Internet du fournisseur de l'abonnement, et état actuel de l'abonnement et cause de l'obtention de cet état), date et heure auxquelles l'application a été activée sur l'appareil, date et heure d'expiration de la licence sur l'appareil.

  - Informations sur l'appareil administré : nom de l'appareil, identifiant de l'appareil, type d'appareil, IMEI de l'appareil (si disponible), numéro de série de l'appareil (si disponible), fabricant de l'appareil, nom de famille du processeur de l'appareil, empreinte du certificat du propriétaire de l'appareil, type de système d'exploitation, version du système d'exploitation, nom du système d'exploitation, espace disque total sur l'appareil, nom du serveur auquel l'appareil appartient, adresse IP de l'appareil, nom du groupe de l'appareil, nom distinctif de l'utilisateur, nom distinctif du domaine, mot de passe à usage unique ou mot de passe de domaine.

  - Informations sur le résultat de l'exécution des commandes personnalisées : identifiant de la commande, état d'exécution de la commande, résultat de l'exécution de la commande ; pour la commande de localisation de l'appareil : latitude, longitude, altitude et vitesse de déplacement de l'appareil ; pour la commande photo furtive : photos prises par la caméra frontale de l'appareil mobile lors de la tentative de déverrouillage.

  - Informations sur l'analyse des appareils : date et heure de la dernière analyse des appareils ; chemin complet dans le système de fichiers à partir duquel l'analyse a démarré ; nombre d'objets analysés ; nombre d'objets malveillants détectés ; nombre d'objets bloqués, supprimés et désinfectés ; nombre d'objets qui n'ont pas pu être désinfectés ; nombre d'erreurs de validation ; nombre de processus interrompus.

  - Informations sur le fonctionnement de chaque composant de l'application et sur l'exécution de chaque tâche, présentées sous forme d'événements :

    - Identifiant de l'événement

    - Gravité

    - Nom et type d'événement.

    - Description de la cause de l'événement.

    - Date et heure auxquelles l'événement s'est produit.

    - Informations sur les événements liés au fonctionnement de l'Antivol (code de déverrouillage de l'appareil, coordonnées de l'appareil, mode de transmission de la commande, liste des données supprimées).

    - Résultats du traitement d'un objet ou d'une action détectés (nom du fichier sur l'appareil ; nom de l'application ; nom de la menace ; type de menace ; type d'action effectuée avec le fichier ; résultat de l'action ; code d'erreur, en cas d'occurrence).

    - Informations sur la règle de conformité déclenchée (critère de la règle ; action appliquée ; description de l'erreur lors de l'application de l'action, en cas d'occurrence).

    - Informations sur l'erreur de fonctionnement de l'application (version de l'application, version du système d'exploitation, nom de l'appareil, description de l'erreur).

    - Informations sur l'erreur de Samsung KNOX (code d'erreur, URL à partir de laquelle le fichier n'a pas pu être téléchargé).
    - Informations sur les autorisations accordées à l'application.
    - Informations sur chacune des applications installées sur l'appareil administré (nom de l'application, état de l'installation).
    - Informations sur l'acceptation globale du Contrat de licence utilisateur final : identifiant du CLUF, horodatage du CLUF, texte du CLUF.
    - Paramètres du service Google Firebase Cloud Messaging : identifiant de l'expéditeur, identifiant d'enregistrement de l'appareil.
  - Informations sur l'adresse IP publique de l'appareil.
- Détails des appareils mobiles transférés via le protocole MDM iOS. Les données répertoriées ci-dessous sont transférées à partir de l'appareil mobile vers le Serveur d'administration :
  - Caractéristiques techniques de l'appareil mobile et de ses modules requis pour l'identification de l'appareil : nom l'appareil, modèle, nom du système d'exploitation, numéro de version du système d'exploitation, numéro de modèle de l'appareil, numéro IMEI, numéro de téléphone, UDID, MEID, numéro de série, quantité de mémoire pleine et disponible, version du firmware du modem, adresse MAC Bluetooth, adresse MAC Wi-Fi et détails de la carte SIM (ICCID en tant que partie de l'ID de carte SIM).
  - Détails du réseau mobile utilisé par l'appareil administré : type de réseau mobile, nom du réseau mobile en cours d'utilisation, nom du réseau mobile domestique, version des paramètres d'opérateur du réseau mobile, état de l'itinérance des appels et de l'itinérance des données, code de pays du réseau domicile, code de pays de résidence, code pays du réseau en cours d'utilisation et niveau de chiffrement.
  - Paramètres de sécurité de l'appareil mobile : utilisation du mot de passe et conformité avec les paramètres de la stratégie, liste des certificats installés, des applications et des profils de configuration.
  - Date et heure de la dernière synchronisation avec le Serveur d'administration et état de l'administration de l'appareil.
- Détails des données de l'appareil mobile transférées à l'aide du protocole WebRTC : image d'écran de l'appareil.
- Détails des fichiers à transférer vers les appareils mobiles. L'Utilisateur saisit les données dans l'interface de 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.
- Données nécessaires à l'intégration de Kaspersky Security Center Linux avec un système SIEM pour l'exportation d'événements. L'Utilisateur saisit les données dans Kaspersky Security Center Web Console.
- Données requises pour intégrer Kaspersky Security Center Linux aux contrôleurs de domaine (Active Directory, Samba, FreeIPA et ALD Pro). L'Utilisateur saisit les données dans Kaspersky Security Center Web Console.
- Fichiers keytab pour la connexion à l'aide de l'authentification unique (SSO) Kerberos. L'Utilisateur saisit les données dans Kaspersky Security Center Web Console.
- Données nécessaires à la configuration de la connexion au serveur proxy pour la connexion Internet. L'Utilisateur saisit les données dans Kaspersky Security Center Web Console.
- 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 ou macOS, il envoie au Serveur d'administration les informations suivantes sur le matériel de l'appareil, si ces informations sont fournies par le système d'exploitation :

  - Volume total de mémoire vive
  - Volume total des appareils de stockage de masse
  - Carte mère
  - Processeur
  - Adaptateurs réseau

- Détails relatifs aux applications et aux correctifs installés sur les appareils administrés (registre des applications). Le logiciel peut être comparé aux informations sur les fichiers exécutables détectées sur les appareils par la fonction Contrôle des applications.
- Détails des vulnérabilités du logiciel tiers détectées sur les appareils administrés.
- Détails des mises à jour disponibles pour les applications tierces installées sur les appareils administrés.

- Données requises pour télécharger les mises à jour sur le Serveur d'administration isolé afin de corriger les vulnérabilités des logiciels tiers sur les appareils administrés. L'utilisateur saisit et transmet les données à l'aide de l'utilitaire klsclag du Serveur d'administration.
- 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.
- Détails des fichiers placés dans la Sauvegarde. L'application administrée transfère les données de l'appareil vers le Serveur d'administration via l'Agent d'administration. Une liste complète des données est fournie dans les fichiers d'aide de l'application correspondante.
- Détails des fichiers placés en Quarantaine. L'application administrée transfère les données de l'appareil vers le Serveur d'administration via l'Agent d'administration. Une liste complète des données est fournie dans les fichiers d'aide de l'application correspondante.
- Détails des fichiers demandés par les spécialistes de Kaspersky pour une analyse détaillée. L'application administrée transfère les données de l'appareil vers le Serveur d'administration via l'Agent d'administration. Une liste complète des données est fournie dans les fichiers d'aide de l'application correspondante.
- Détails de l'état et du déclenchement des règles de Contrôle évolutif des anomalies. L'application administrée transfère les données de l'appareil vers le Serveur d'administration via l'Agent d'administration. Une liste complète des données est fournie dans les fichiers d'aide de l'application correspondante.
- Détails des appareils externes (unités de mémoire, outils de transfert d'informations, outils de copie papier des informations et bus de connexion) installés ou connectés à l'appareil administré et détectés par la fonctionnalité Contrôle des appareils. L'application administrée transfère les données de l'appareil vers le Serveur d'administration via l'Agent d'administration. Une liste complète des données est fournie dans les fichiers d'aide de l'application correspondante.

- Informations sur les appareils 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.

- 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. Une liste complète des données est fournie dans les fichiers d'aide de l'application correspondante.

- Liste des contrôleurs logiques programmables (PLC) administrés. L'application administrée transfère les données de l'appareil vers le Serveur d'administration via l'Agent d'administration. Une liste complète des données est fournie dans les fichiers d'aide de l'application correspondante.

- Données nécessaires à la création d'une chaîne de développement des menaces. L'application administrée transfère les données de l'appareil vers le Serveur d'administration via l'Agent d'administration. Une liste complète des données est fournie dans les fichiers d'aide de l'application correspondante.

- Informations sur les tentatives d'accès aux services cloud par les employés d'une organisation. L'application administrée transfère les données de l'appareil vers le Serveur d'administration via l'Agent d'administration. Une liste complète des données est fournie dans les fichiers d'aide de l'application correspondante.

- Données requises pour l'intégration de Kaspersky Security Center avec le service Kaspersky Managed Detection and Response (le plug-in dédié doit être installé pour Kaspersky Security Center Web Console) : jeton de lancement d'intégration, jeton d'intégration et jeton de session utilisateur. L'Utilisateur saisit le jeton d'initiation d'intégration dans l'interface de Kaspersky Security Center Web Console : Le service Kaspersky MDR transfère le jeton d'intégration et le jeton de session utilisateur via le plug-in dédié.

- Données nécessaires à l'intégration de Kaspersky Security Center Linux avec Kaspersky Cloud Sandbox et Kaspersky Threat Intelligence Portal (requiert l'installation du plug-in approprié pour Kaspersky Security Center Web Console) : un jeton d'intégration, un jeton d'autorisation. L'Utilisateur saisit un jeton pour l'intégration dans l'interface de Kaspersky Security Center Web Console. Kaspersky Security Center Web Console transfère un jeton d'autorisation dans une demande adressée à l'API de Kaspersky Cloud Sandbox.

- Données nécessaires à l'intégration de Kaspersky Security Center Linux avec le service Kaspersky Automated Security Awareness Platform (KASAP) : jeton d'API pour accéder à l'API ouverte de KASAP, URL (un lien pour accéder à KASAP via l'API ouverte).

- Détails des codes d'activation saisis et des fichiers clés. L'Utilisateur saisit les données dans l'interface de Kaspersky Security Center Web Console.

- Comptes utilisateurs : nom, description, nom complet, adresse email, numéro de téléphone principal, mot de passe, clé secrète générée par le Serveur d'administration et mot de passe à usage unique pour l'authentification à deux facteurs. 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.

- Adresse IP de l'appareil sur lequel l'utilisateur a créé une révision. L'adresse IP est définie automatiquement par le Serveur d'administration.

- Registre des objets de gestion supprimés. L'Utilisateur 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 et transmet les données à l'aide de l'utilitaire klsetsrvcert du Serveur d'administration.

- Certificats permettant d'établir la confiance dans les ressources Internet internes de l'organisation. L'Utilisateur saisit les données dans l'interface de Kaspersky Security Center Web Console.

- Informations sur l'acceptation par l'utilisateur des termes et conditions des accords légaux avec Kaspersky.

- Les données du Serveur d'administration que l'utilisateur saisit dans 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 sont transférées de l'appareil mobile vers le Serveur d'administration à l'aide du protocole MDM iOS ou mobile.

Les données répertoriées sont stockées dans la base de données du Serveur d'administration. Les hachages des mots de passe sont stockés sous forme chiffrée.

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.

Les informations obtenues sont protégées par Kaspersky Lab conformément aux exigences fixées par la loi et aux règles en vigueur de Kaspersky Lab. Les données sont transmises par des canaux de communication sécurisés.

En suivant les liens de Kaspersky Security Center 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 les données collectées sous forme anonymisée et uniquement à des fins statistiques générales. Les statistiques récapitulatives sont générées automatiquement à partir des données brutes reçues et ne contiennent aucune information personnelle ou autre information confidentielle. À mesure que de nouvelles données s'accumulent, les données plus anciennes sont supprimées (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 le nom du Serveur d'administration.

   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 par exemple, que pour cet appareil, deux des clés de licence du stockage peuvent être appliquées à l'appareil : la clé de licence *Key_1* et la clé de licence *Key_2*. Une de ces clés de licence est déployée sur l'appareil. Une des clés de licence adaptées est diffusée, et dans ce cas, il n'est pas possible de savoir laquelle de ces deux clés sera diffusée sur l'appareil car le déploiement automatique des clés de licence ne prévoit pas l'intervention de l'administrateur.

Lors du déploiement de la clé, les appareils sont recalculés pour cette clé de licence. Vous devez vous assurer que le nombre d'appareils sur lequel la clé de licence est diffusée ne dépasse pas la restriction de licence. Si le nombre d'appareils dépasse la restriction de licence, l'état *Critique* est attribué à tous les appareils non couverts par la licence.

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, puis 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

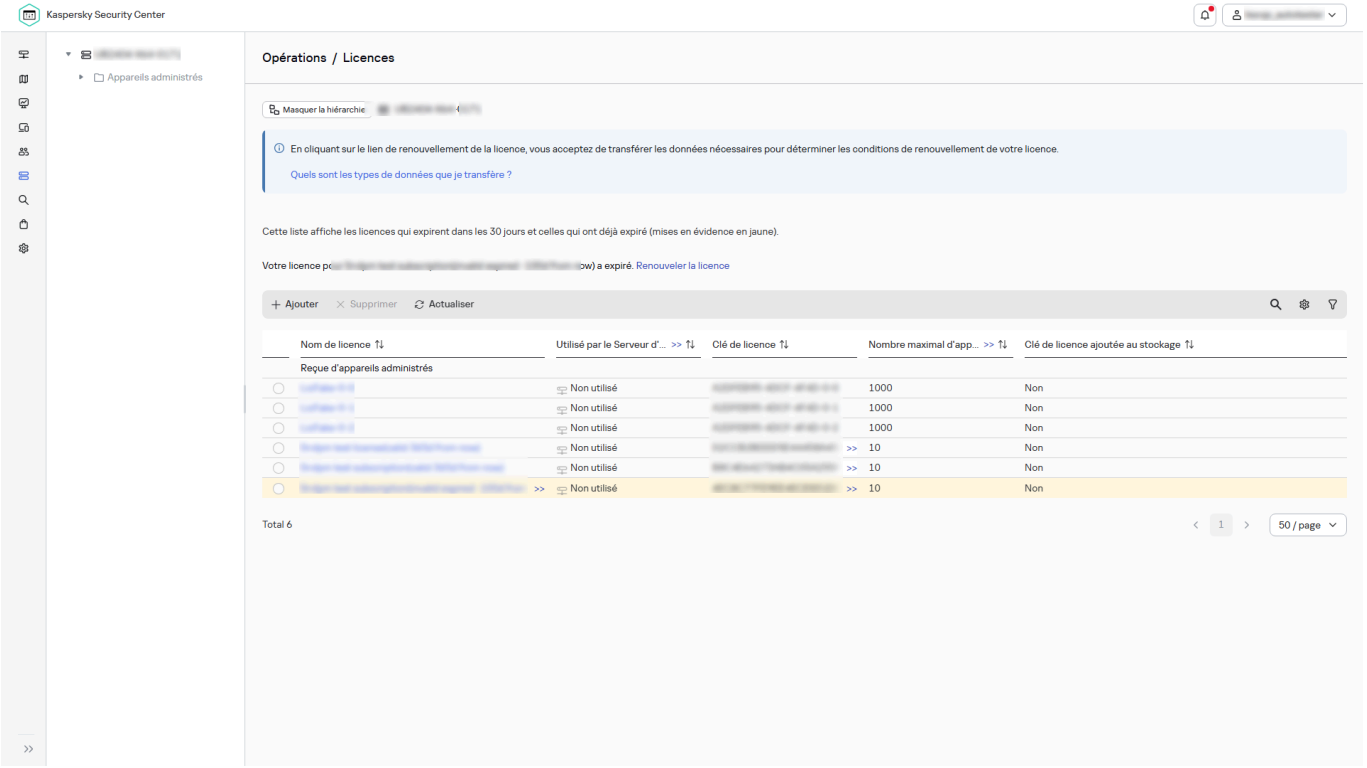
Ajout d'un code d'activation ou d'un fichier clé manuellement sur les appareils

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**.



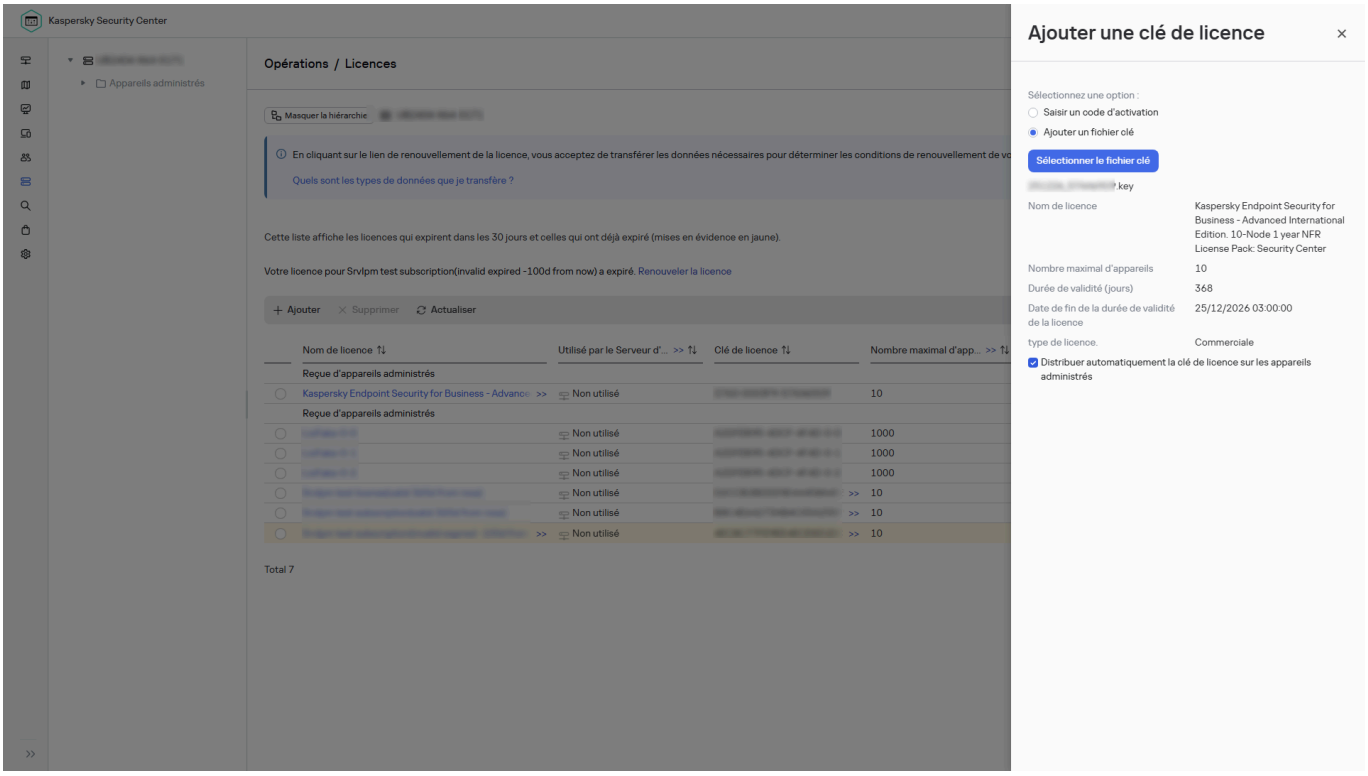
Liste des clés de licence de Kaspersky ajoutées

2. Cliquez sur **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.



Ajout d'une clé de licence par application d'un fichier clé

- **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 **Gestion des ressources** → **Tâches**.

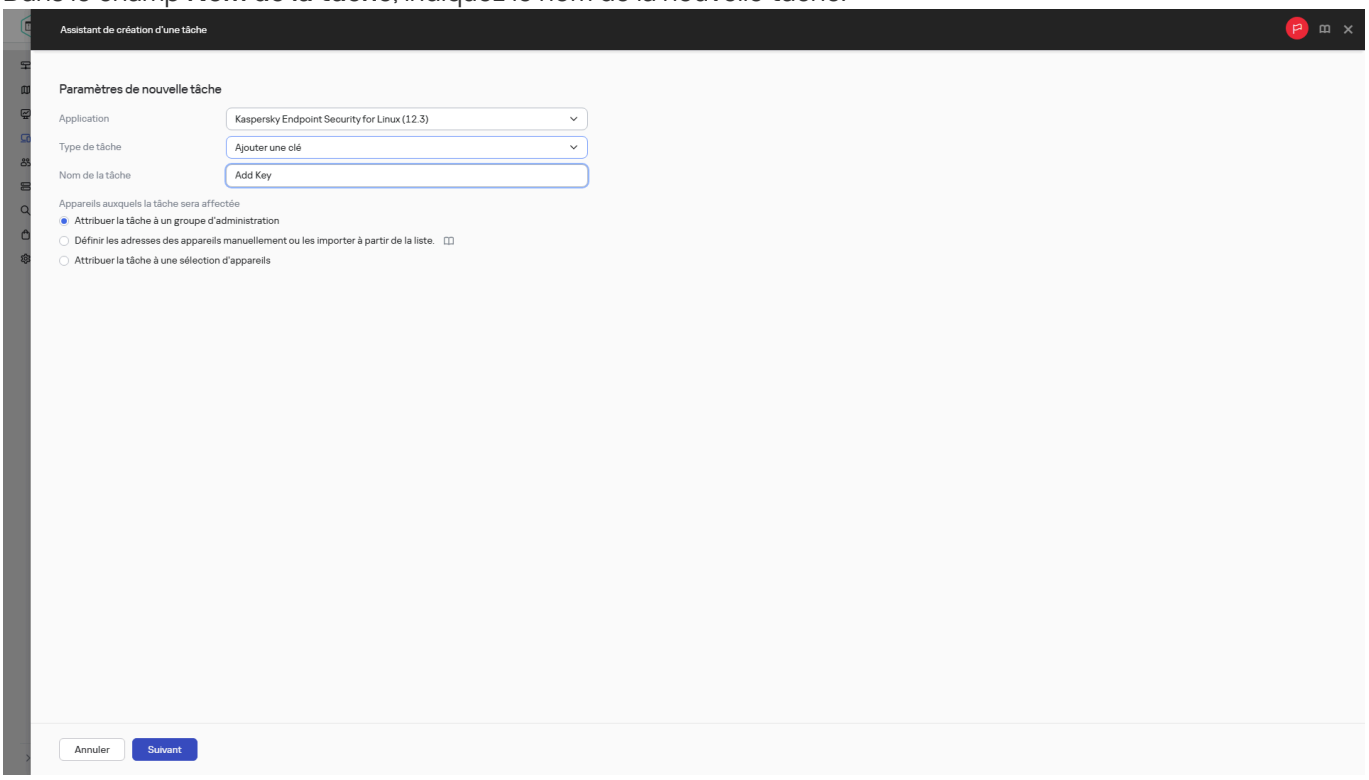
2. Cliquez sur **Ajouter**.

   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.

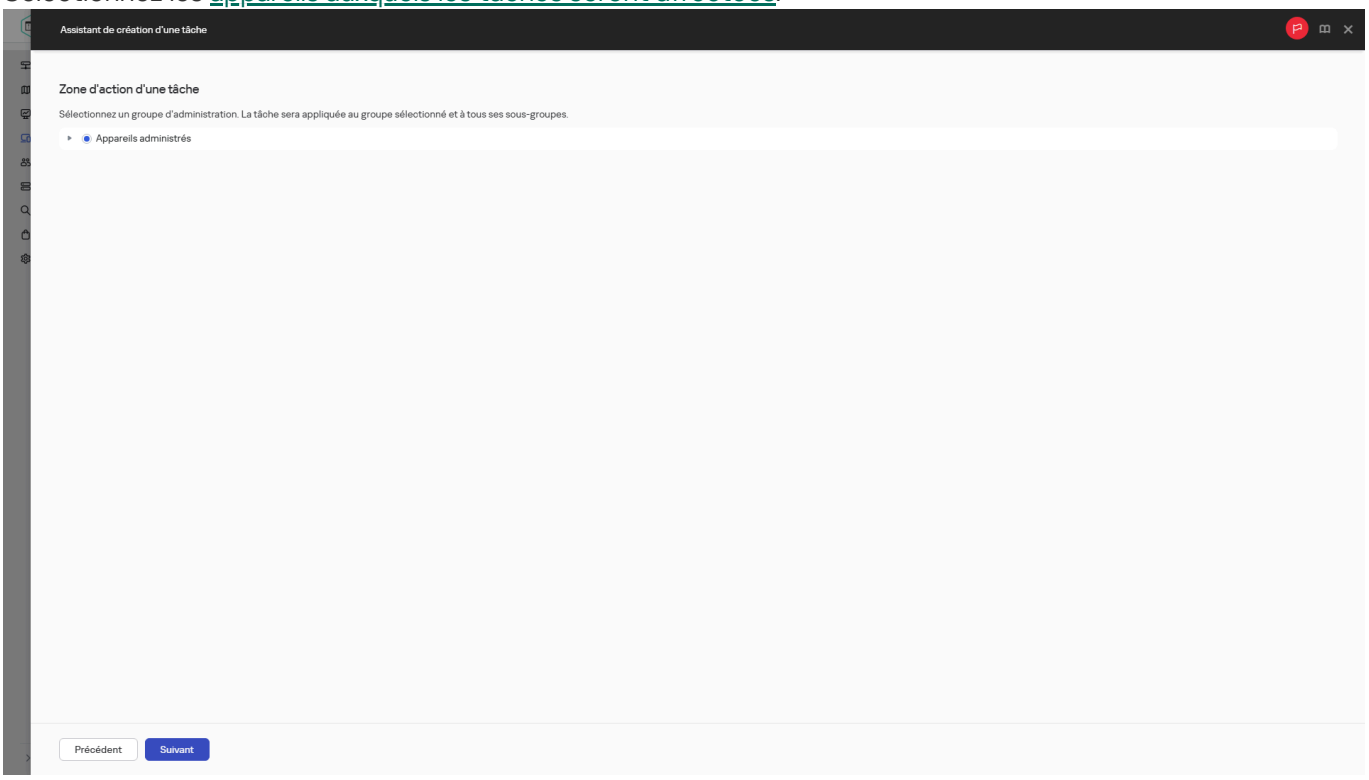
4. À partir de la liste **Type de tâche**, sélectionnez la tâche **Activation de l'application**.

5. Dans le champ **Nom de la tâche**, indiquez le nom de la nouvelle tâche.



Création d'une tâche Ajout d'une clé

6. Sélectionnez les appareils auxquels les tâches seront affectées.



Spécification de la zone de la tâche

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**.

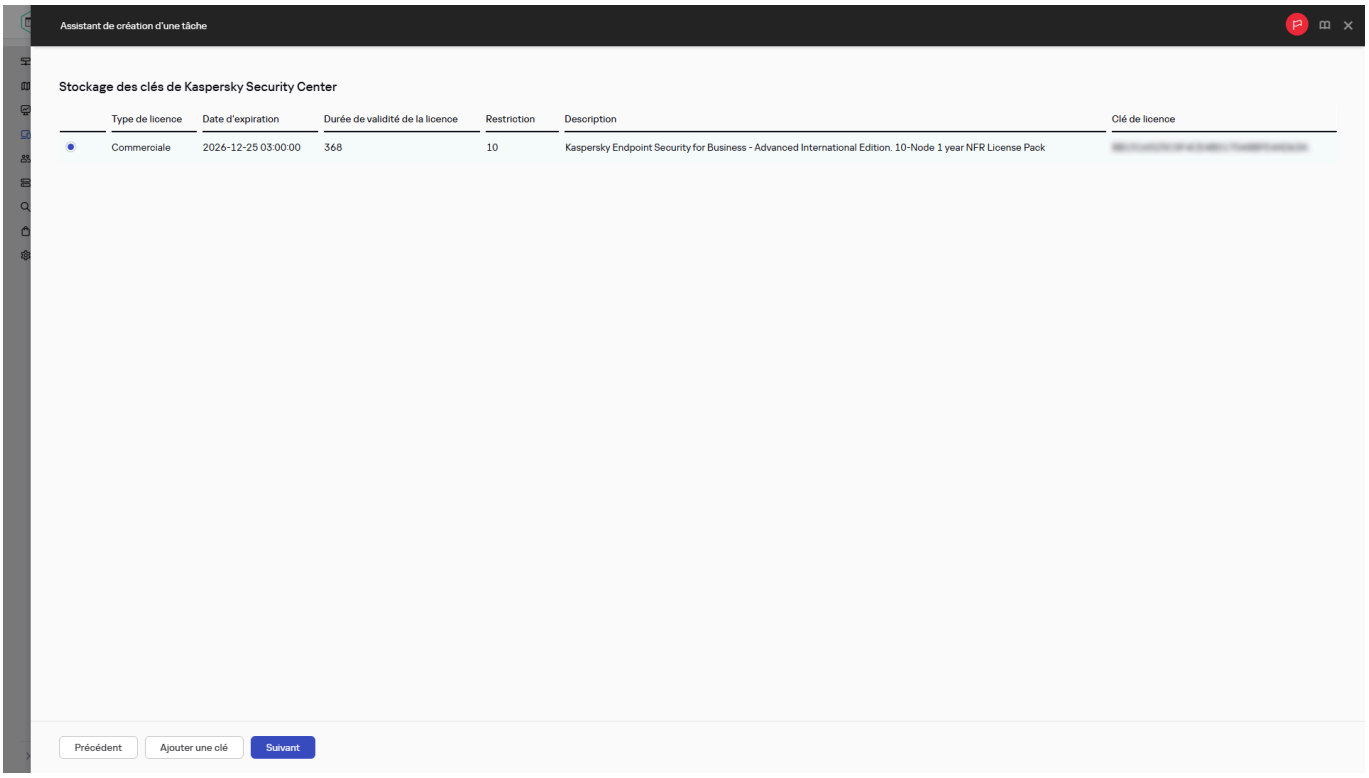
  Les informations sur la clé de licence apparaissent dans le volet d'ajout d'une clé de licence.

  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.

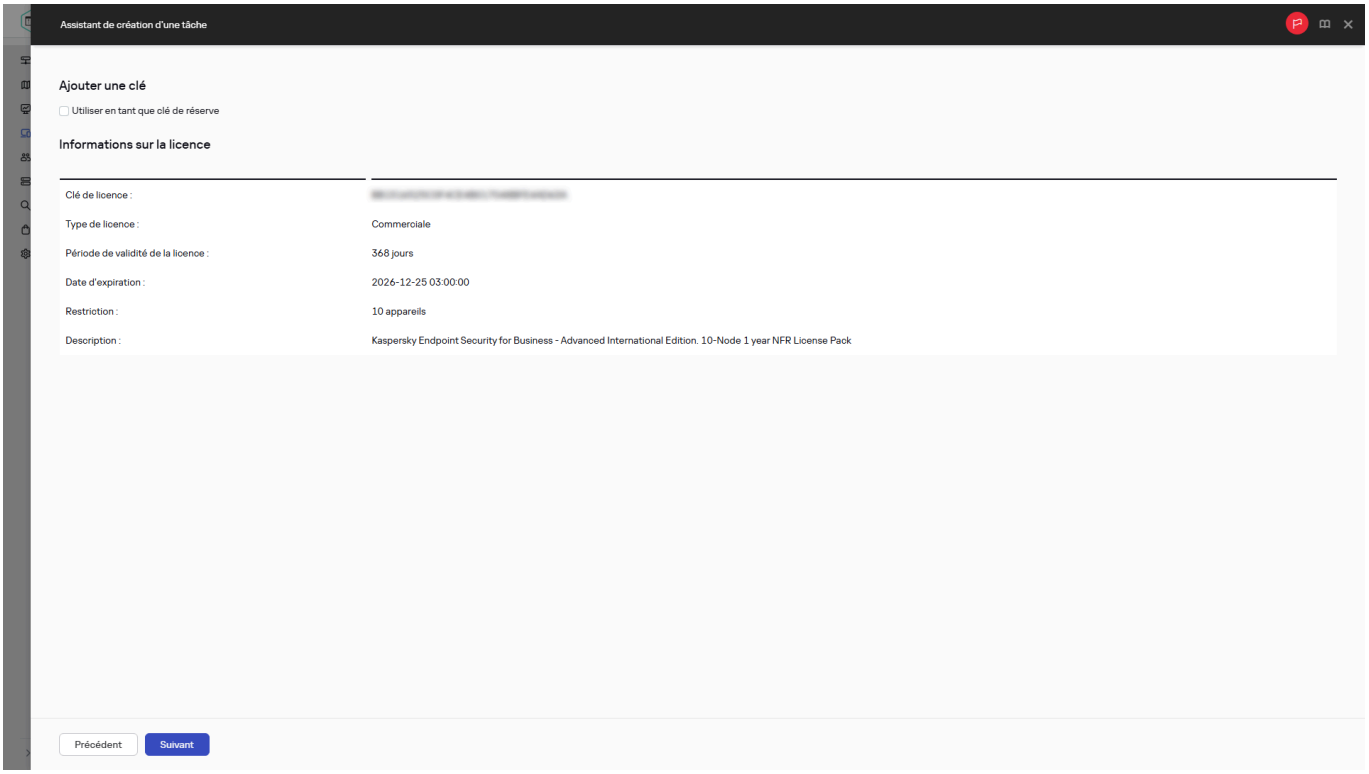


Sélection de la clé de licence

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.



Spécification de la clé de licence de réserve

11. Si, à l'étape **Fin de la création de la tâche** de l'Assistant, vous activez l'option **Ouvrir les détails de la tâche à la fin de la création**, vous pouvez modifier les paramètres par défaut de la tâche.

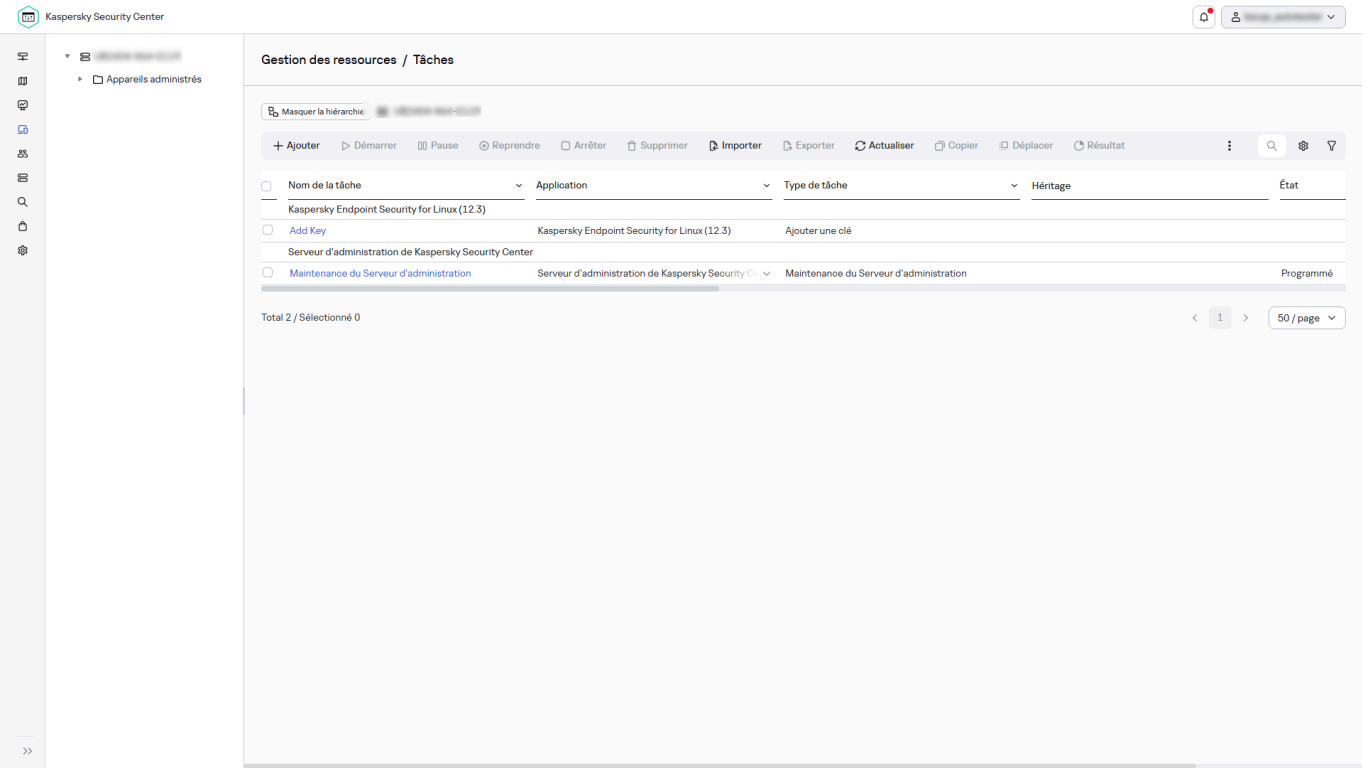
    Si vous n'activez pas cette tâche, la tâche est créée selon les paramètres par défaut. Vous pourrez modifier ces paramètres par défaut plus tard.

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.



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.

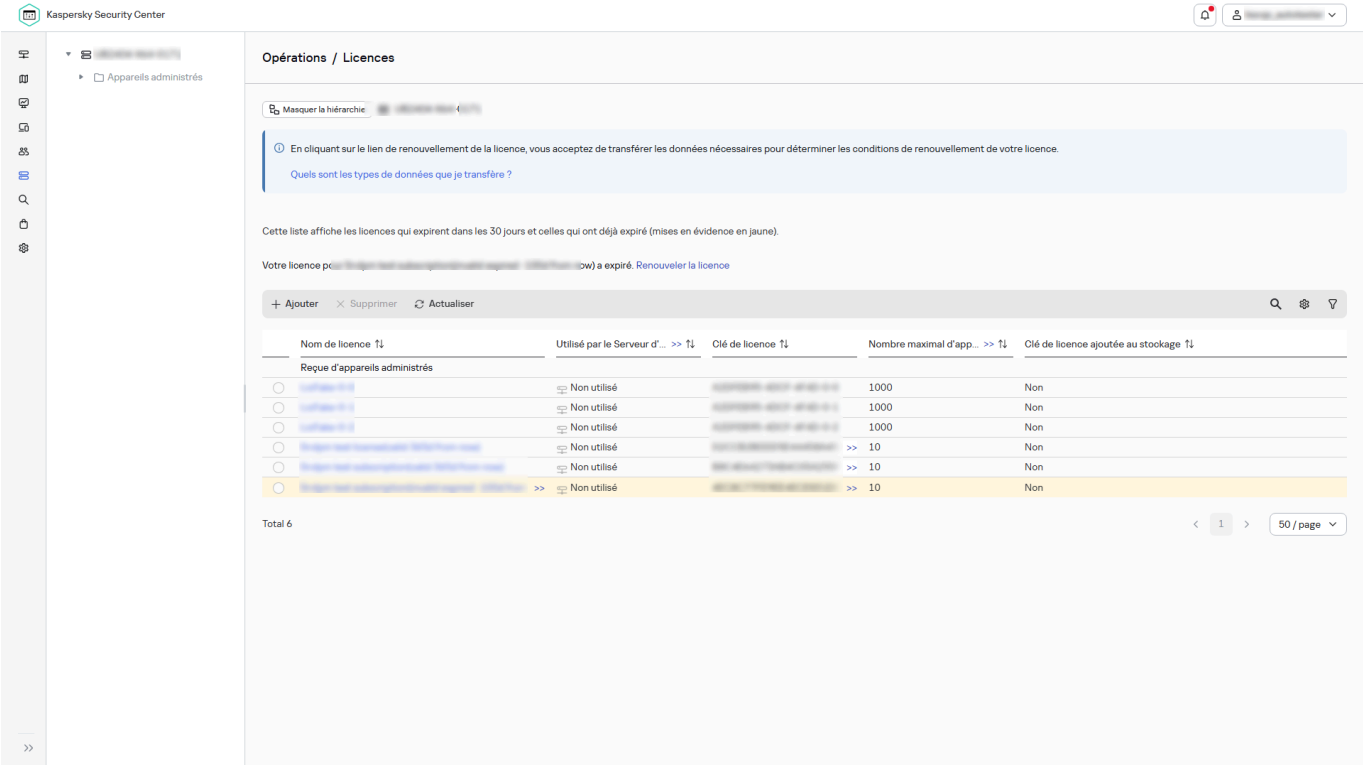
Une fois la tâche terminée, la clé de licence est déployée sur les appareils sélectionnés.

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 :

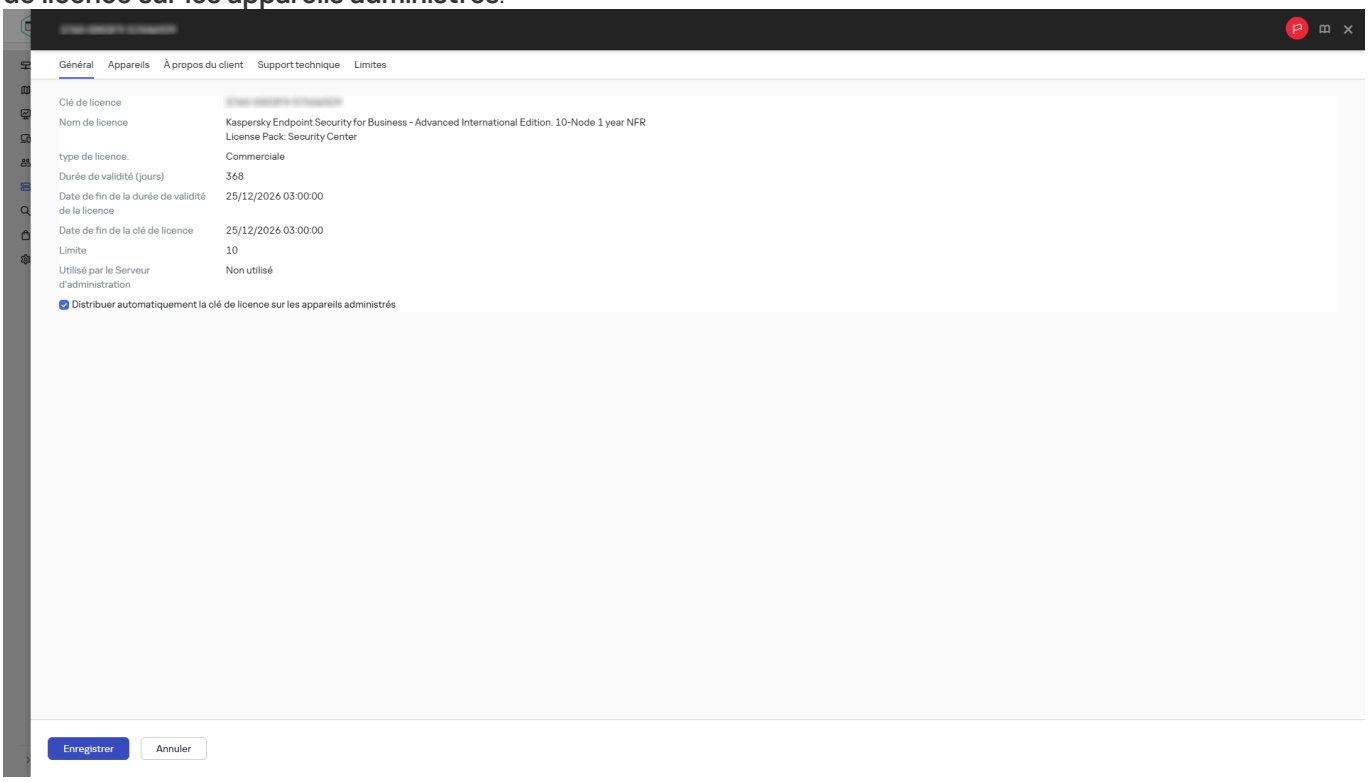
1. Dans le menu principal, accédez à **Opérations** → **Licence** → **Licences**.



La liste des licences

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**.



La fenêtre des propriétés de la clé de licence

4. Cliquez sur le bouton **Enregistrer**.

La clé de licence sera automatiquement distribuée à tous les appareils compatibles.

La diffusion de la clé de licence est exécutée via les moyens de l'Agent d'administration. Aucune tâche de distribution de la clé de licence n'est créée pour l'application.

Lors de la distribution automatique de la clé de licence, la limite de licences sur le nombre d'appareils est prise en compte. La restriction de la licence est définie dans les propriétés de la clé de licence. Si la limite liée à la restriction de la 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**.

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**.
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
- Dans l'onglet **Limites**, la liste des limites de la licence

  Si vous avez activé le Serveur d'administration sous licence pour Kaspersky Next XDR Optimum, l'onglet **Limites** affiche le champ **XDR-O** avec la valeur **Activé**.

Pour voir quelles clés de licence sont déployées sur un appareil client spécifique :

1. Dans le menu principal, accédez à **Gestion des ressources** → **Ressources (Appareils)**.
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 licences 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 lancer le test, procédez comme suit :

   a. Dans le menu principal, cliquez sur le nom du Serveur d'administration.

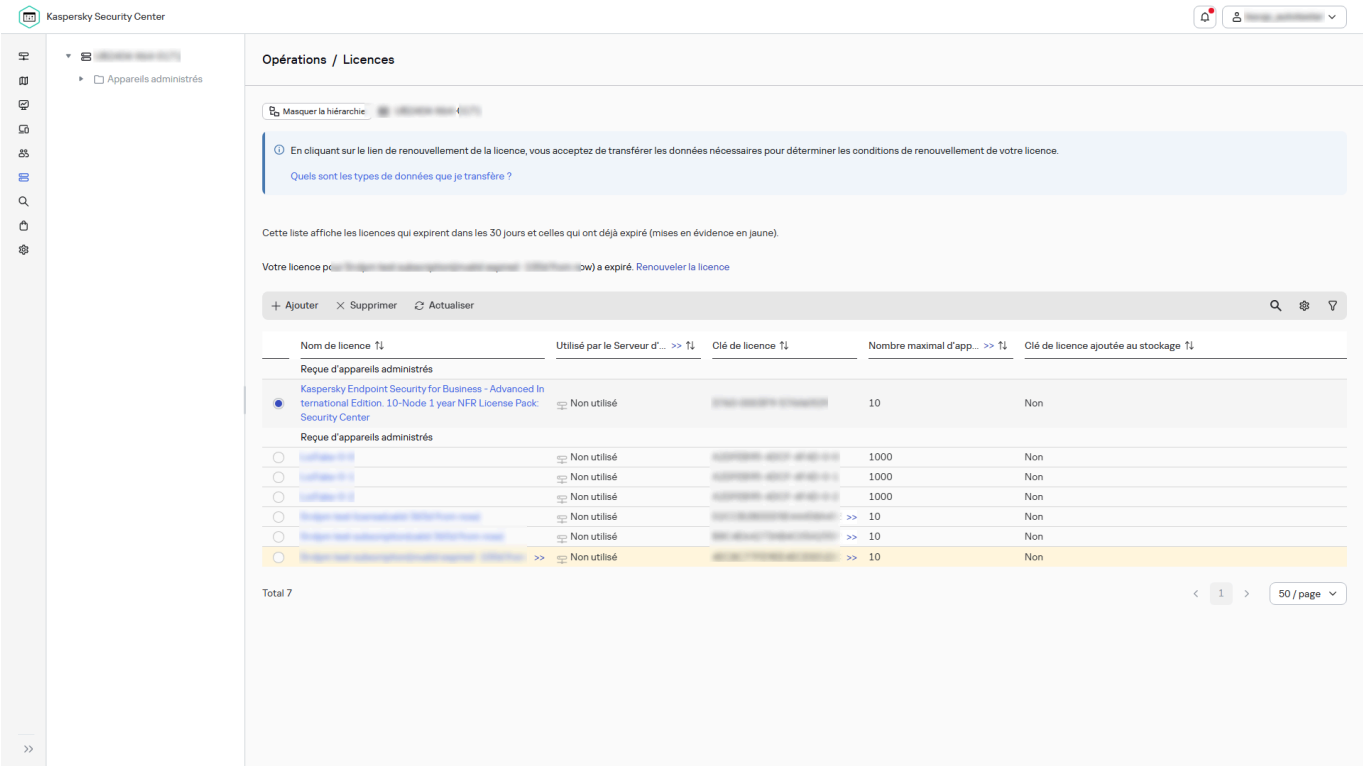
      La fenêtre des propriétés du Serveur d'administration s'ouvre.

   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**.

3. Sélectionnez le fichier clé ou le code d'activation requis, puis cliquez sur le bouton **Supprimer**.



La liste des licences

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.

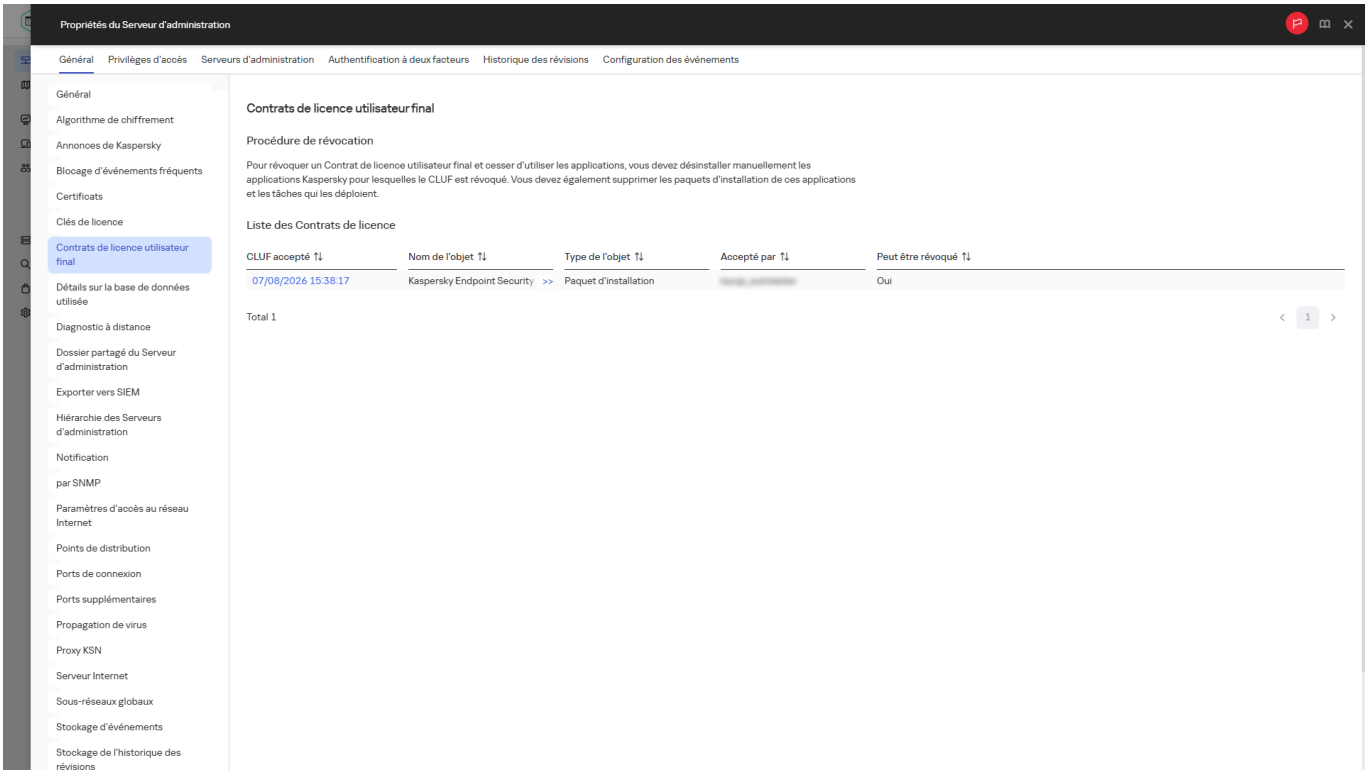
Révocation d'un Contrat de licence utilisateur final

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 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.



La liste des CLUF

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. Exécutez une des actions suivantes :

   - Dans le menu principal, accédez à **Opérations** → **Licence** → **Licences**.
   - Dans le menu principal, accédez à **Surveillance** → **Tableau de bord**, puis cliquez sur le lien **Afficher les licences arrivant à expiration** à côté d'une notification.

   La fenêtre **Licences** 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
  - Tâche *Recherche de vulnérabilités et de mises à jour requises*

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 aussi 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 pratiques : Paramétrage de la tâche de groupe de mise à jour de Kaspersky Endpoint Security, Création d'une tâche Recherche de vulnérabilités et de mises à jour requises.

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 :

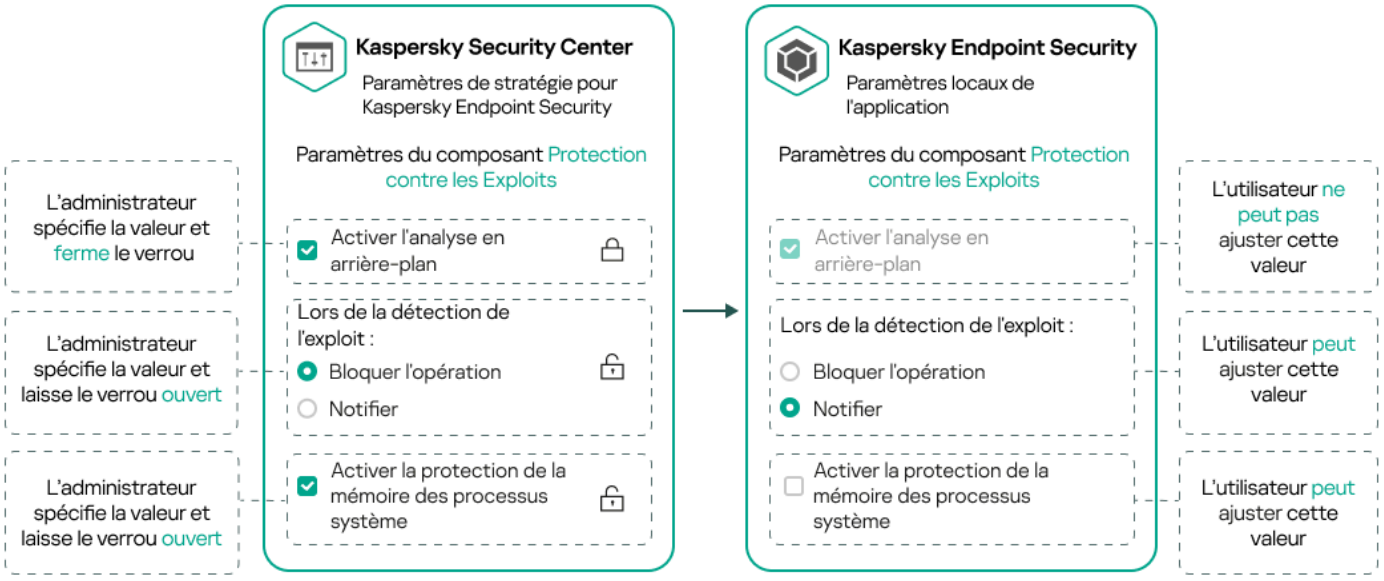
- Paramètres de verrouillage pour une stratégie de sous-groupe d'administration
- Paramètres de verrouillage d'une application Kaspersky sur un appareil administré

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

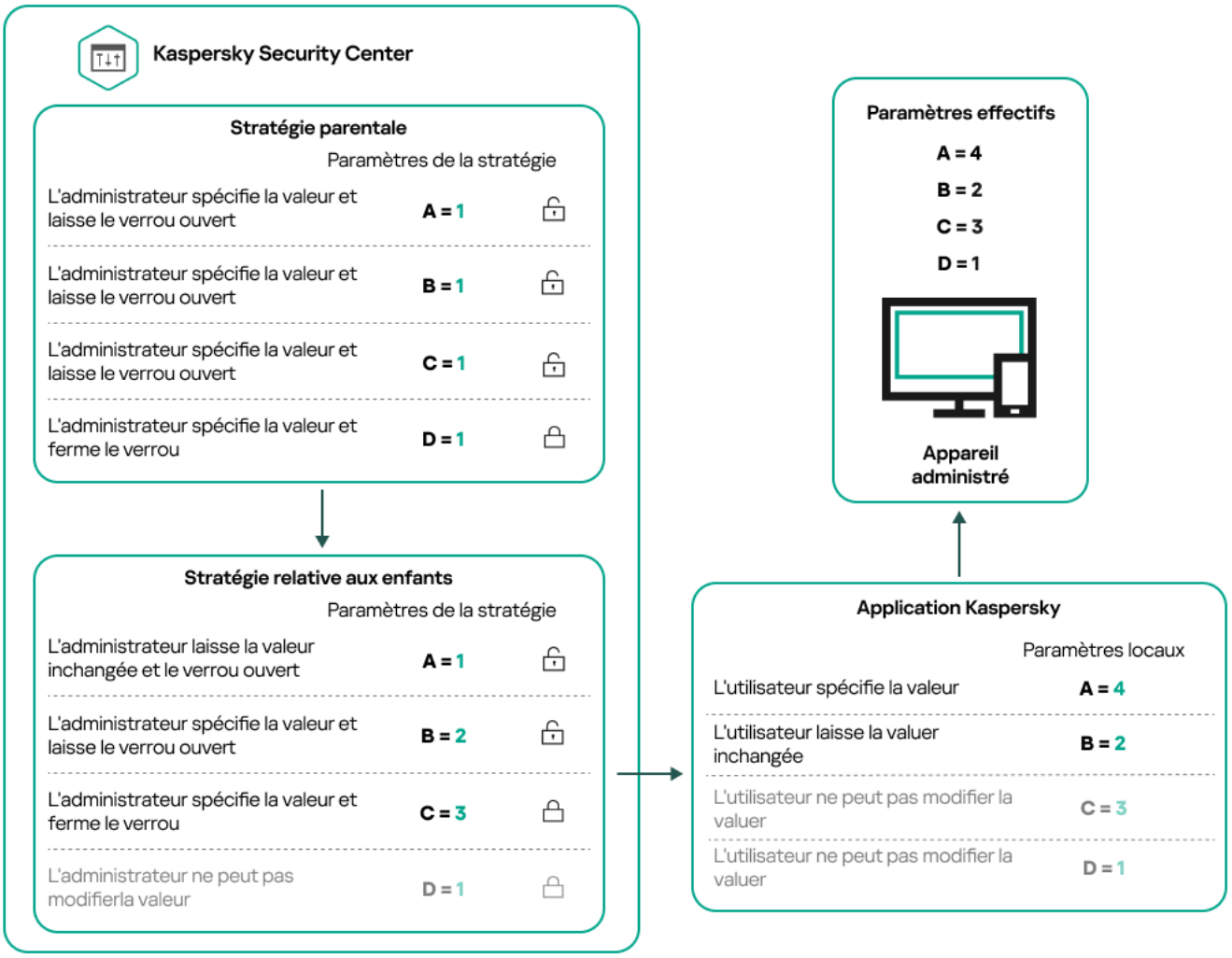
Si des appareils différents requièrent des paramètres différents, vous pouvez organiser les appareils en groupes d'administration.

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'ungroupe 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

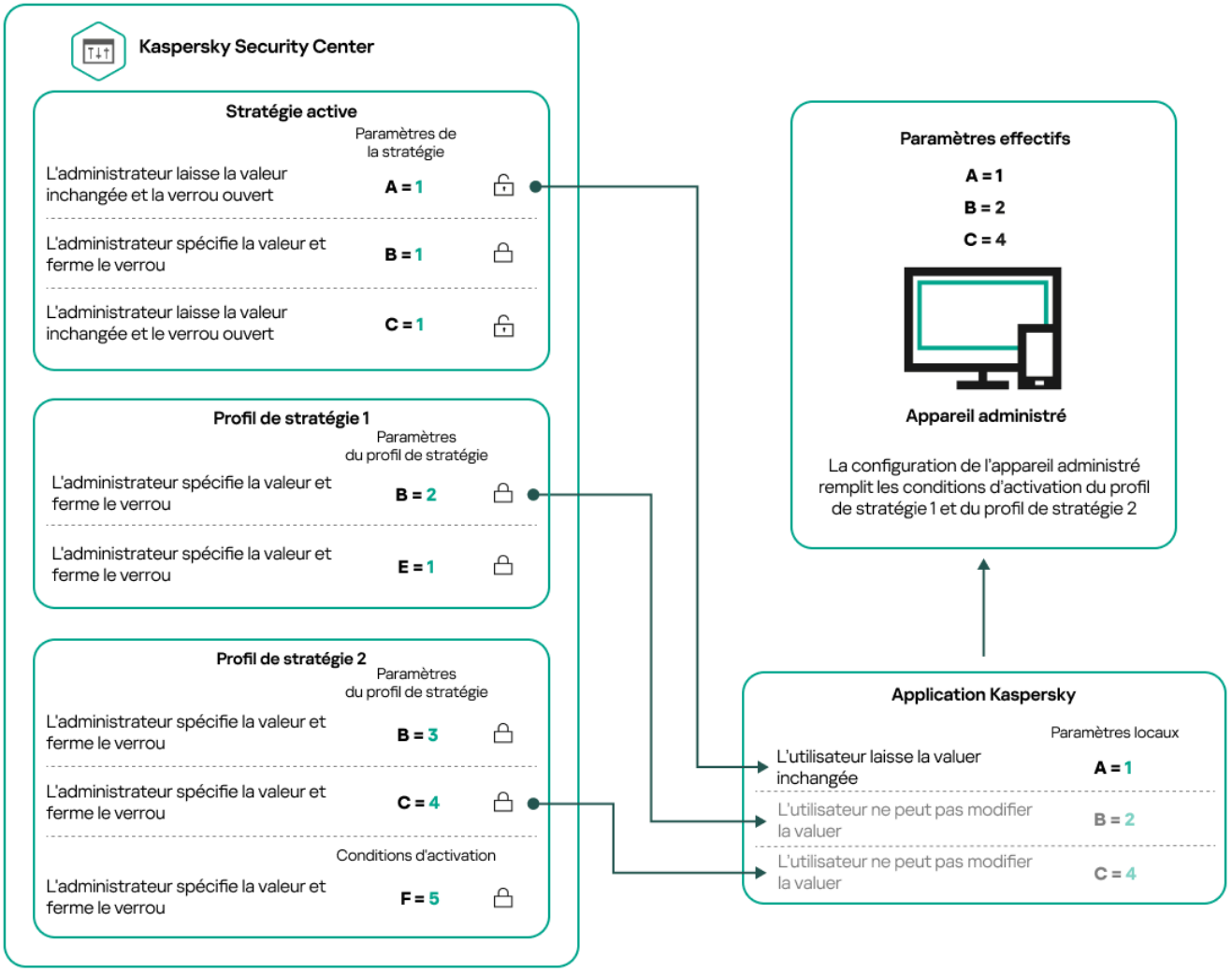
Profils de stratégie dans une hiérarchie de stratégies

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).



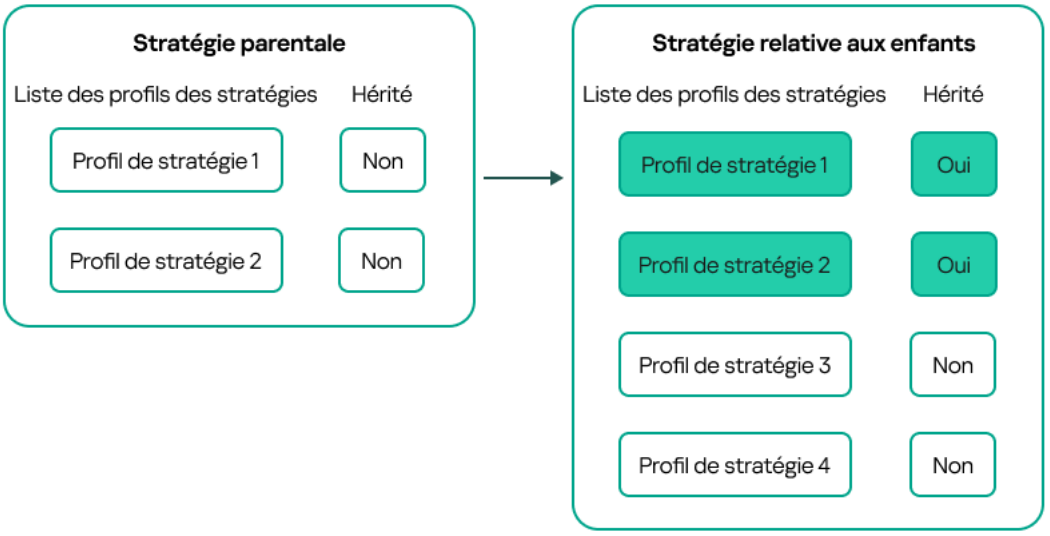
La configuration de l'appareil administré satisfait aux conditions d'activation de plusieurs profils de stratégie

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).

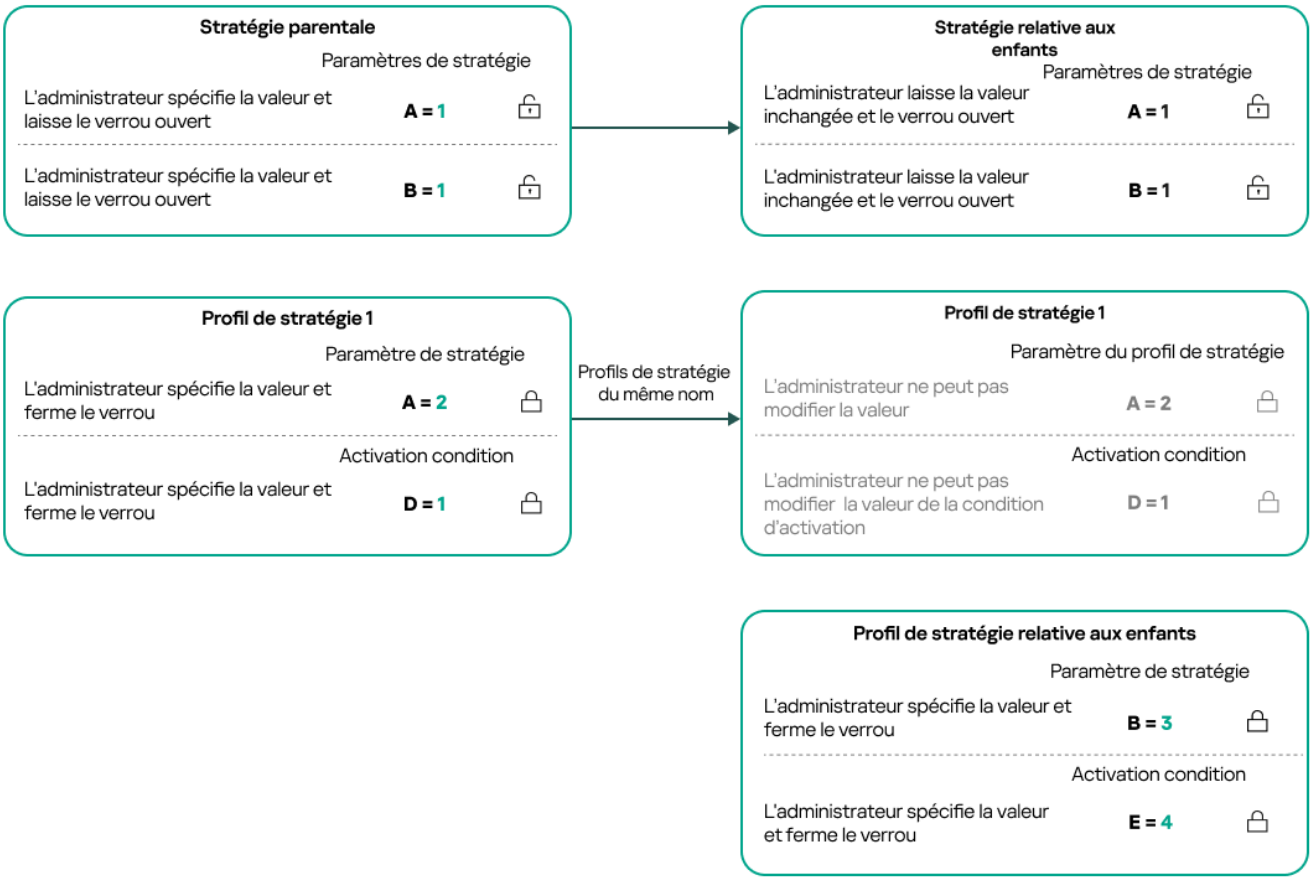


Héritage des profils de stratégie

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 **Gestion des ressources** → **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 **Gestion des ressources** → **Stratégies**.

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.

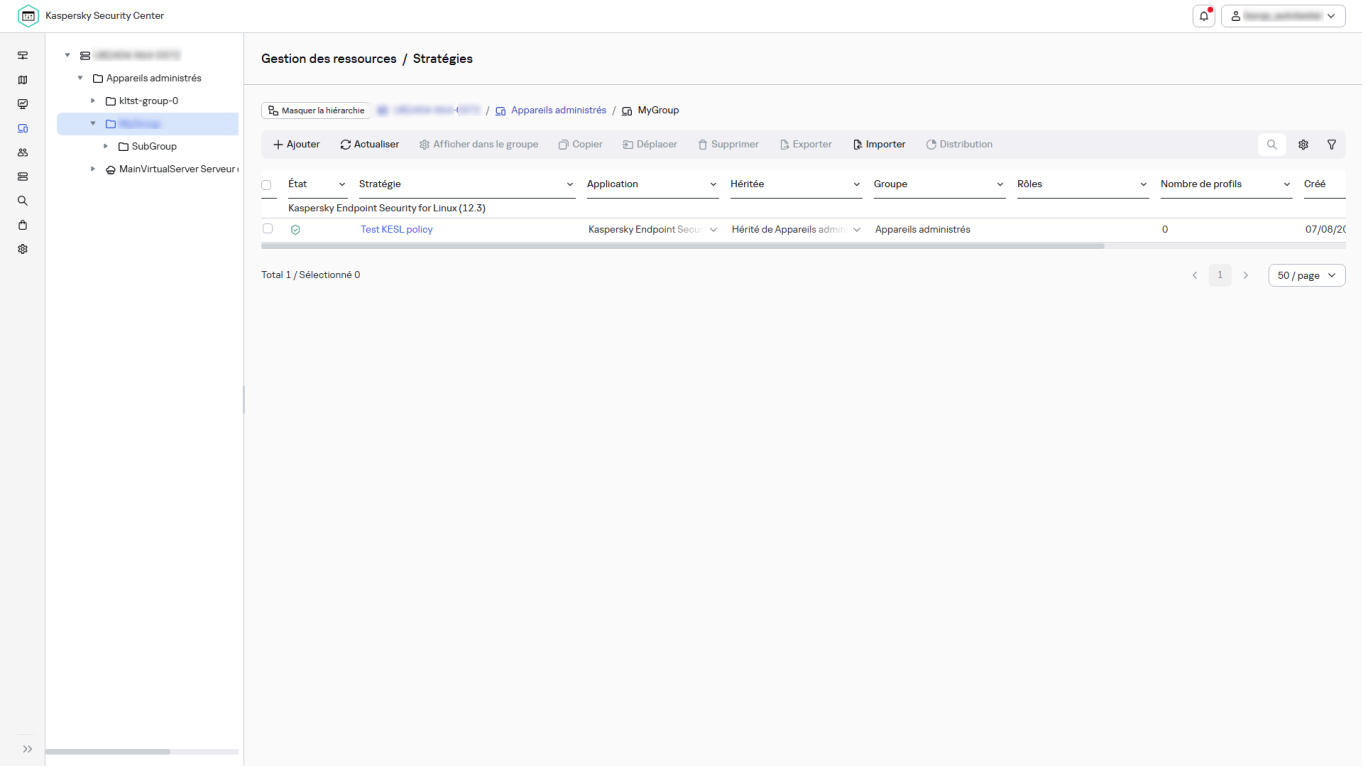
   - Pour un sous-groupe :

     a. Cliquez sur le bouton **Afficher la hiérarchie** en haut de la page.

     Le nom du bouton devient **Masquer la hiérarchie**.

     b. Dans la fenêtre qui s'ouvre, cliquez sur le nom du sous-groupe requis.

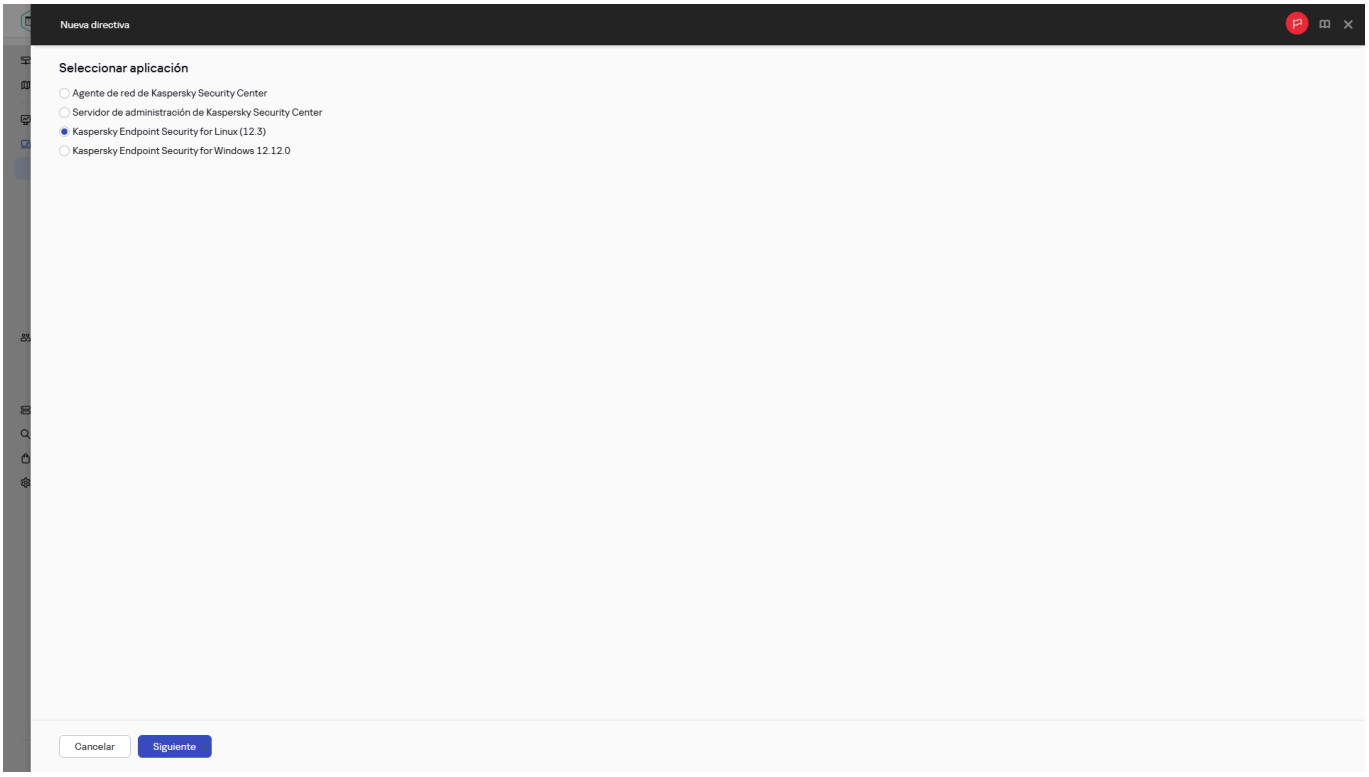
Le chemin vers le groupe sélectionné est affiché en haut de la page. Si nécessaire, vous pouvez cliquer sur un lien avec le nom du groupe d'administration pour accéder au groupe. Par défaut, le dernier lien du chemin est inactif. Vous pouvez également fermer la fenêtre de la hiérarchie en cliquant sur le bouton **Masquer la hiérarchie**.



La liste des stratégies

3. Cliquez sur **Ajouter**.

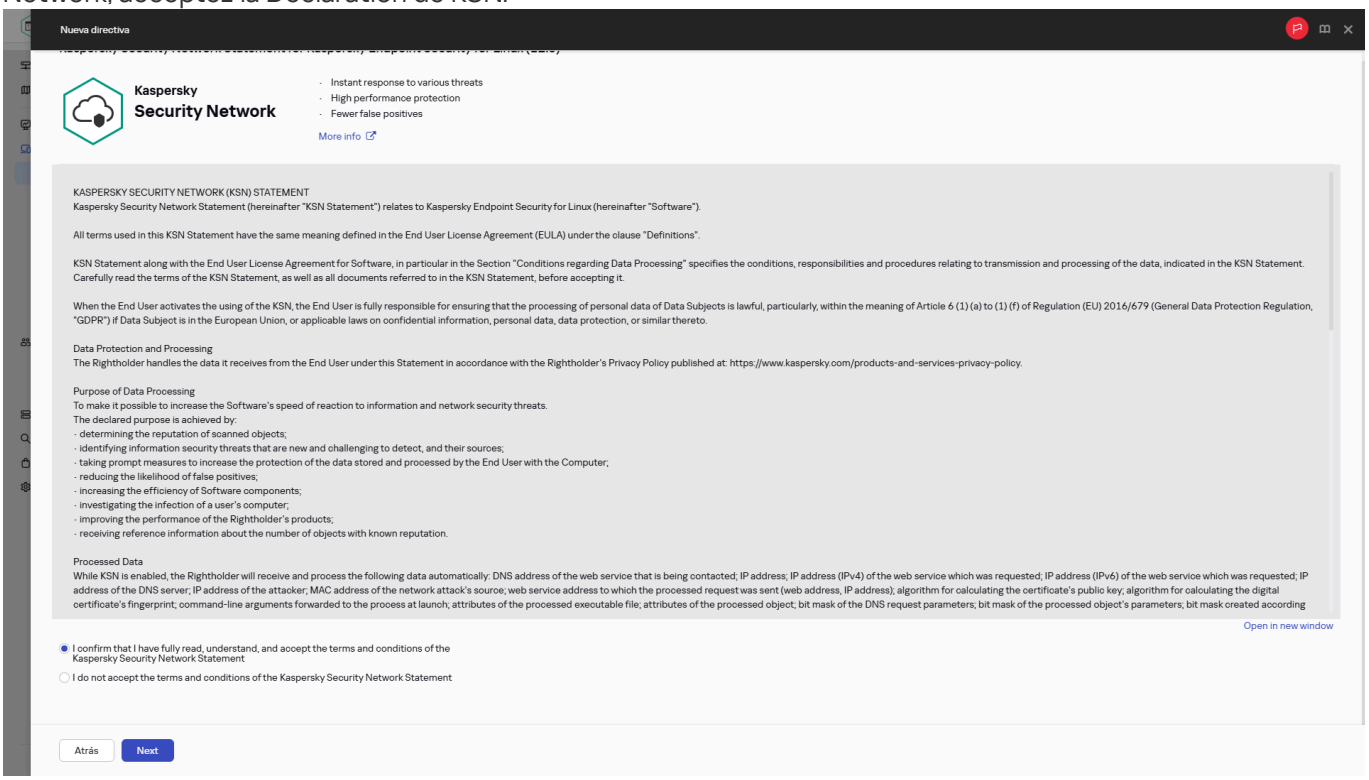
   La fenêtre **Sélectionnez l'application** s'ouvre.



Création d'une stratégie

4. Sélectionnez l'application pour laquelle vous souhaitez créer une stratégie.

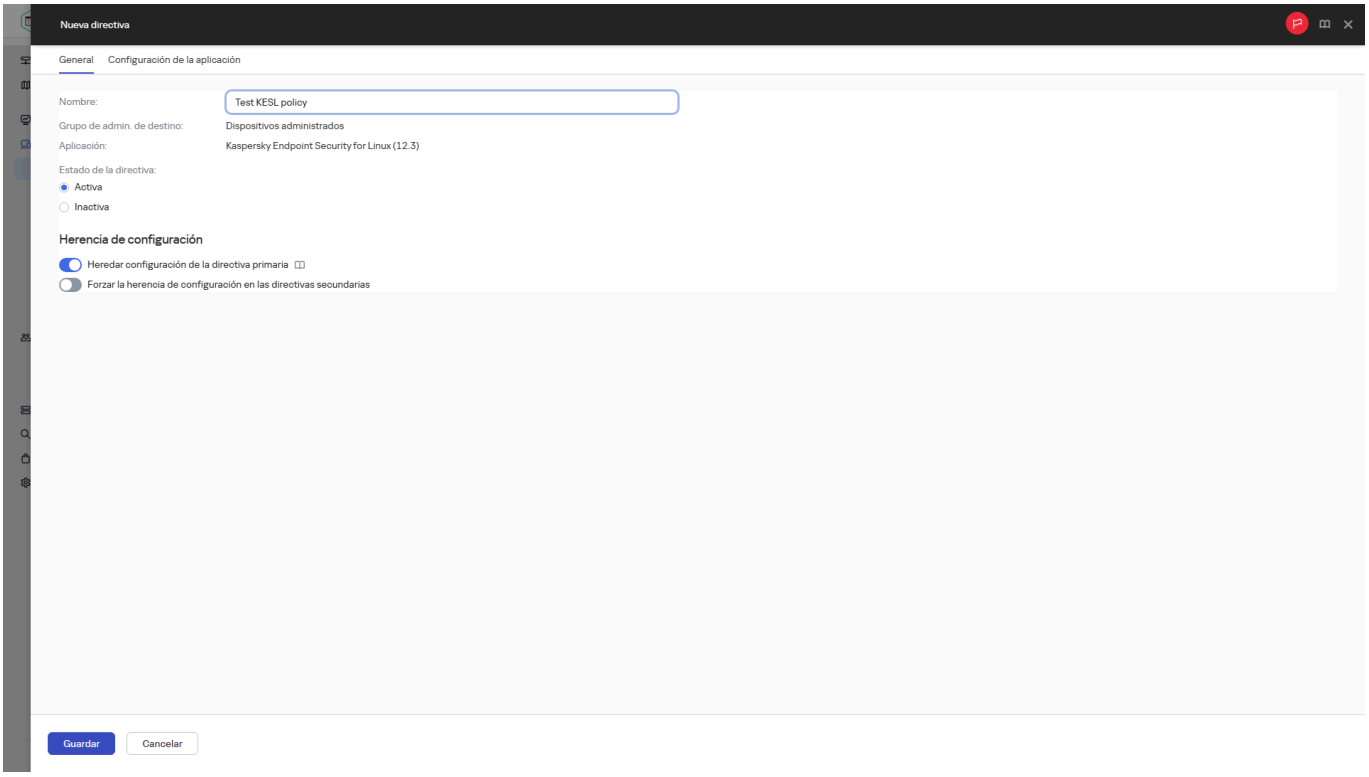
5. Si Kaspersky Security Network est pris en charge par l'application Kaspersky pour laquelle vous créez une stratégie, vous serez invité à accepter la Déclaration de KSN. Si vous souhaitez utiliser Kaspersky Security Network, acceptez la Déclaration de KSN.



Acceptation de la Déclaration de KSN

6. Cliquez sur **Suivant**.

La fenêtre des paramètres de la nouvelle stratégie s'ouvre à l'onglet **Général**. Si vous le souhaitez, modifiez le nom par défaut, l'état par défaut et les paramètres d'héritage par défaut pour la stratégie.



La fenêtre des paramètres de la nouvelle stratégie

7. Sélectionnez l'onglet **Paramètres de l'application**.

Ou vous pouvez cliquer sur **Enregistrer** et quitter. La stratégie apparaît dans la liste des stratégies et vous pouvez modifier ses paramètres ultérieurement.

8. Sous l'onglet **Paramètres de l'application**, sélectionnez dans le volet de gauche la catégorie que vous souhaitez, puis dans le panneau des résultats à droite, modifiez les paramètres de la stratégie. Vous pouvez modifier les paramètres de la stratégie dans chaque catégorie (section).

   L'ensemble des paramètres dépend de l'application pour laquelle vous créez une stratégie. Pour plus de détails, reportez-vous à ce qui suit :

   - Configuration du Serveur d'administration
   - Paramètres de la stratégie de l'Agent d'administration
   - Aide de Kaspersky Endpoint Security for Linux
   - Aide de Kaspersky Endpoint Security for Windows

   Pour plus de détails sur les paramètres des autres programmes de protection, consultez la documentation du programme correspondant.

   Pendant la modification des paramètres, vous pouvez cliquer sur **Annuler** pour annuler la dernière opération.

9. Cliquez sur **Enregistrer** afin d'enregistrer la stratégie.

Finalement, la stratégie ajoutée s'affiche dans la liste des stratégies.

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 :
  - **Actif**

    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 des 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 indique les types d'événements et la durée de conservation par défaut des événements sur le Serveur d'administration (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**.

De plus, l'onglet **Configuration des événements** affiche une notification lorsque de nouveaux types d'événements sont ajoutés (par exemple, dans une nouvelle version de l'application) et vous permet d'appliquer les nouveaux paramètres en cliquant sur le bouton **Enregistrer** ou **Enregistrer et fermer**.

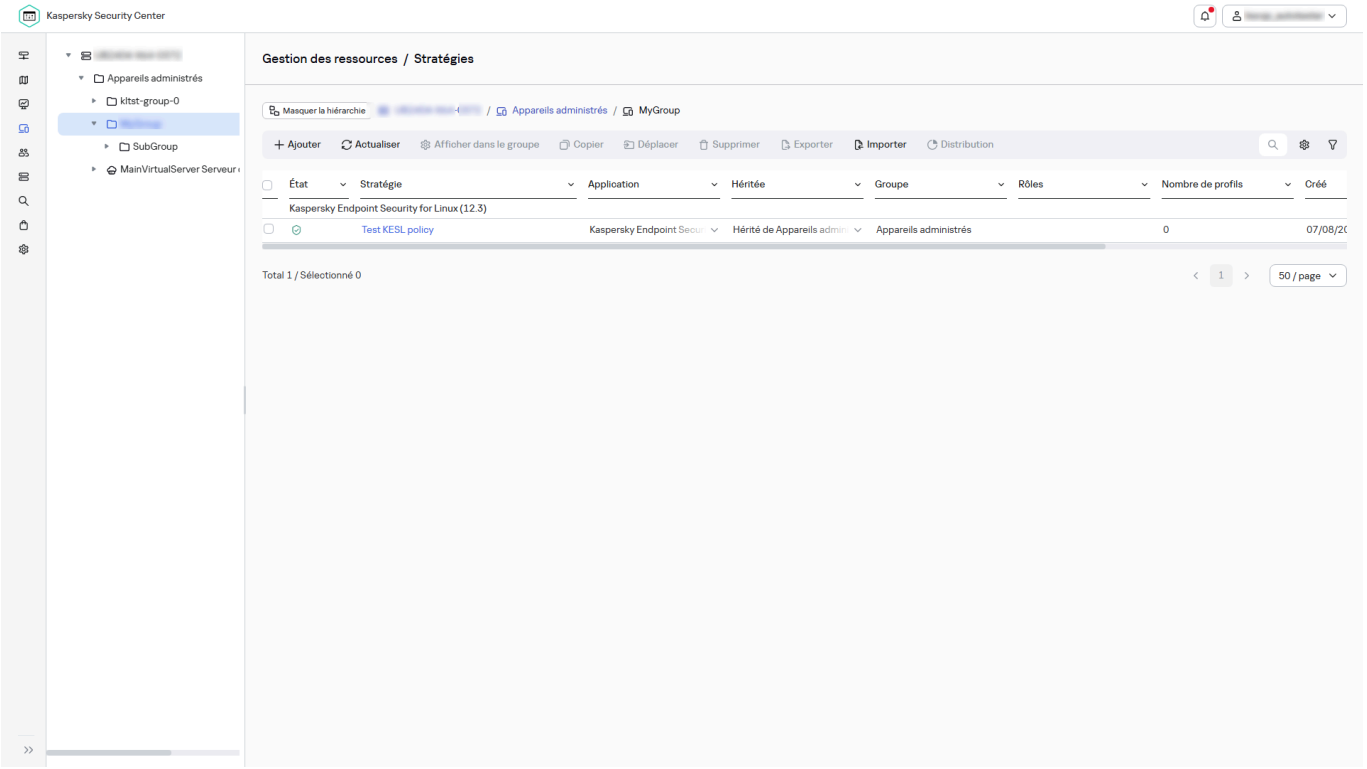
Historique des révisions

L'onglet **Historique des révisions** vous permet de consulter la liste des révisions de la stratégie, de comparer les révisions de la stratégie et de restaurer les modifications apportées à la stratégie, si nécessaire.

Modification d'une stratégie

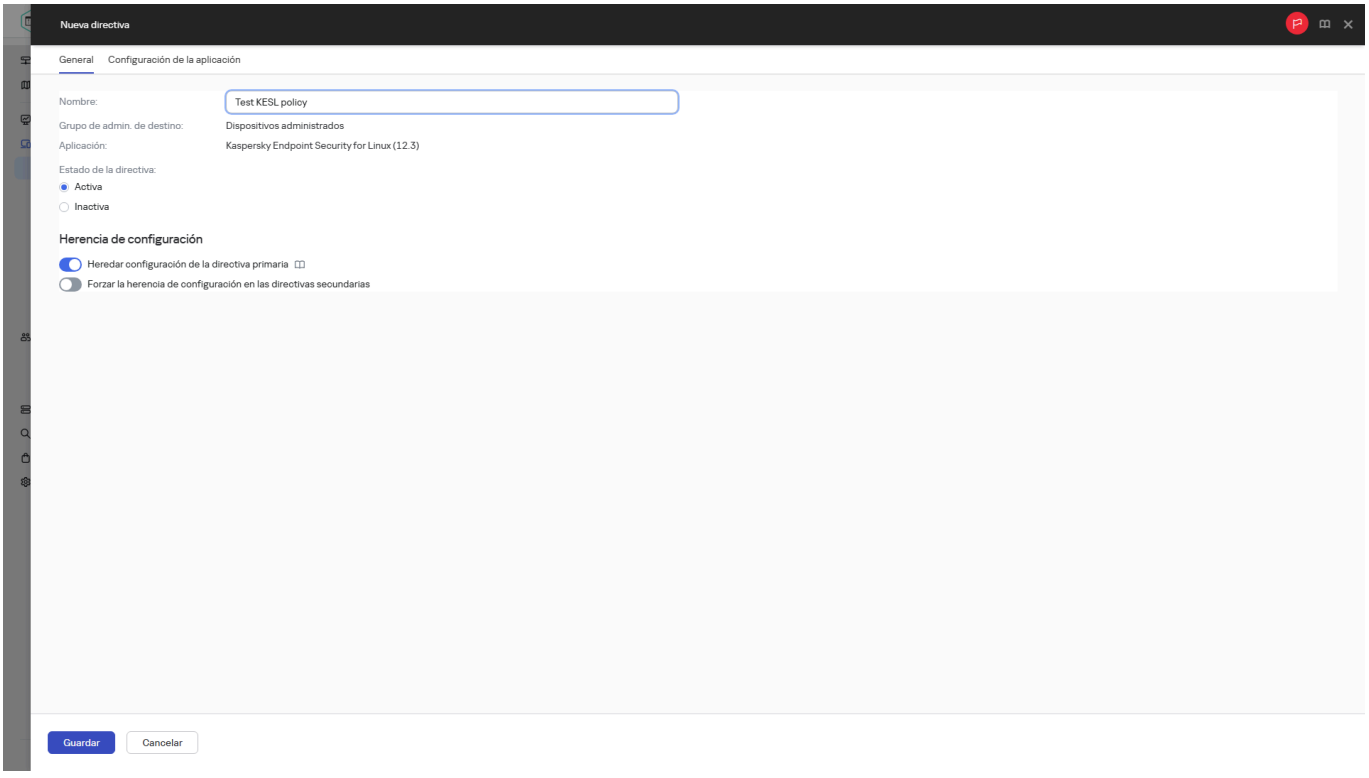
Pour modifier une stratégie, procédez comme suit :

1. Dans le menu principal, accédez à **Gestion des ressources** → **Stratégies**.



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**.

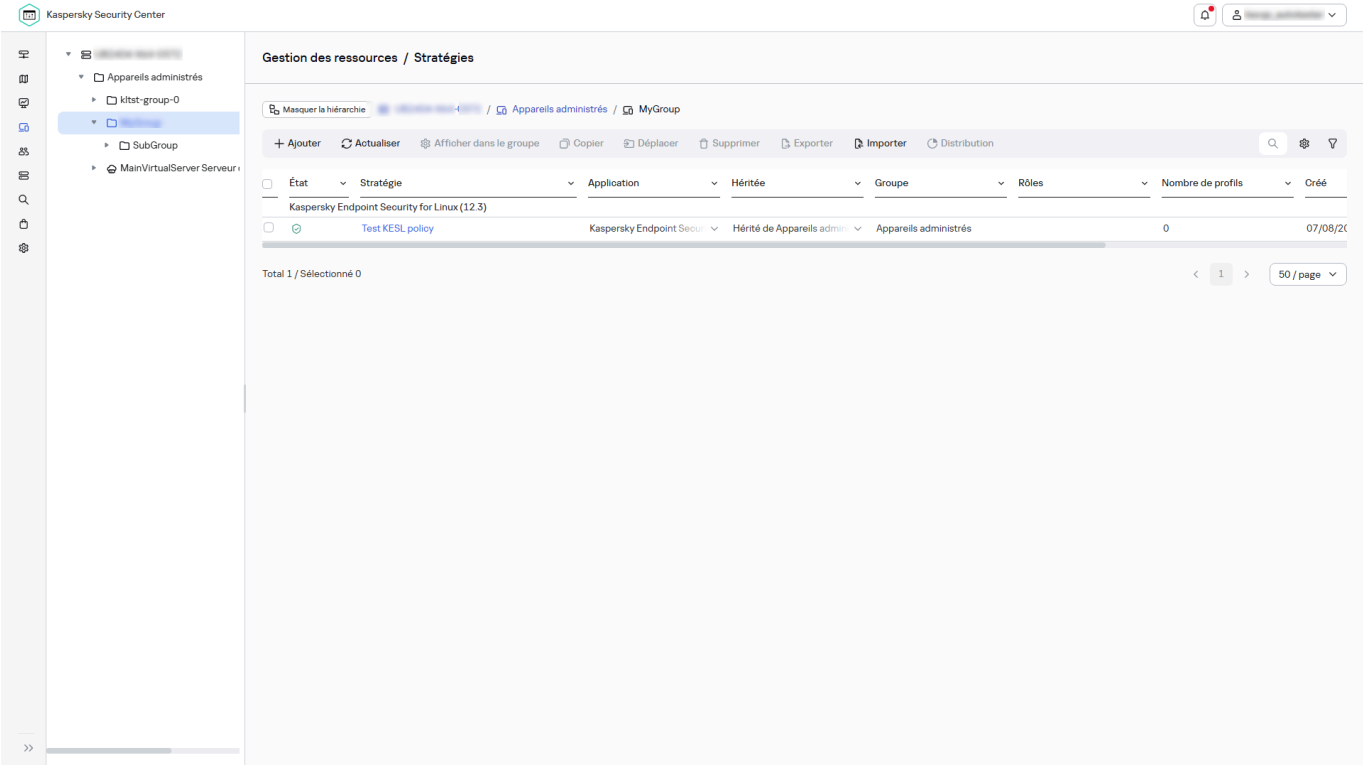
   Les modifications de la stratégie seront enregistrées dans les propriétés de la stratégie et seront affichées dans la section **Historique des révisions**.

Si nécessaire, vous pouvez comparer les révisions des stratégies. Cette option est disponible pour les stratégies du Serveur d'administration, de l'Agent d'administration, de Kaspersky Endpoint Security for Windows (à partir de la version 14.0 du plug-in Internet) et de Kaspersky Endpoint Security for Mac (à partir de la version 12.2.1 Correctif A du plug-in Internet).

Activation et désactivation d'une option d'héritage de stratégie

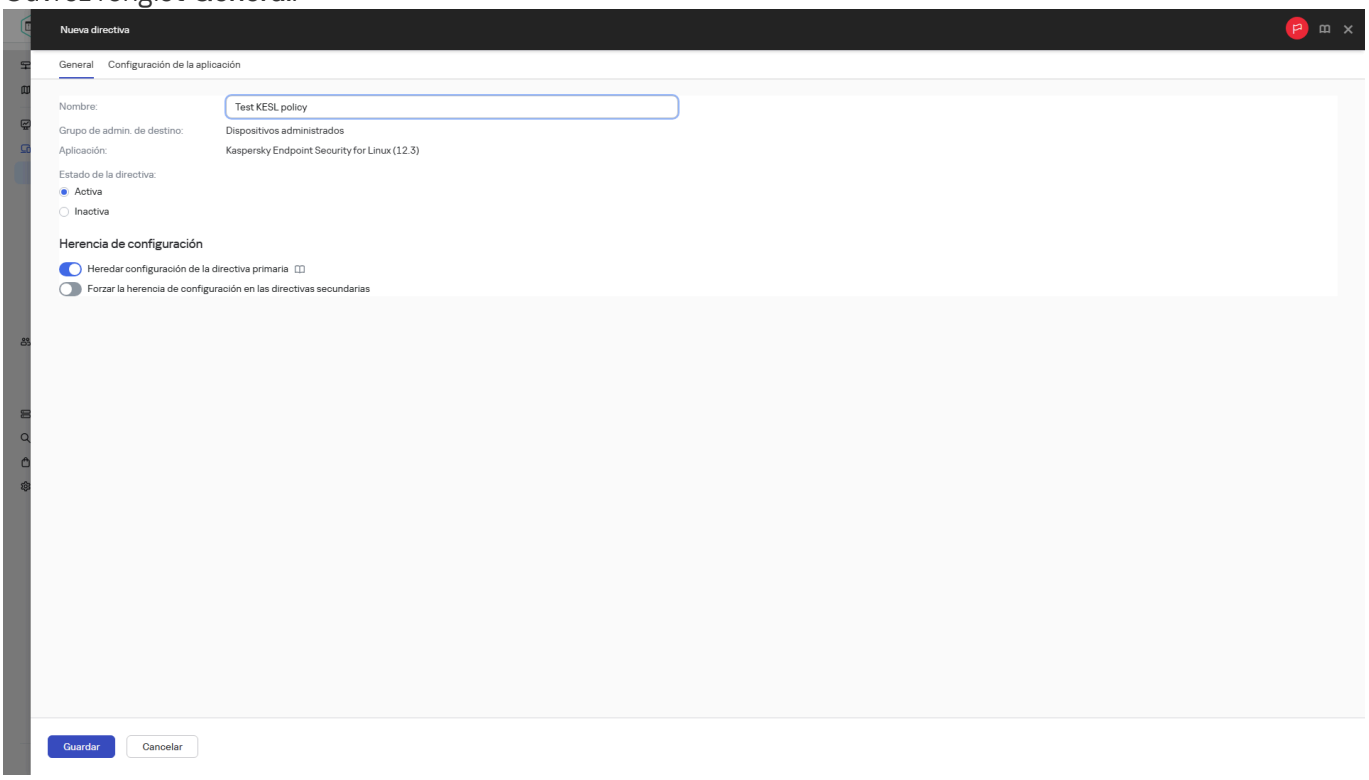
Pour activer ou désactiver l'option d'héritage dans une stratégie :

1. ouvrez la stratégie concernée.



La liste des stratégies

2. Ouvrez l'onglet **Général**.



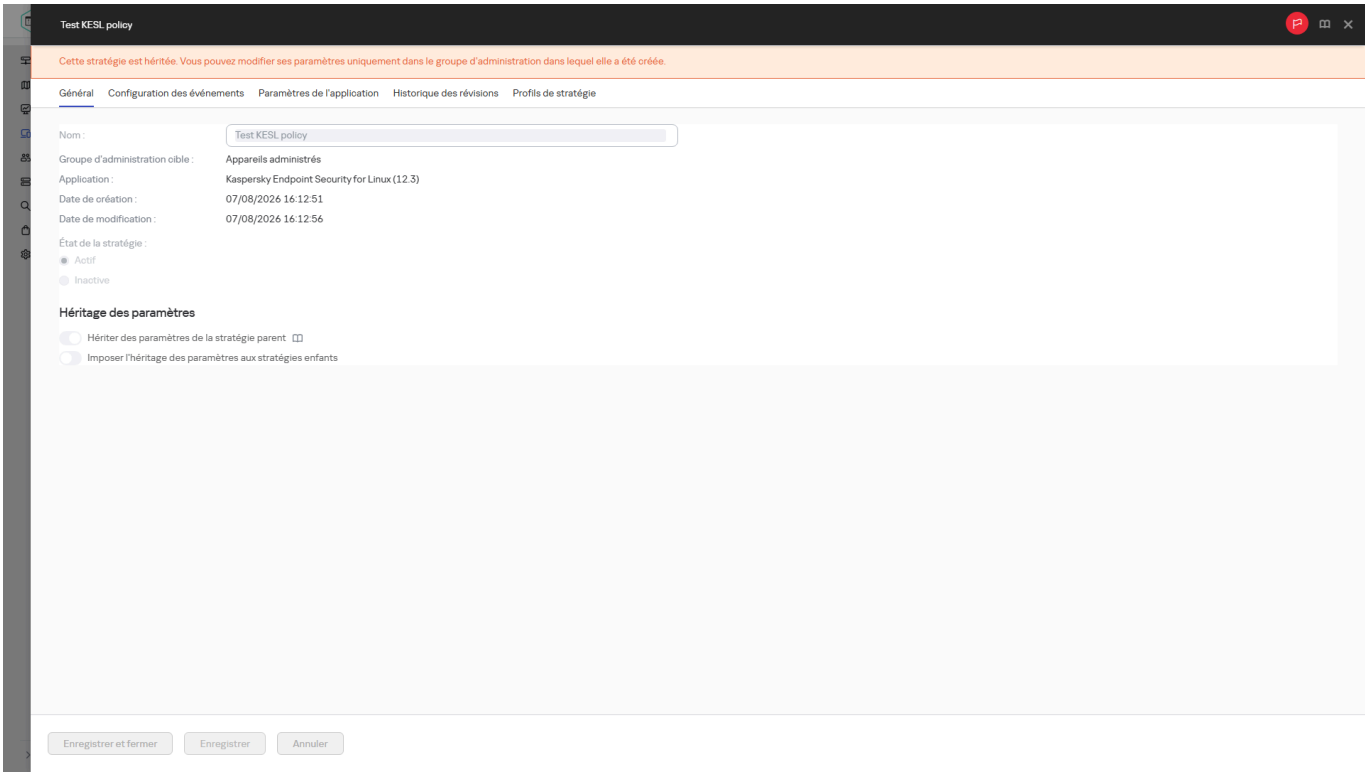
Création d'une stratégie

3. Activez ou désactivez l'héritage de la stratégie :

- si vous activez l'option **Hériter des 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 des 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 des 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.



Paramètres de stratégie verrouillés

4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications ou sur le bouton **Annuler** pour refuser les modifications.

Par défaut, l'option **Hériter des paramètres de la stratégie parent** est activée pour une nouvelle stratégie.

Si une stratégie possède des profils, toutes les stratégies enfants héritent de ces profils.

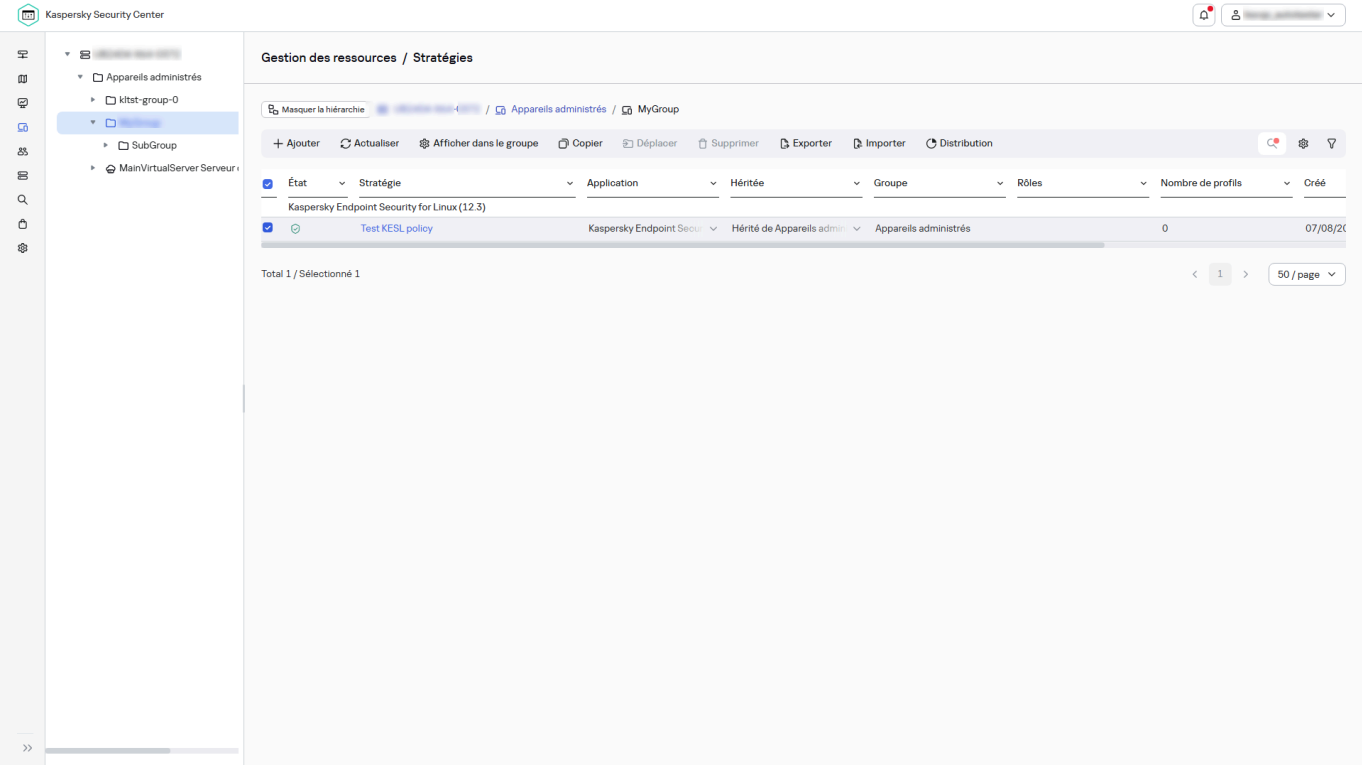
Copie d'une stratégie

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 :

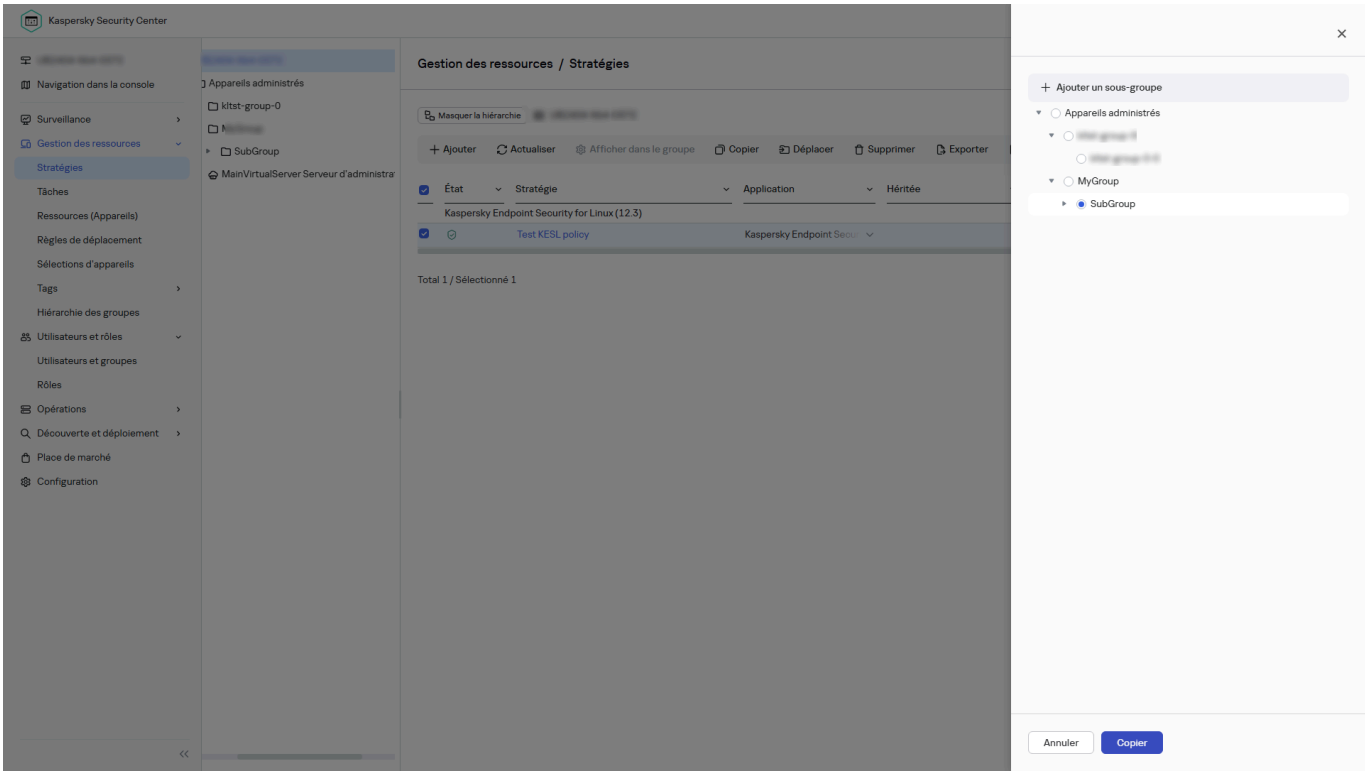
1. Dans le menu principal, accédez à **Gestion des ressources** → **Stratégies**.

2. Cochez la case en regard de la stratégie (ou des stratégies) que vous souhaitez copier.



3. Cliquez sur **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 **Actif** 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

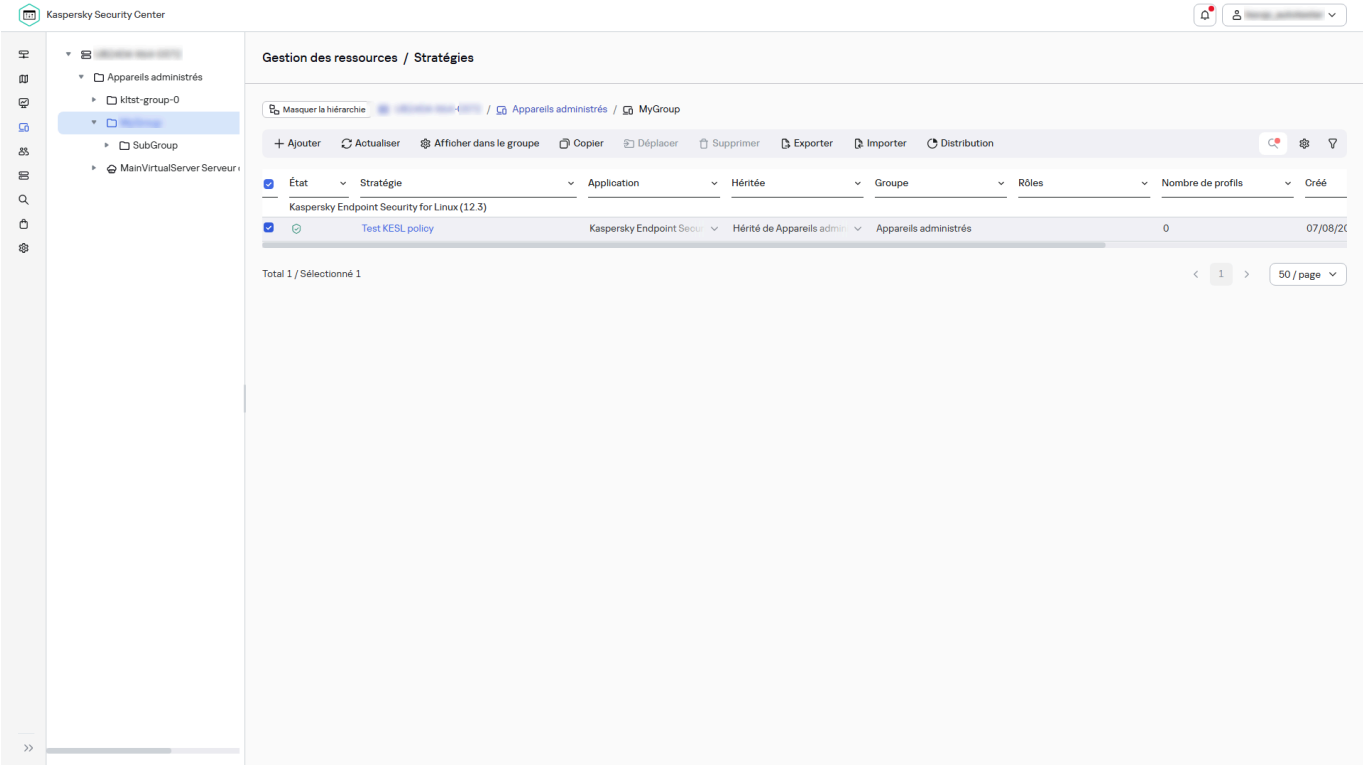
Vous pouvez déplacer les stratégies d'un groupe d'administration vers un autre. Par exemple, vous souhaitez supprimer un groupe mais vous souhaitez utiliser ses stratégies pour un autre groupe. Dans ce cas, vous pourriez vouloir déplacer la stratégie de l'ancien groupe vers le nouveau avant de supprimer l'ancien groupe.

> Lorsqu'une stratégie est déplacée vers un autre groupe d'administration, l'historique des révisions de cette stratégie est effacé. L'onglet **Historique des révisions** affiche uniquement les informations sur la dernière modification.

Pour déplacer une stratégie vers un autre groupe d'administration, procédez comme suit :

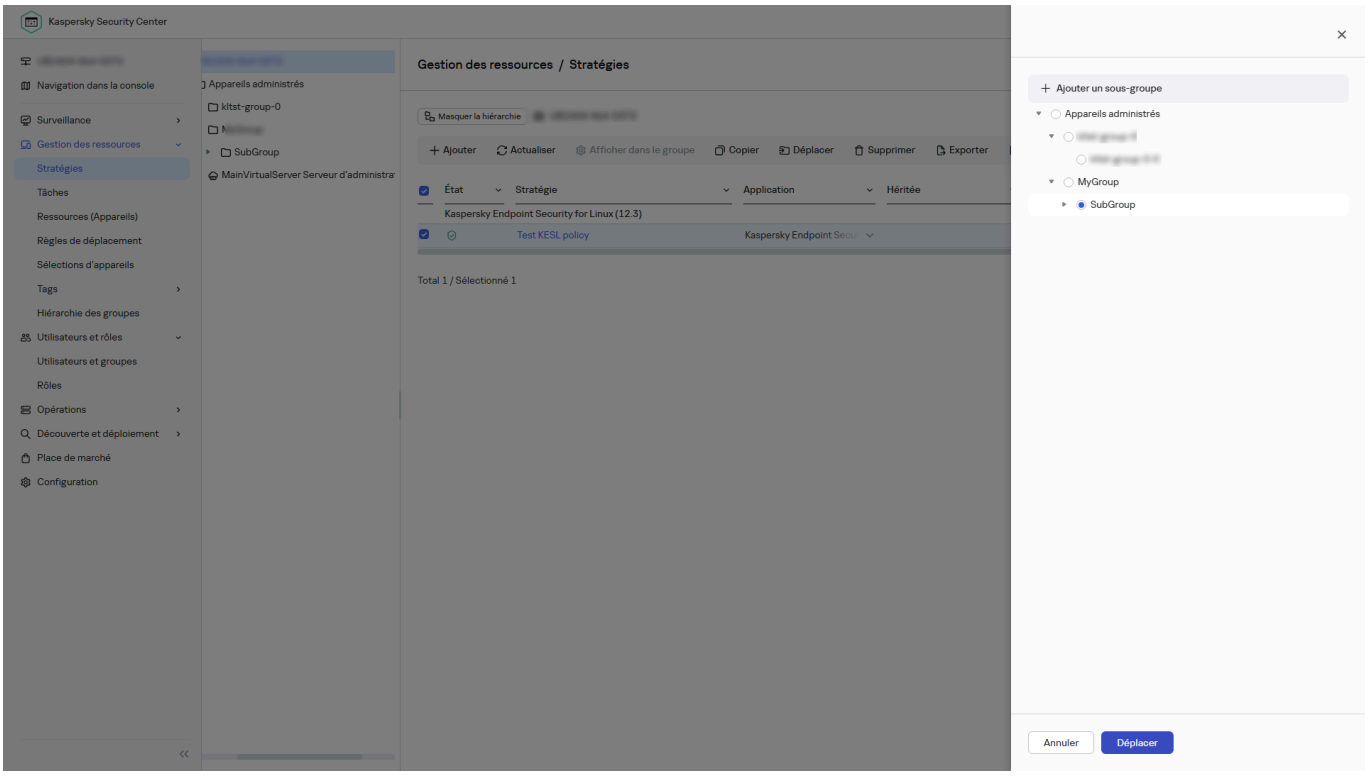
1. Dans le menu principal, accédez à **Gestion des ressources** → **Stratégies**.

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 **Actif** 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 **Actif** 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

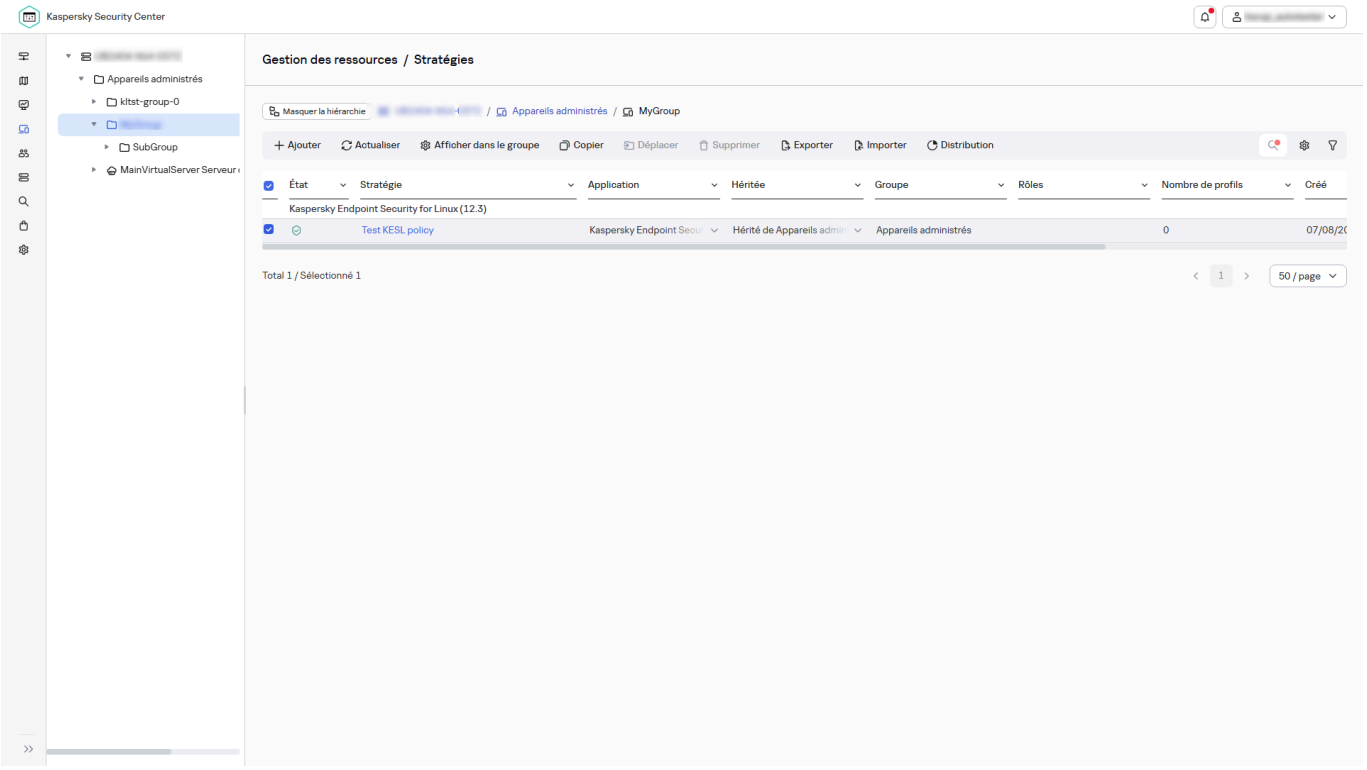
Kaspersky Security Center Linux permet d'enregistrer une tâche, ses paramètres et les profils de stratégie dans un fichier KLP. Vous pouvez utiliser ce fichier KLP pour importer la stratégie enregistrée dans Kaspersky Security Center Windows et Kaspersky Security Center Linux.

Pour exporter une stratégie, procédez comme suit :

1. Dans le menu principal, accédez à **Gestion des ressources** → **Stratégies**.

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.



Sélection d'une stratégie à exporter

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 **Gestion des ressources** → **Stratégies**.

2. Cliquez sur le bouton **Importer**.

3. Cliquez sur le bouton **Parcourir** pour choisir le fichier de stratégie à importer.

4. Dans la fenêtre qui s'ouvre, indiquez le chemin d'accès au fichier de stratégie KLP, puis cliquez sur le bouton **Ouvrir**. Notez que vous ne pouvez sélectionner qu'un seul fichier de stratégie.

   Le traitement de la stratégie démarre.

5. Une fois que la stratégie a été traitée avec succès, sélectionnez le groupe d'administration auquel vous souhaitez appliquer la stratégie.

6. Cliquez sur le bouton **Terminée** pour terminer l'importation de la stratégie.

La notification avec les résultats de l'importation s'affiche. Si la stratégie est importée avec succès, vous pouvez cliquer sur le lien **En savoir plus** pour afficher les propriétés de la stratégie.

Après une importation réussie, la stratégie s'affiche dans la liste des stratégies. Les paramètres et les profils de la stratégie sont également importés. Quel que soit l'état de la stratégie sélectionné lors de l'exportation, la stratégie importée est inactive. Vous pouvez modifier l'état de la stratégie dans les propriétés de la stratégie.

Si la stratégie importée porte le même nom que la stratégie existante, le nom de la stratégie importée est suivi de l'index **(<numéro de séquence suivant>)**, par exemple : **(1)**, **(2)**.

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 **Gestion des ressources** → **Ressources (Appareils)**.

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 :
   - Exécutez une sélection d'appareils pour afficher la liste des appareils.
   - Dans le menu principal, accédez à **Gestion des ressources** → **Ressources (Appareils)**, puis sélectionnez le groupe d'administration qui contient les appareils à synchroniser.
     - Pour le groupe racine, vous pouvez passer à l'étape suivante.
     - Pour un sous-groupe, cliquez sur le bouton **Afficher la hiérarchie** en haut de la page, puis dans la fenêtre qui s'ouvre, cliquez sur le nom du sous-groupe.

       Le chemin vers le groupe sélectionné est affiché en haut de la page. Si nécessaire, vous pouvez cliquer sur un lien avec le nom du groupe d'administration pour accéder au groupe. Par défaut, le dernier lien du chemin est inactif. Vous pouvez également fermer la fenêtre de la hiérarchie en cliquant sur le bouton **Masquer la hiérarchie**.
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 **Gestion des ressources** → **Ressources (Appareils)**.
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.

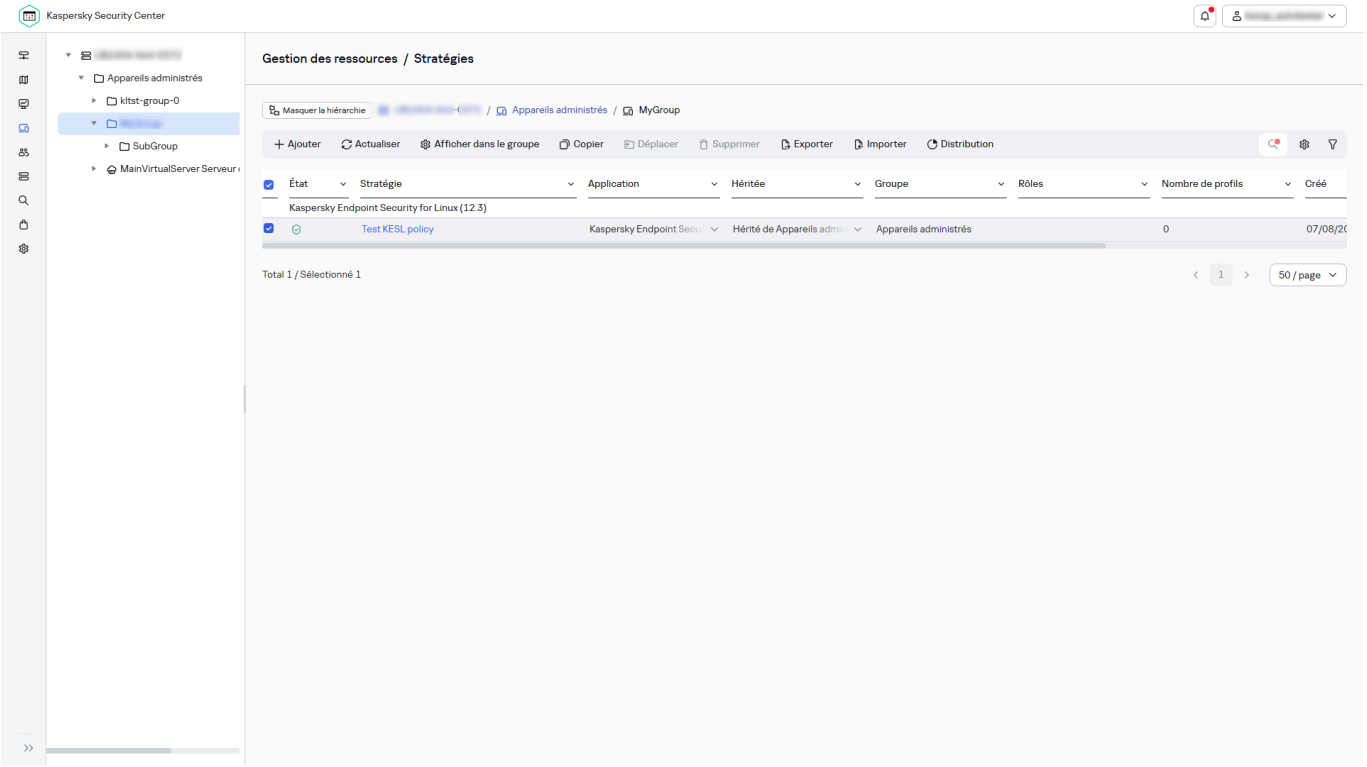
Affichage du graphique de l'état de la distribution des stratégies

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 **Gestion des ressources** → **Stratégies**.

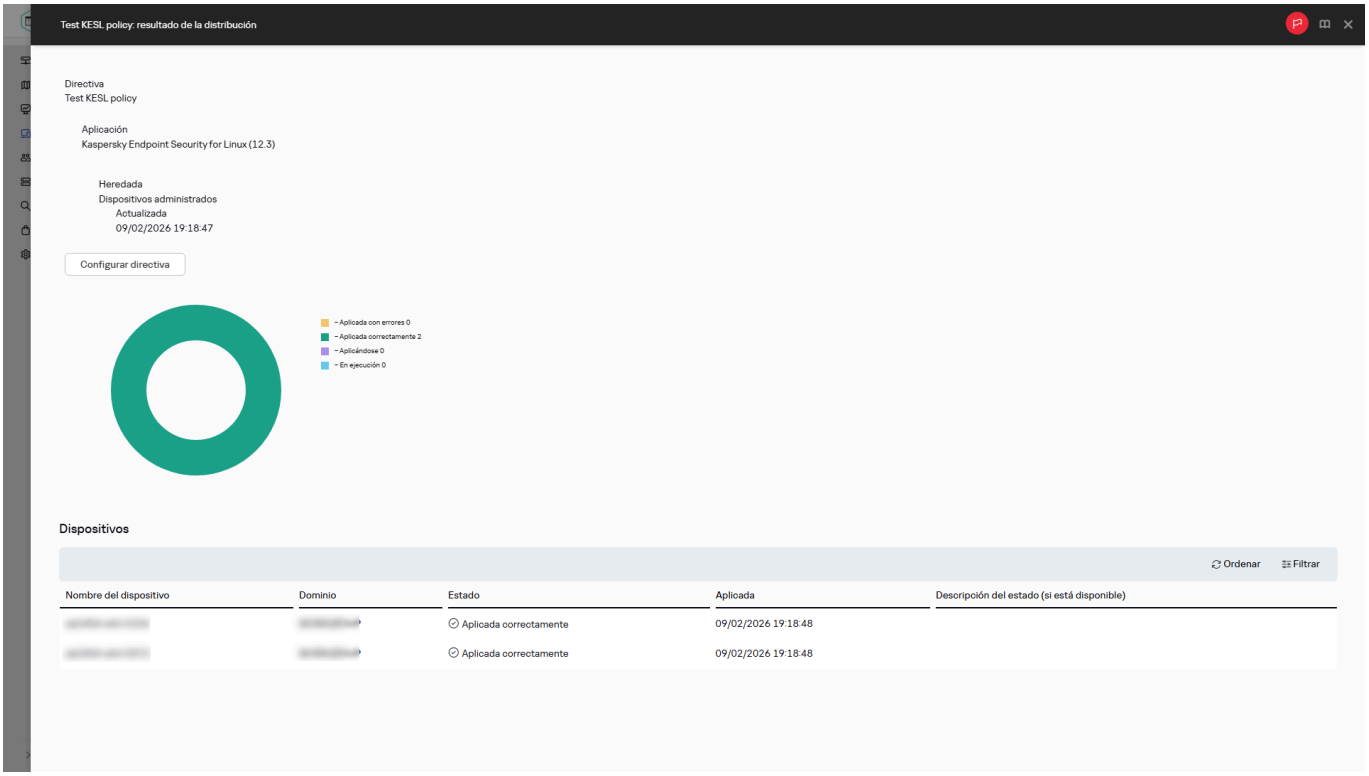
2. Cochez la case située à côté du nom de la stratégie dont vous souhaitez consulter l'état de la distribution sur les appareils.



La liste des stratégies

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.



Les résultats de distribution de la stratégie

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, accédez à **Configuration** → **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.

Activation automatique d'une stratégie lors d'un événement " Propagation de virus "

Pour que la stratégie soit automatiquement activée lors d'un événement « Attaque de virus », procédez comme suit :

1. Dans le menu principal, cliquez sur le nom du Serveur d'administration.

   La fenêtre des propriétés du Serveur d'administration s'ouvre avec l'onglet **Général** sélectionné.

2. Sélectionnez la section **Propagation de virus**.

3. Dans le volet droit, cliquez sur le lien **Configurer l'activation des stratégies dans le cas d'un événement "Propagation de virus"**.

   Le fenêtre **Activation des stratégies** s'ouvre.

4. Dans la section liée au composant qui détecte une propagation de virus (antivirus pour les postes de travail et les serveurs de fichier, antivirus pour les serveurs de messagerie, ou antivirus pour la défense du périmètre) sélectionnez le bouton d'option suivant vers l'entrée souhaitée, puis cliquez sur **Ajouter**.

   Une fenêtre s'ouvre avec le groupe d'administration **Appareils administrés**.

5. Cliquez sur le chevron (>) à côté de **Appareils administrés**.

   Une hiérarchie des groupes d'administration et leurs stratégies s'affiche.

6. Dans la hiérarchie des groupes d'administration et leurs stratégies, cliquez sur le nom d'une stratégie or des stratégies qui sont activées quand une propagation de virus est détectée.

   Pour sélectionner toutes les stratégies d'une liste ou d'un groupe, sélectionnez la case à cocher à côté du nom requis.

7. Cliquez sur **Enregistrer**.

   La fenêtre avec la hiérarchie des groupes d'administration et leurs stratégies est fermée.

Les stratégies sélectionnées sont ajoutées à la liste des stratégies qui sont activées quand une propagation de virus est détectée. Les stratégies sélectionnées sont activées en cas de propagation de virus, qu'elles soient actives ou inactives.

Si une stratégie a été désactivée en fonction de l'événement Propagation de virus, vous ne pouvez rétablir la stratégie précédente que manuellement.

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 **Gestion des ressources** → **Stratégies**.

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, ainsi que la suppression, l'exportation et l'importation de profil de stratégie.

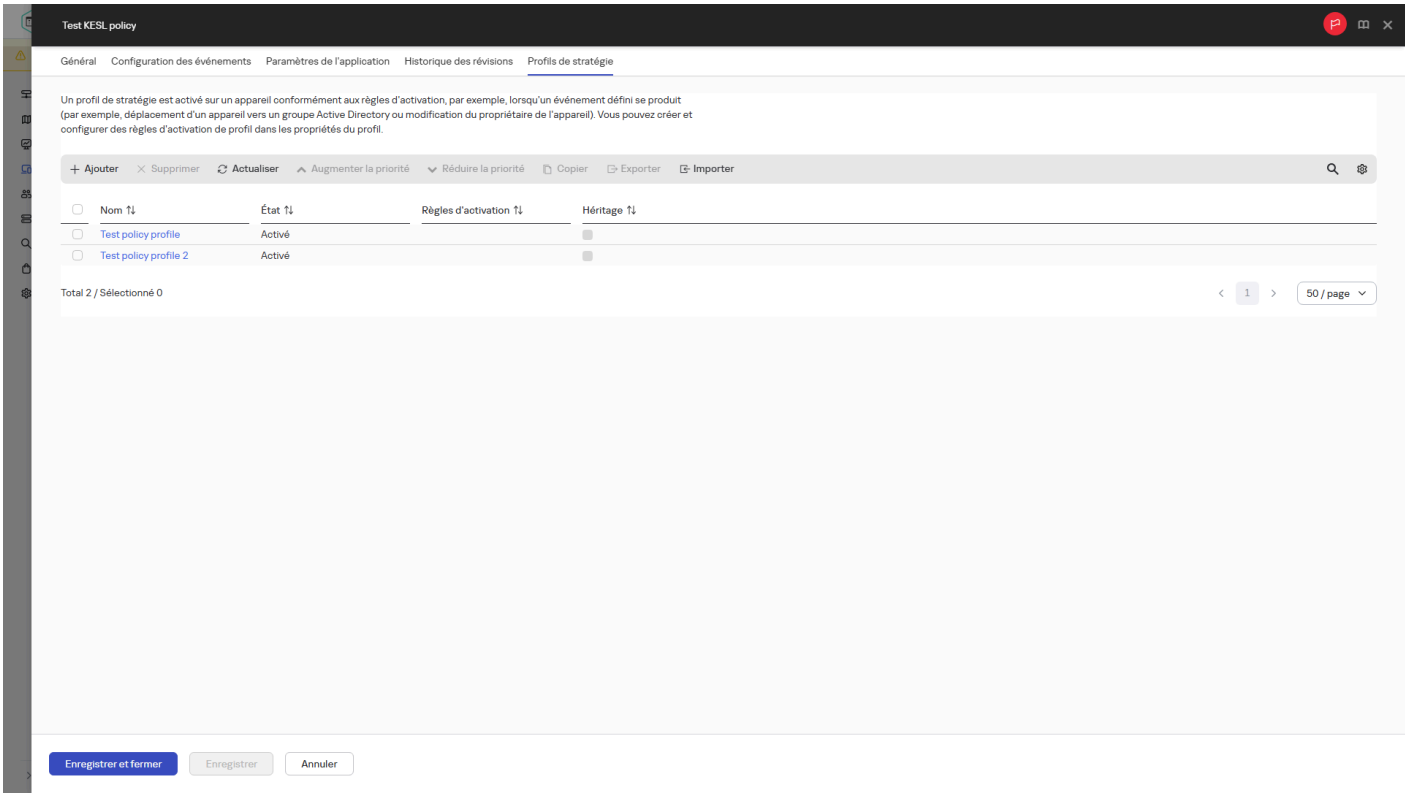
Consultation des profils d'une stratégie

Pour consulter les profils d'une stratégie, procédez comme suit :

1. Dans le menu principal, accédez à **Gestion des ressources** → **Stratégies**.
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.



La liste des profils de la stratégie

Modification de la priorité d'un profil de stratégie

Pour modifier la priorité d'un profil de stratégie, procédez comme suit :

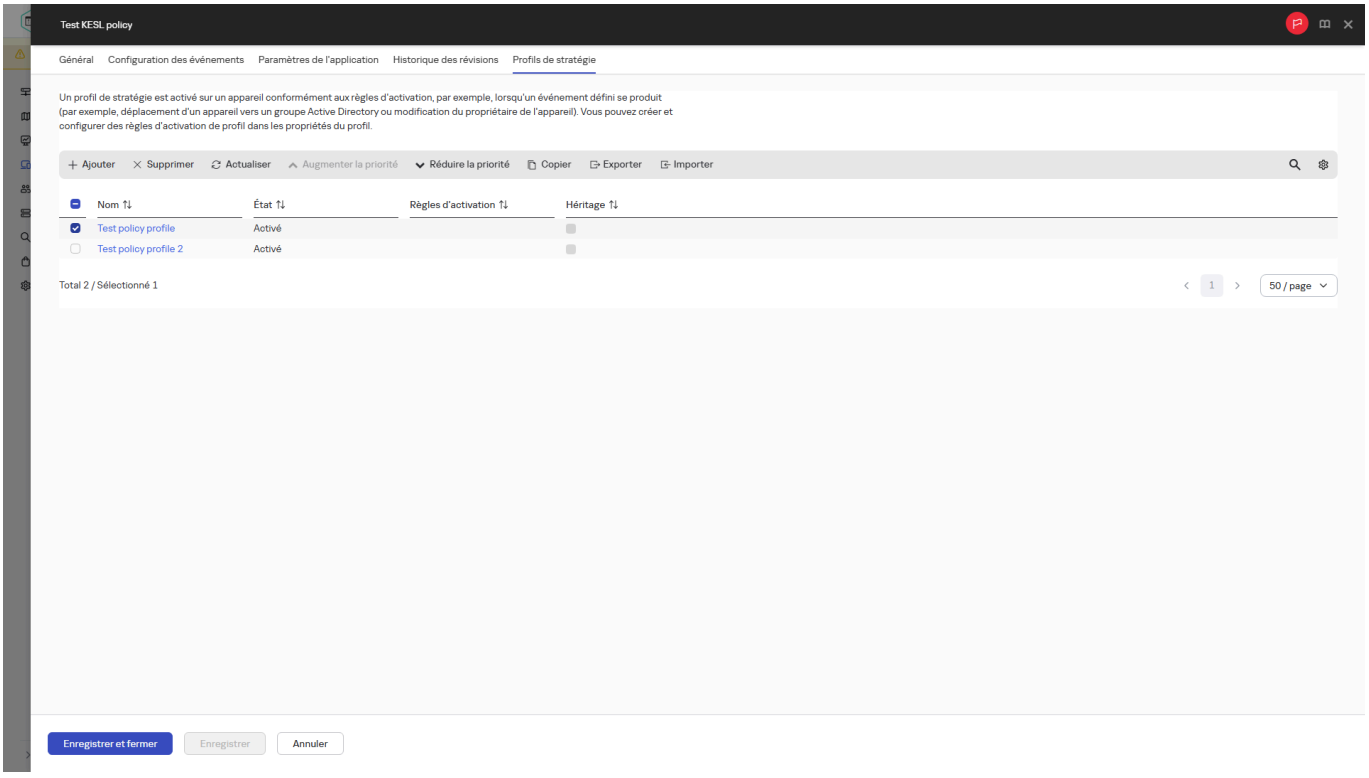
1. Passez à la liste des profils d'une stratégie que vous voulez.

   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

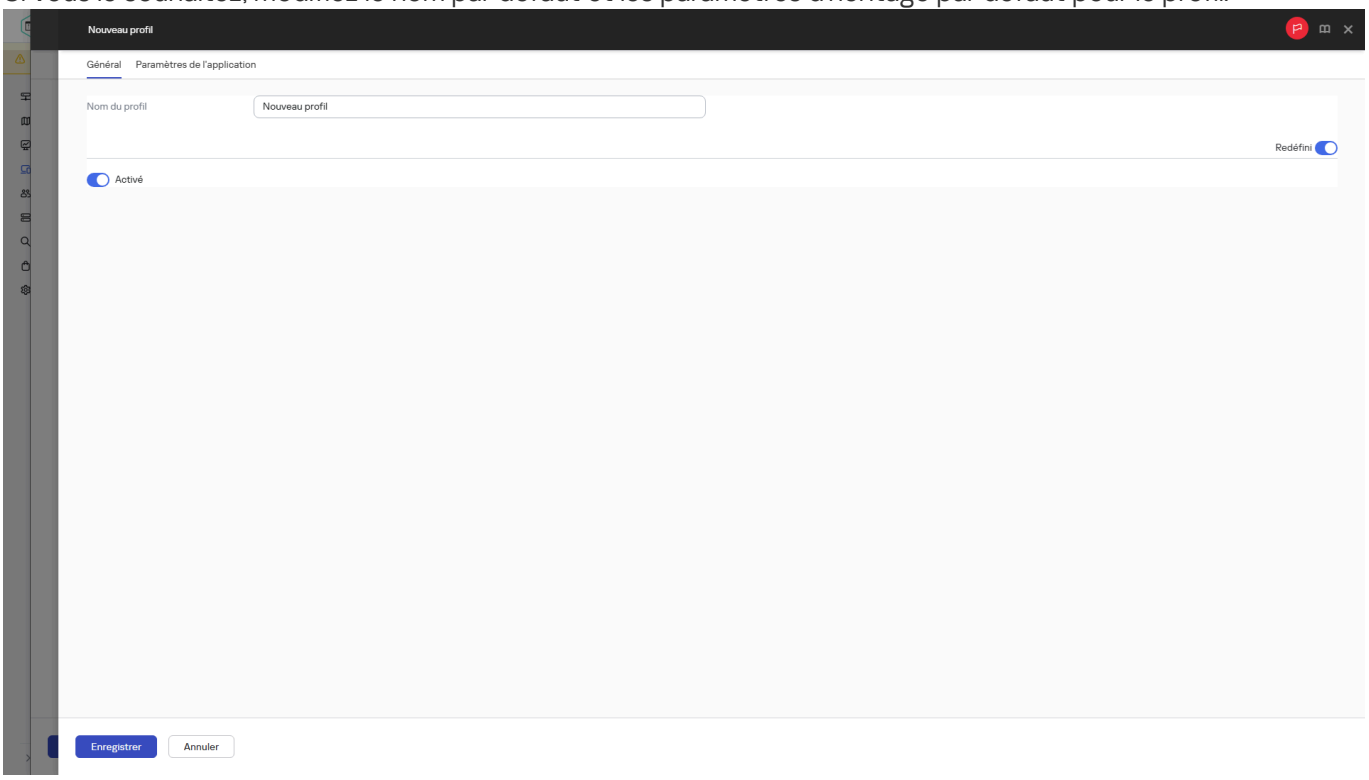
Pour créer un profil de stratégie, procédez comme suit :

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.



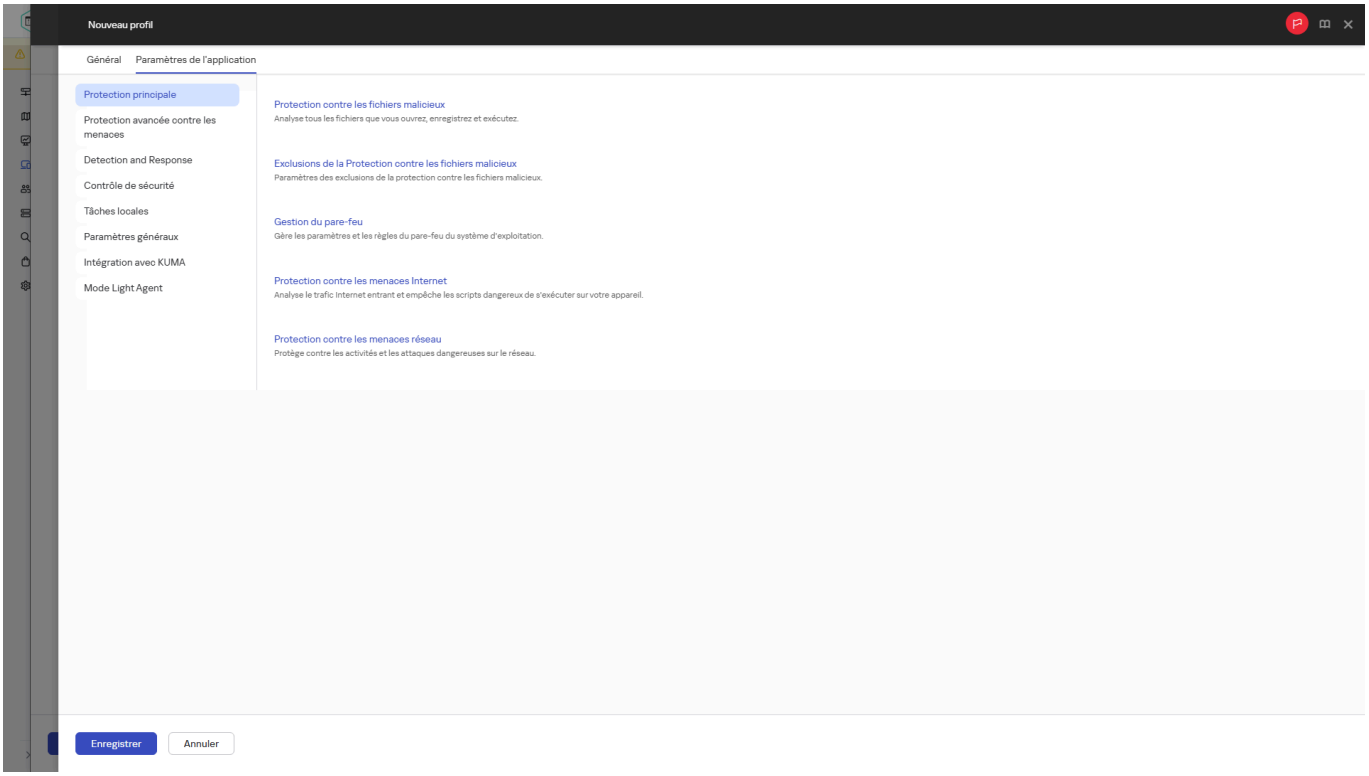
Création d'un profil de stratégie

4. Sélectionnez l'onglet **Paramètres de l'application**.

   Ou vous pouvez cliquer sur **Enregistrer** et quitter. Le profil que vous avez créé apparaît dans la liste des profils des stratégies et vous pouvez modifier ses paramètres ultérieurement.

5. Sous l'onglet **Paramètres de l'application**, sélectionnez dans le volet de gauche la catégorie que vous souhaitez, puis dans le panneau des résultats à droite, modifiez les paramètres du profil. Vous pouvez modifier les paramètres du profil de stratégie dans chaque catégorie (section).

Pendant la modification des paramètres, vous pouvez cliquer sur **Annuler** pour annuler la dernière opération.



Spécification des paramètres du profil de stratégie

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.

Vous pouvez modifier ultérieurement les paramètres du profil de stratégie, y compris son nom et sa priorité. Dans ce cas, le profil de stratégie d'origine n'est pas modifié.

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.

     - **Emplacement réseau de l'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 est repris dans 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 :

  - **Volume de la mémoire (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**

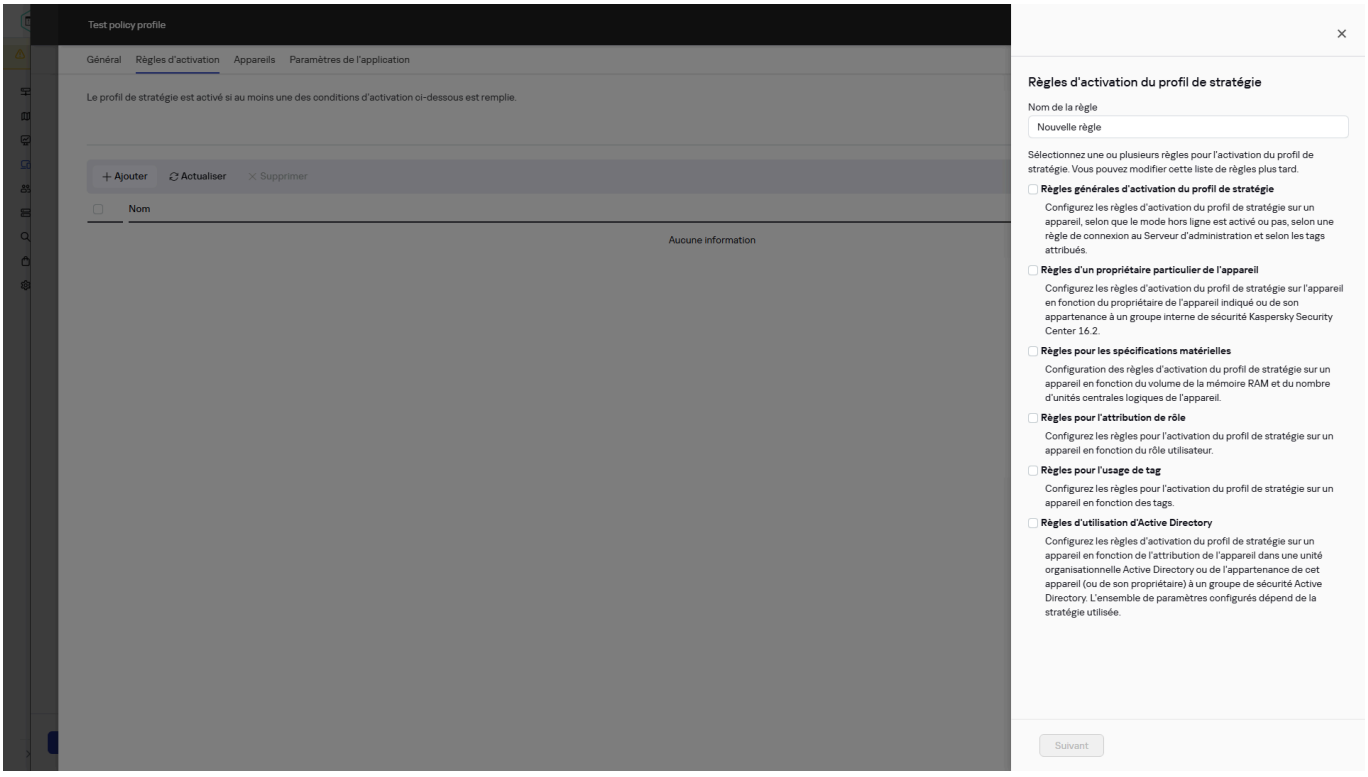
    Si cette option est activée, le profil de stratégie est activé sur l'appareil. Si l'option est désactivée, les critères d'activation du profil ne sont pas appliqués. Cette option est Inactif par défaut.

  - **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.



Création d'une règle d'activation du profil de stratégie

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.

Exportation et importation d'un profil de stratégie

Vous pouvez enregistrer un profil de stratégie dans un fichier KLPROF sans exporter de stratégie, puis utiliser ce fichier KLPROF pour importer le profil enregistré dans la stratégie.

Cela vous permet de restaurer rapidement les paramètres du profil de stratégie, au lieu de les configurer à nouveau.

Un profil de stratégie est importé dans la stratégie de la même version de l'application à partir de laquelle vous avez exporté le profil. Pour les applications qui prennent en charge la rétrocompatibilité des stratégies (par exemple, Kaspersky Endpoint Security for Windows), vous pouvez importer des profils de stratégie dans différentes versions de la stratégie.

Pour exporter un profil de stratégie, procédez comme suit :

1. Passez à la liste des profils d'une stratégie que vous voulez.

   La liste des profils de la stratégie s'ouvre.

2. Sous l'onglet **Profils de stratégie**, cliquez sur le profil de stratégie que vous souhaitez exporter.

3. Dans la barre d'outils, cliquez sur le bouton **Exporter**.

4. Dans la fenêtre qui s'ouvre, indiquez le répertoire dans lequel vous souhaitez enregistrer le fichier contenant le profil de stratégie.

   Vous pouvez modifier le nom du fichier, si nécessaire.

5. Cliquez sur **Enregistrer**.

Si l'opération réussit, un message correspondant s'affiche à l'écran. Dans le cas contraire, un message d'erreur s'affiche.

Pour importer 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. Dans la barre d'outils, cliquez sur le bouton **Importer**.

3. Dans la fenêtre qui s'ouvre, sélectionnez le fichier KLPROF contenant le profil de stratégie requis, puis cliquez sur le bouton **Ouvrir**.

   La taille maximale du fichier importé est de 4 Mo.

Si l'opération réussit, un message correspondant s'affiche à l'écran. Dans le cas contraire, un message d'erreur s'affiche.

Le profil de stratégie est importé sous le nom qu'il portait lors de son exportation, et non sous le nom du fichier KLPROF.
Le fichier est importé avec l'état **Désactivé** et la priorité la plus basse, quelle que soit la priorité du profil de stratégie avant l'exportation.

Un importation est impossible :

- Si la Stratégie possède déjà un profil du même nom.
- Si le nombre de profils dans la stratégie est de 100.

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 de l'application, accédez à **Gestion des ressources** → **Stratégies**.

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 champ **Nom** permet de modifier le nom de la stratégie.
- Le groupe **État de la stratégie** permet de sélectionner l'un des modes de stratégie :
  - **Actif**

    Si cette option a été sélectionnée, la stratégie devient active.

    Cette option est sélectionnée par défaut.

  - **Inactive**

    Si cette option a été sélectionnée, la stratégie devient inactive, mais elle est conservée dans le dossier **Stratégies**. Elle pourra être activée en fonction des besoins.

- Le groupe de paramètres **Héritage des paramètres** permet de configurer l'héritage de la stratégie :
  - **Hériter des 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 détecte un problème de sécurité, vous pouvez gérer ce problème en utilisant les paramètres d'un appareil administré.

Paramètres de l'application

Paramètres

La section **Paramètres** vous permet de configurer les paramètres de la stratégie de l'Agent d'administration :

- **Distribuer les fichiers uniquement via les points de distribution**

  Si cette option est activée, les agents d'administration sur les Appareils administrés récupèrent les mises à jour à partir des points de distribution uniquement.

  Si cette option est désactivée, les agents d'administration sur les appareils administrés récupèrent les mises à jour des points de distribution ou du Serveur d'administration.

  > Notez que les applications de sécurité sur les Appareils administrés récupèrent les mises à jour sur la source définie dans la tâche de mise à jour pour chaque application de sécurité. Si vous activez l'option **Distribuer les fichiers uniquement via les points de distribution**, assurez-vous que Kaspersky Security Center est défini comme source des mises à jour dans les tâches de mise à jour.

Cette option est Inactif par défaut.

- **Taille maximale de la file d'attente d'événements (Mo)**

  Le champ permet d'indiquer l'espace maximal sur le disque, que la file d'attente d'événements peut occuper.

  La valeur par défaut est de 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 :

- **Détails sur les applications installées**

  Si l'option est activée, les informations sur les applications installées sur les appareils clients sont envoyées au Serveur d'administration.

  Cette option est activée par défaut.

- **Inclut les informations sur les correctifs**

  Les informations sur les correctifs des applications installées sur les appareils clients sont envoyées au Serveur d'administration. L'activation de cette option peut augmenter la charge sur le Serveur d'administration et le SGBD, et causer une augmentation du volume de la base de données.

  Cette option est activée par défaut. Il est disponible uniquement pour Windows.

- **Détails sur les mises à jour Windows Update**

  Si cette option est activée, les informations sur les mises à jour Microsoft Windows qui doivent être installées sur les appareils clients sont envoyées au Serveur d'administration.

  Cette option est activée par défaut. Il est disponible uniquement pour Windows.

  Les informations sur les mises à jour facultatives de Microsoft Windows Update ne sont pas envoyées au Serveur d'administration.

- **Détails sur les vulnérabilités dans les applications et les mises à jour correspondantes**

  Si cette option est activée, les informations sur les vulnérabilités des logiciels tiers (y compris les logiciels Microsoft), détectées sur les appareils administrés, et sur les mises à jour du logiciel destinées à corriger les vulnérabilités des logiciels tiers (à l'exception des logiciels Microsoft) sont envoyées au Serveur d'administration.

  La sélection de cette option (**Détails sur les vulnérabilités dans les applications et les mises à jour correspondantes**) augmente la charge du réseau, la charge du disque du Serveur d'administration et la consommation des ressources de l'Agent d'administration.

  Cette option est activée par défaut. Il est disponible uniquement pour Windows.

  Pour administrer les mises à jour des logiciels Microsoft, utilisez l'option **Détails sur les mises à jour Windows Update**.

- **Informations sur le registre du matériel**

  L'Agent d'administration installé sur un appareil envoie des informations sur le matériel de l'appareil au Serveur d'administration. Vous pouvez consulter les détails sur le matériel dans les propriétés de l'appareil.

  Assurez-vous que l'utilitaire lshw est installé sur les appareils Linux à partir desquels vous souhaitez récupérer les détails du matériel. Les détails du matériel récupérés depuis les machines virtuelles peuvent être incomplets en fonction de l'hyperviseur utilisé.

Si la stratégie de l'Agent d'administration bloque la modification ce certains paramètres de cette section, vous ne pouvez pas modifier ceux-ci.

Mises à jour et vulnérabilités du logiciel

Le groupe **Mises à jour et vulnérabilités du logiciel** permet d'activer l'analyse des vulnérabilités dans les fichiers exécutables :

- **Analyser les fichiers exécutables à la recherche de vulnérabilités lors du lancement**

  Si cette option est activée, lors du lancement des fichiers exécutables, leur analyse sur la présence des vulnérabilités est exécutée.

  Cette option est activée par défaut.

Administration du redémarrage

Dans la section **Administration du redémarrage**, vous pouvez définir l'action à exécuter si le système d'exploitation d'un appareil administré doit être redémarré en vue d'une utilisation, d'une installation ou une désinstallation correctes d'une application :

- **Ne pas redémarrer le système d'exploitation**

  Les appareils clients ne redémarrent pas automatiquement après l'opération. Pour arrêter le fonctionnement, il faut redémarrer l'appareil (par exemple, manuellement ou à l'aide d'une tâche d'administration des appareils). Les informations sur la nécessité du redémarrage sont enregistrées dans les résultats de la tâche et dans l'état de l'appareil. Cette option convient aux tâches d' sur les serveurs et autres appareils pour lesquels la continuité des opérations est critique.

- **Redémarrer le système d'exploitation automatiquement si nécessaire**

  Dans ce cas, le redémarrage des appareils clients est toujours exécuté automatiquement, si celui-ci est requis pour terminer l'opération. Cette option convient aux tâches d' sur des appareils pour lesquels des interruptions périodiques sont admises (débranchement, redémarrage).

- **Confirmer l'action auprès de l'utilisateur**

  Le message qui signale que l'appareil client doit être redémarré manuellement s'affiche sur l'écran de l'appareil. Pour cette option, il est possible de configurer des paramètres avancés : le texte du message pour l'utilisateur, la fréquence du message, ainsi que le délai à l'issue duquel le redémarrage sera forcé (sans confirmation de l'utilisateur). Cette option convient le mieux pour les postes de travail sur lesquels les utilisateurs doivent pouvoir sélectionner l'heure de redémarrage qui leur convient le mieux.

Cette option est sélectionnée par défaut.

- **Fréquence de rappel de la nécessité de réaliser l'installation (min.)**

  Quand cette option est activée, l'application invite l'utilisateur à redémarrer le système d'exploitation selon la fréquence indiquée.

  Cette option est activée par défaut. L'intervalle par défaut est de 5 minutes. La valeur peut être comprise entre 1 et 1 440 minutes.

  Si cette option est désactivée, l'invite est affichée une seule fois.

- **Forcer le redémarrage au bout de (min.)**

  Après avoir averti l'utilisateur, l'application force le redémarrage du système d'exploitation à l'issue de l'intervalle défini.

  Cette option est activée par défaut. Le délai par défaut est de 30 minutes. La valeur peut être comprise entre 1 et 1 440 minutes.

- **Forcer la fermeture des applications dans les sessions bloquées**

  Les applications en cours d'exécution peuvent empêcher le redémarrage de l'appareil client. Par exemple, si un document est en train d'être modifié dans un logiciel de traitement de texte et qu'il n'est pas enregistré, l'application n'autorise pas le redémarrage de l'appareil.

  Quand cette option est activée, l'arrêt forcé de ces applications sur un appareil verrouillé doit avoir lieu avant de pouvoir redémarrer l'appareil. Les utilisateurs pourraient perdre toute modification qui n'a pas été enregistrée à ce moment.

  Si cette option est désactivée, un appareil verrouillé n'est pas redémarré. L'état de la tâche sur cet appareil indique qu'il faut redémarrer l'appareil. Les utilisateurs doivent quitter manuellement toutes les applications en cours d'exécution sur les appareils verrouillés, puis redémarrer ces appareils.

  Cette option est Inactif par défaut.

Administration des correctifs et des mises à jour

Dans la section Administration des correctifs et des mises à jour, vous pouvez configurer la réception et la diffusion des mises à jour et l'installation des correctifs vers les appareils administrés :

- **Installer automatiquement les mises à jour et les correctifs nécessaires pour les modules dont l'état est Non défini**

  Si la case est Activé, les correctifs de Kaspersky avec l'état d'approbation *Non défini* s'installent automatiquement sur les appareils administrés juste après avoir été téléchargés depuis les serveurs de mises à jour.

  Si l'option est désactivée, les correctifs de Kaspersky chargés avec l'état *Non défini* sont installés après que l'administrateur a modifié leur état pour qu'il soit *Approuvé*.

  Cette option est activée par défaut.

- **Télécharger au préalable les mises à jour et les bases antivirus depuis le Serveur d'administration (recommandé)**

  Si la case est Activé, le modèle hors ligne de téléchargement des mises à jour est désactivé. Quand le serveur d'administration reçoit des mises à jour, il signale à l'Agent d'administration (sur les appareils où il est installé) les mises à jour qui seront requises pour les applications administrées. Quand l'Agent d'administration reçoit des informations sur les mises à jour, il télécharge les fichiers nécessaires au préalable sur le Serveur d'administration. Lors de la première connexion à Agent d'administration, le Serveur d'administration initialise le téléchargement des mises à jour. Une fois que l'Agent d'administration sur l'appareil client a téléchargé toutes les mises à jour, celles-ci deviennent accessibles aux applications situées sur ce même appareil.

  Lorsque l'application administrée sur l'appareil client s'adresse à l'Agent d'administration pour obtenir des mises à jour, l'Agent vérifie s'il a les mises à jour nécessaires. Si des mises à jour ont été reçues du Serveur d'administration au plus tôt 25 heures après la requête de l'application administrée, l'Agent d'administration ne se connecte pas au Serveur d'administration et fournit à l'application administrée des mises à jour du cache local. Il se peut que la connexion au Serveur d'administration ne soit pas établie lorsque l'Agent d'administration fournit les mises à jour aux applications sur les appareils client, mais la connexion n'est pas requise pour la mise à jour.

  Si l'option est désactivée, le modèle hors ligne de téléchargement des mises à jour n'est pas utilisé. Les mises à jour sont distribuées conformément à la programmation de la tâches de téléchargement des mises à jour.

  Cette option est activée par défaut.

Connectivité

La section **Connectivité** inclut trois sous-sections :

- **Réseau**
- **Profils de connexion**
- **Calendrier de connexion**

Dans la sous-section **Réseau**, vous pouvez configurer la connexion au Serveur d'administration, activer l'utilisation d'un port UDP et spécifier le numéro de port UDP.

- Dans le groupe de paramètres **Se connecter au Serveur d'administration**, vous pouvez configurer les paramètres de connexion au Serveur d'administration et indiquer l'intervalle de synchronisation des appareils clients avec le Serveur d'administration :

  - **Période de synchronisation (min.)**

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

- **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**. Par défaut, cette option est activée. 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.

- **Utiliser un &point de distribution pour forcer la connexion au Serveur d'administration**

  Sélectionnez cette option si vous avez sélectionné l'option **Utiliser ce point de distribution comme serveur push** dans la fenêtre des paramètres du point de distribution. Sinon, le point de distribution n'agira pas comme un serveur push.

La sous-section **Profils de connexion** permet d'indiquer les paramètres d'emplacement réseau et d'activer le mode de l'utilisateur autonome quand le Serveur d'administration n'est pas disponible :

- **Paramètres d'emplacement réseau**

  Les paramètres d'emplacement réseau définissent les caractéristiques du réseau auquel l'appareil client est connecté et spécifient les règles de commutation de l'Agent d'administration d'un profil de connexion du Serveur d'administration sur l'autre en cas de modification des caractéristiques du réseau.

- **Profils de connexion au Serveur d'administration**

  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 :

- **Réseau Windows**

  Cette option n'est disponible que pour les points de distribution sous Windows.

  Si l'option est activée, le Serveur d'administration sonde automatiquement le réseau en respectant la planification défini en cliquant sur les liens **Planifier le sondage rapide** et **Planifier le sondage complet**.

  Si cette option est désactivée, le Serveur d'administration sonde le réseau à l'intervalle indiqué dans le champ **Fréquence des sondages du réseau (min.)**.

  L'intervalle de recherche d'appareils pour les versions de l'Agent d'administration peut être configuré dans les champs **Fréquence des sondages des domaines Windows (min.)** (pour un sondage rapide du réseau Windows) et **Fréquence des sondages du réseau (min.)** (pour un sondage complet du réseau Windows).

  Cette option est Inactif par défaut.

- **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.

- **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.

- **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**

  Si cette option est activée, un serveur proxy internet est utilisé pour connecter les points de distribution aux serveurs de mise à jour de Kaspersky.

- **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.

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 TCP**

  Le numéro du port TCP que les appareils administrés utilisent pour se connecter au serveur proxy KSN. Le numéro de port par défaut est 13111.

- **Port UDP**

  Si vous avez besoin que l'Agent d'administration se connecte au Serveur d'administration via un port UDP, activez l'option **Utiliser le port UDP** et indiquez le **Numéro de port UDP**. Par défaut, cette option est activée. Par défaut, la connexion au Serveur d'administration est exécutée via le port UDP 15000.

- **Port HTTPS**

  Si vous souhaitez que les appareils administrés se connectent au serveur proxy KSN via un port HTTPS, activez l'option **Utiliser HTTPS**, puis spécifiez un numéro de port dans le champ **Port HTTPS**. Cette option est Inactif par défaut. Par défaut, la connexion au serveur proxy KSN est exécutée via le port HTTPS 17111.

Mises à jour (Points de distribution)

Dans la section **Mises à jour (Points de distribution)**, vous pouvez activer la fonctionnalité de téléchargement de fichiers diff, pour que les points de distribution prennent donc les mises à jour sous la forme de fichiers diff à partir des serveurs de mise à jour de Kaspersky.

Gestion des comptes locaux (Linux uniquement)

La section **Gestion des comptes locaux (Linux uniquement)** comprend trois sous-sections :

- **Gestion des certificats utilisateurs**
- **Ajouter ou modifier les groupes d'administration locale applicables**
- **Charger un fichier de référence pour protéger le fichier sudoers sur l'appareil de l'utilisateur contre toute modification**

La sous-section **Gestion des certificats utilisateurs** permet d'indiquer les certificats racines à installer. Ces certificats peuvent servir, par exemple, à vérifier l'authenticité de sites Internet ou de serveurs Internet.

- **Installer les certificats racine**

  Si l'option est activée, les certificats ajoutés au tableau seront installés sur les appareils spécifiés.

  Si cette option est désactivée, aucun certificat ne sera installé sur les appareils spécifiés.

  Cette option est Inactif par défaut.

- **Ajouter**

  Cliquez sur ce bouton pour ouvrir la fenêtre dans laquelle vous pouvez ajouter un certificat.

  La taille du certificat doit être inférieure à 10 Mo.

  Kaspersky Security Center prend en charge les certificats avec les extensions CER, CRT, CERT, PEM et KEY.

Dans la sous-section **Ajouter ou modifier les groupes d'administration locale applicables**, vous pouvez gérer les groupes d'administrateurs locaux. Ces groupes sont utilisés, par exemple, lors de la révocation des droits d'administrateur local. Vous pouvez également consulter la liste des comptes utilisateurs à privilèges à l'aide du **Rapport sur les utilisateurs d'appareils à privilèges (Linux uniquement)**.

- **Ajouter**

  Cliquez sur ce bouton pour ouvrir la fenêtre dans laquelle vous pouvez ajouter un groupe d'administrateurs locaux.

- **Modifier**

  Cliquez sur ce bouton pour ouvrir la fenêtre dans laquelle vous pouvez modifier le groupe des administrateurs locaux.

  Ce bouton est accessible si la case en regard du groupe d'administrateurs local est cochée.

- **Supprimer ;**

  Cliquez sur ce bouton pour supprimer du tableau le groupe d'administrateurs locaux sélectionné.

Ce bouton est accessible si la case en regard du groupe d'administrateurs local est cochée.

Dans la sous-section **Charger un fichier de référence pour protéger le fichier sudoers sur l'appareil de l'utilisateur contre toute modification**, vous pouvez configurer la gestion du fichier sudoers. Les groupes privilégiés et les utilisateurs d'appareils sont définis dans le fichier sudoers sur l'appareil. Le fichier sudoers se trouve dans `/etc/sudoers`. Vous pouvez charger un fichier sudoers de référence pour protéger le fichier sudoers contre toute modification. Cette mesure empêchera toute modification indésirable du fichier sudoers.

Un fichier de référence sudoers non valide peut entraîner un dysfonctionnement de l'appareil de l'utilisateur.

- **Contrôler le fichier sudoers**

  Si l'option est activée, le fichier sudoers sera remplacé par le fichier sudoers de référence actuel.

  Si l'option est désactivée, le fichier sudoers reste inchangé.

  Cette option est Inactif par défaut.

- **Fichier de référence sudoers**

  Ce champ affiche le nom du fichier sudoers de référence chargé.

- **Charger**

  Cliquez sur ce bouton pour ouvrir la fenêtre dans laquelle vous pouvez charger le fichier de référence sudoers.

- **Fichier sudoers de référence actuel**

  Cliquez sur ce bouton pour afficher le contenu du fichier sudoers actuel.

Historique des révisions

Sous l'onglet **Historique des révisions**, vous pouvez :

- Consulter et enregistrer l'historique des révisions des stratégies.
- Restaurer une révision des stratégies.
- Ajouter et modifier des descriptions de révisions des stratégies.
- Comparer les révisions de la stratégie.

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	✓ Limitation : non pris en charge par l'Agent d'administration pour Microsoft Windows sur l'architecture ARM.	✓	✓
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	✓	✓	✓ À l'exception des serveurs push
Point de distribution			
Utilisation comme point de distribution	✓ Limitation : non pris en charge par l'Agent d'administration pour Microsoft Windows sur l'architecture ARM.	✓	✓
Calcul de la quantité et de la configuration des points de distribution	✓ Limitation : non pris en charge par l'Agent d'administration pour Microsoft Windows sur l'architecture ARM.	✓ Sans utiliser la reconnaissance de l'emplacement réseau (NLA).	✓ Sans utiliser la reconnaissance de l'emplacement réseau (NLA).

Fonctionnalité de l'Agent d'administration	Windows	Linux	macOS
Modèle hors ligne de téléchargement des mises à jour	✓ Limitation : non pris en charge par l'Agent d'administration pour Microsoft Windows sur l'architecture ARM.	✓	✓
Sondage réseau	✓ • Sondage des plages IP • Sondage du contrôleur de domaine (Microsoft Active Directory) Limitation : non pris en charge par l'Agent d'administration pour Microsoft Windows sur l'architecture ARM.	✓ Sondage des plages IP Sondage Zeroconf Sondage du contrôleur de domaine (Microsoft Active Directory, Samba 4 Active Directory, FreeIPA, ALD Pro)	—
Activer le service KSN proxy côté point de distribution	✓ Limitation : non pris en charge par l'Agent d'administration pour Microsoft Windows sur l'architecture ARM.	✓	—
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	✓ Limitation : non pris en charge par l'Agent d'administration pour Microsoft Windows sur l'architecture ARM.	✓	— (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	✓ Limitation : non pris en charge par l'Agent d'administration pour Microsoft Windows sur l'architecture ARM.	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	✓ Limitation : non pris en charge par l'Agent d'administration pour Microsoft Windows sur l'architecture ARM.	✓	—
Administration des applications tierces			
Installation à distance des applications sur les appareils	✓	✓	✓ Consultez l'article suivant : Installation à distance d'applications sur les appareils macOS.
Configuration des mises à jour du système d'exploitation dans une stratégie d'Agent d'administration	✓ Limitation : non pris en charge par l'Agent d'administration pour Microsoft Windows sur l'architecture ARM.	—	—
Consultation des informations relatives aux vulnérabilités dans les applications	✓ Limitation : non pris en charge par l'Agent d'administration pour Microsoft Windows sur l'architecture ARM.	—	—

Fonctionnalité de l'Agent d'administration	Windows	Linux	macOS
Recherche de vulnérabilités dans les applications	✓ Limitation : non pris en charge par l'Agent d'administration pour Microsoft Windows sur l'architecture ARM.	—	—
Mises à jour du logiciel	✓ Limitation : non pris en charge par l'Agent d'administration pour Microsoft Windows sur l'architecture ARM.	—	—
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)	✓ Limitation : non pris en charge par l'Agent d'administration pour Microsoft Windows sur l'architecture ARM.	✓	✓
Prise en charge des machines virtuelles dynamiques	✓ Limitation : non pris en charge par l'Agent d'administration pour Microsoft Windows sur l'architecture ARM.	✓	✓
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	✓	✓	✓
Profils de connexion pour les utilisateurs itinérants	✓	✓	✓
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. Utilitaire klnagchk	✓	✓	✓

Fonctionnalité de l'Agent d'administration	Windows	Linux	macOS
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.	✓ Les informations sur le matériel des appareils macOS envoyées au Serveur d'administration par l'Agent d'administration installé sur ces appareils se limitent aux informations spécifiées dans la description des paramètres des appareils administrés.

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**	✓ L'option **Informations sur le registre du matériel** est disponible.
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	✓	✓	✓

Section Paramètres	Windows	Linux	macOS
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	✓	✓	✓

Activation et désactivation du mode de faible consommation de ressources pour l'Agent d'administration

Le mode de faible consommation de ressources permet de limiter l'utilisation de la mémoire vive de l'Agent d'administration installé sur l'appareil client. Par défaut, le mode de faible consommation de ressources est désactivé.

En mode de faible consommation de ressources, les fonctionnalités suivantes ne sont pas exécutées :

- L'Agent d'administration ne peut pas être affecté à la fonction de point de distribution (que ce soit manuellement ou automatiquement).
- L'Agent d'administration n'enregistre pas les informations relatives à l'état de l'Agent d'administration dans un fichier texte distinct.
- L'Agent d'administration ne prend pas en charge le modèle hors ligne de téléchargement des mises à jour.
- Les modules et processus suivants sont désactivés :
  - Obtention d'informations sur les mises à jour tierces et les vulnérabilités.
  - Exécution du proxy KSN du côté du point de distribution.
  - Chargement des mises à jour dans le stockage des points de distribution.
  - Contournement du blocage du serveur DNS.
  - Obtention d'informations concernant l'espace libre du disque.

Les modules et les processus reprennent leur fonctionnement après la désactivation du mode de faible consommation de ressources.

Pour activer le mode de faible consommation de ressources, procédez comme suit :

1. Exécutez la commande suivante dans la ligne de commande de l'appareil client :

   ```
   sudo /opt/kaspersky/klnagent64/sbin/klscflag -fset -pv klnagent -n
   KLNAG_FLAG_TEST_VM_PERF -t d -v 1
   ```

2. Redémarrez l'Agent d'administration à l'aide de la commande suivante :

   ```
   sudo service klnagent64 restart
   ```

3. Dans le journal du système d'exploitation, vérifiez si l'entrée **L'Agent d'administration de Kaspersky Security Center fonctionne en mode de faible consommation de ressources** s'affiche.

Le mode de faible consommation de ressources est activé.

Pour désactiver le mode de faible consommation de ressources, procédez comme suit :

1. Exécutez la commande suivante dans la ligne de commande de l'appareil client :

   ```
   sudo /opt/kaspersky/klnagent64/sbin/klscflag -fset -pv klnagent -n
   KLNAG_FLAG_TEST_VM_PERF -t d -v 0
   ```

2. Redémarrez l'Agent d'administration à l'aide de la commande suivante :

   ```
   sudo service klnagent64 restart
   ```

Le mode de faible consommation de ressources est désactivé.

Vous pouvez aussi activer à distance le mode de faible consommation de ressources à l'aide de la tâche *Exécuter des scripts à distance*.

Configuration des paramètres de protection des applications administrées

Pour configurer les paramètres de protection des applications Kaspersky administrées, vous pouvez utiliser des stratégies.

Pour en savoir plus sur la configuration des stratégies de Kaspersky Endpoint Security, consultez l'aide correspondante :

- Aide de Kaspersky Endpoint Security for Windows
- Aide de Kaspersky Endpoint Security for Linux
- Aide de Kaspersky Endpoint Security for Mac

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 sur les stockages** quand la case **Adopter un décalage aléatoire automatique pour les lancements de tâche** est cochée.

Configuration manuelle d'une tâche de groupe d'analyse de l'appareil de Kaspersky Endpoint Security

L'Assistant de configuration initiale de l'application crée la tâche de groupe d'analyse d'un appareil. 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.

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 à Kaspersky Security Network, vous acceptez de fournir automatiquement à Kaspersky des informations sur le fonctionnement des applications de sécurité installées sur les ordinateurs et les appareils mobiles administrés à l'aide de 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. 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. 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 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.

  Vous pouvez configurer les paramètres d'accès de Kaspersky Private Security NetworK dans la section **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 **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) dans les propriétés du Serveur d'administration ou d'un point de distribution.

Pour configurer l'accès du Serveur d'administration à KSN dans les propriétés du Serveur d'administration :

1. Dans le menu principal, cliquez sur le nom du Serveur d'administration.

   La fenêtre des propriétés du Serveur d'administration s'ouvre.

2. Sous l'onglet **Général**, sélectionnez la section **Proxy KSN**.

3. Basculez le commutateur sur la position **Activer le proxy KSN sur le Serveur d'administration Activé**.

   Si cette option est activée, le serveur proxy KSN envoie des données à KSN pour augmenter l'efficacité des modules de Kaspersky Security Center et améliorer les performances des applications de Kaspersky. La transmission des informations depuis les appareils clients vers KSN est régie par la stratégie Kaspersky Endpoint Security active sur ces appareils. Si ce commutateur est désactivé, la transmission des données depuis le Serveur d'administration ou les appareils clients vers KSN via le Kaspersky Security Center 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. Sélectionnez la solution d'infrastructure KSN.

   Dans la sous-section **Participation à KSN**, exécutez une des actions suivantes :

   - Si vous utilisez KSN global, basculez le commutateur sur la position **Utiliser Kaspersky Security Network Activé**.

     Une fois que vous avez activé cette option, vous devez lire et accepter la Déclaration KSN.

   - Si vous utilisez KPSN, basculez le commutateur sur la position **Utiliser Kaspersky Private Security Network Activé** et cliquez sur le bouton **Sélectionner le fichier de paramètres de proxy KSN** pour télécharger les paramètres du KPSN (fichiers avec les extensions .pkcs7 et .pem). Suite au téléchargement des paramètres, l'interface affiche le nom du fournisseur, ses coordonnées et la date de création du fichier avec les paramètres de KPSN.

   Lorsque vous basculez le commutateur sur la position **Utiliser Kaspersky Private Security Network Activé**, un message s'affiche avec des détails sur le KPSN.

   Les applications Kaspersky suivantes prennent en charge KPSN :

   - Kaspersky Security Center 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 **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 **Port HTTPS**. Cette option est désactivée et le port TCP est utilisé par défaut. Si cette option est activée, la connexion au serveur proxy KSN est exécutée par défaut via le port HTTPS 17111.

7. Basculez le commutateur sur la position **Connecter les Serveurs d'administration secondaires à KSN via le Serveur d'administration principal Activé**.

   Si cette option est activée, les Serveurs d'administration secondaires utilisent le Serveur d'administration principal comme serveur proxy KSN. Si cette option est désactivée, les Serveurs d'administration secondaires se connectent au KSN indépendamment. Dans ce cas, les appareils administrés utilisent les Serveurs d'administration secondaires comme serveurs proxy KSN.

   Les Serveurs d'administration secondaires utilisent le Serveur d'administration principal comme serveur proxy si dans le volet droit de la section **Proxy KSN**, dans les propriétés des Serveurs d'administration secondaires, le commutateur est sur la position **Activer le proxy KSN sur le Serveur d'administration Activé**.

8. Cliquez sur le bouton **Enregistrer**.

Les paramètres d'accès à KSN sont enregistrés.

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 le nom du Serveur d'administration.

   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 le nom du Serveur d'administration.

   La fenêtre des propriétés du Serveur d'administration s'ouvre.

2. Sous l'onglet **Général**, sélectionnez la section **Proxy KSN**.

3. Placez le commutateur **Activer le proxy KSN sur le Serveur d'administration** sur Activé.

Le serveur proxy KSN est activé et envoie des données à KSN pour augmenter l'efficacité des modules de Kaspersky Next XDR Expert 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, placez le commutateur **Utiliser Kaspersky Security Network sur Activé**.

     L'envoi de données à KSN est désormais disponible. Une fois que vous avez activé cette option, vous devez lire et accepter la Déclaration KSN.

   - Si vous utilisez KPSN, placez le commutateur **Utiliser Kaspersky Private Security Network** sur Activé, puis cliquez sur le bouton **Sélectionner le fichier de paramètres de proxy KSN** pour charger les paramètres KPSN (fichiers portant 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 placez le commutateur **Utiliser Kaspersky Private Security Network** sur Activé, un message contenant des informations détaillées sur KPSN s'affiche.

2. Cliquez sur **Enregistrer**.

Pour désactiver l'utilisation de KSN, procédez comme suit :

1. Dans le menu principal, cliquez sur le nom du Serveur d'administration.

   La fenêtre des propriétés du Serveur d'administration s'ouvre.

2. Sous l'onglet **Général**, sélectionnez la section **Proxy KSN**.

3. Placez le commutateur **Activer le proxy KSN sur le Serveur d'administration** sur Désactivé pour désactiver le Service KSN Proxy.

4. Cliquez sur le bouton **Enregistrer**.

Affichage de la Déclaration KSN acceptée

Lorsque vous activez Kaspersky Security Network (KSN), vous devez lire et accepter la Déclaration KSN. Vous pouvez consulter à tout moment la déclaration KSN.

Pour afficher la Déclaration KSN acceptée, procédez comme suit :

1. Dans le menu principal, cliquez sur le nom du Serveur d'administration.

   La fenêtre des propriétés du Serveur d'administration s'ouvre.

2. Sous l'onglet **Général**, sélectionnez la section **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 de 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.

Consultation des statistiques du serveur proxy KSN

Kaspersky Security Center Web Console vous permet de consulter les statistiques d'utilisation du serveur proxy KSN.

Les statistiques incluent les paramètres suivants :

- État de la connexion à KSN

- Nombre d'enregistrements de cache

- Nombre de paquets traités dans le cache
- Nombre de paquets reçus

Si vous utilisez KPSN comme solution d'infrastructure, les statistiques d'utilisation de KPSN seront affichées.

Pour consulter les statistiques :

1. Dans le menu principal, cliquez sur le nom du Serveur d'administration.

   La fenêtre des propriétés du Serveur d'administration s'ouvre.

2. Dans l'onglet **Général**, sélectionnez la section **Proxy KSN**, puis ouvrez l'onglet **Statistiques**.

   Cet onglet affiche les statistiques réelles d'utilisation du serveur proxy KSN. Les statistiques sont actualisées toutes les 15 secondes.

Vous pouvez copier les statistiques en cliquant sur le bouton **Copier dans le presse-papiers**.

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. Vous pouvez également sélectionner les appareils détectés sur le réseau par le Serveur d'administration.

- 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 **Gestion des ressources** → **Tâches**.

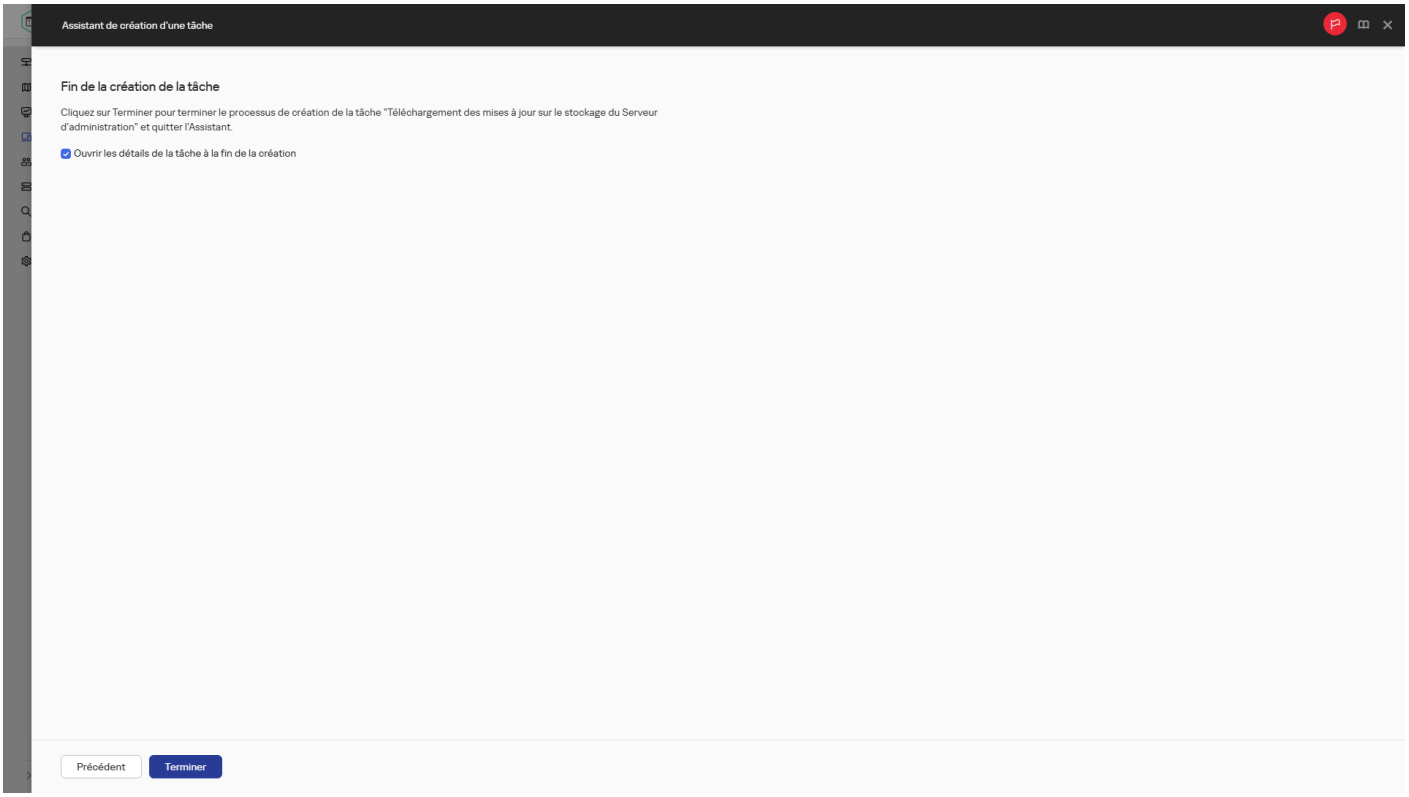
2. Cliquez sur **Ajouter**.

   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.



Fin de la création de la tâche

Pour créer une tâche attribuée aux appareils sélectionnés, procédez comme suit :

1. Dans le menu principal, accédez à **Gestion des ressources** → **Ressources (Appareils)**.

   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

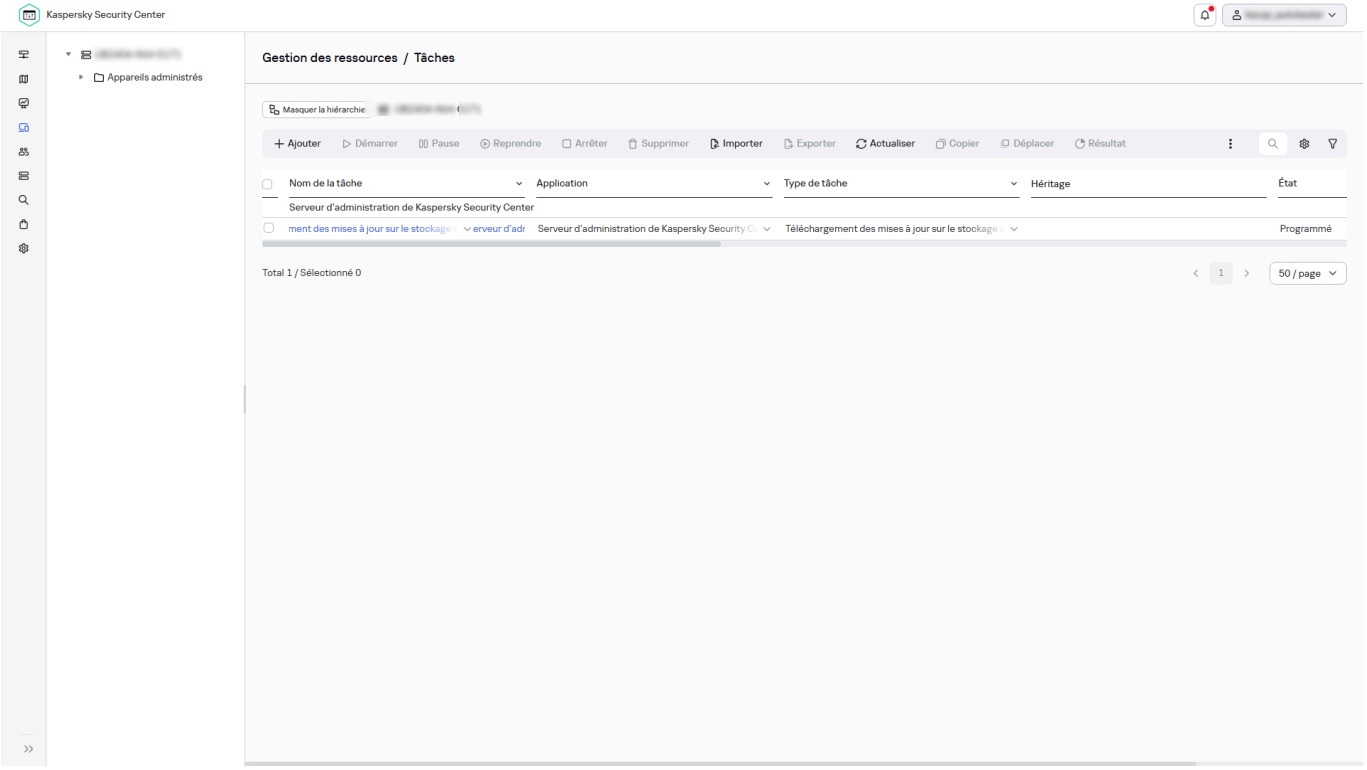
L'application démarre les tâches en fonction des paramètres de planification spécifiés dans les propriétés de chaque tâche. Vous pouvez lancer une tâche manuellement à tout moment à partir de la liste des tâches. Vous pouvez également sélectionner des appareils dans la liste **Ressources (Appareils)**, puis démarrer une tâche existante pour eux.

Pour démarrer une tâche manuellement :

1. Dans le menu principal, accédez à **Gestion des ressources** → **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**.



Lancement d'une tâche à partir de la liste des tâches

La tâche sera lancée. Vous pouvez vérifier l'état de la tâche dans la colonne **État** ou en cliquant sur le bouton **Résultat**.

Lancement d'une tâche pour les appareils sélectionnés

Vous pouvez sélectionner un ou plusieurs appareils clients dans la liste des appareils clients, puis lancer une tâche créée précédemment pour eux. Cela vous permet d'exécuter les tâches créées précédemment pour un ensemble spécifique d'appareils.

Cela modifie les appareils auxquels la tâche a été affectée à la liste des appareils que vous sélectionnez lorsque vous exécutez la tâche.
L'ancienne zone d'application de la tâche est supprimée et remplacée par la zone d'application sélectionnée.

Pour lancer une tâche pour les appareils sélectionnés :

1. Dans le menu principal, accédez à **Gestion des ressources** → **Ressources (Appareils)**. La liste des appareils administrés s'affiche.

2. Dans la liste des appareils administrés, cochez les cases des appareils pour lesquels vous souhaitez exécuter la tâche. 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 **Appliquer la tâche existante**.

   La liste des tâches existantes s'affiche.

4. Les appareils sélectionnés s'affichent au-dessus de la liste des tâches. Si nécessaire, vous pouvez supprimer un appareil de cette liste. Vous pouvez supprimer tous les appareils sauf un.

5. Sélectionnez la tâche souhaitée dans la liste. Le champ de recherche en haut de la liste permet de rechercher la tâche souhaitée sur la base de son nom. Une seule tâche peut être sélectionnée.

6. Cliquez sur **Enregistrer et lancer la tâche**.

La tâche sélectionnée est lancée immédiatement pour les appareils sélectionnés. Les paramètres de lancement planifié dans la tâche ne sont pas modifiés.

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 **Gestion des ressources** → **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 :

  Le type de planification peut varier en fonction de la tâche.

  Certains types de planification peuvent ne pas être disponibles pour d'autres applications Kaspersky.

  - **Paramètre Démarrer la tâche :**
    - **Toutes les N heures**

      La tâche s'exécute régulièrement, selon l'intervalle défini en heures, à partir de la date et heure définis.

La tâche s'exécute par défaut toutes les six heures à partir de la date et de l'heure actuelles du système.

- **Tous les N jours**

  La tâche s'exécute régulièrement, selon l'intervalle défini en jours. En outre, vous pouvez spécifier la date et l'heure de la première exécution de la tâche. Ces options supplémentaires deviennent disponibles si elles sont prises en charge par l'application pour laquelle vous créez la tâche.

  La tâche s'exécute par défaut chaque jour, à partir de la date et de l'heure actuelle du système.

- **Toutes les N minutes**

  La tâche s'exécute régulièrement, à l'intervalle défini en minutes, à partir de l'heure indiquée le jour de la création de la tâche.

  La tâche s'exécute par défaut toutes les 30 minutes, à partir de l'heure actuelle du système.

- **Selon les jours de la semaine**

  La tâche s'exécute régulièrement les jours définis de la semaine, à l'heure indiquée.

  Par défaut, la tâche s'exécute chaque vendredi à 18h00.

- **Chaque mois**

  La tâche s'exécute régulièrement le jour du mois défini, à l'heure indiquée.

  Si le jour en question ne figure pas dans le mois, la tâche s'exécute le dernier jour.

  La tâche s'exécute par défaut le premier jour de chaque mois, à l'heure système actuelle.

- **Mode manuel**

  La tâche ne s'exécute pas automatiquement. Vous pouvez uniquement la lancer manuellement.

  Cette option est sélectionnée par défaut.

- **Une fois**

  La tâche est exécutée une seule fois, à la date et à l'heure indiquées (par défaut, le jour de la création de la tâche).

- **Immédiatement**

  La tâche s'exécute immédiatement après l'enregistrement de ses paramètres.

- **Chaque mois, un jour de semaine donné**

  La tâche s'exécute régulièrement les jours du mois définis, à l'heure indiquée.

Par défaut, l'heure de début est 18:00 et aucun jour du mois n'est sélectionné.

Notez que vous ne sélectionnez ni une date précise dans le mois, ni le numéro de la semaine (première, deuxième semaine du mois) mais le numéro d'ordre du jour de la semaine à l'intérieur d'un mois. Par exemple, si vous placez le curseur dans la cellule **Ma** de la ligne **Premier**, cela signifie que la tâche sera exécutée tous les premiers mardis de chaque nouveau mois.

Vous pouvez sélectionner plusieurs jours de la semaine.

- **Lors du téléchargement des mises à jour sur les stockages**

  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*.

- **À la fin d'une autre tâche**

  La tâche actuelle démarre à la fin d'une autre tâche. Cette option ne fonctionne que si les deux tâches sont affectées aux mêmes appareils. Par exemple, vous pouvez exécuter la tâche *Administration des appareils* avec l'option **&Activer l'appareil** et, une fois celle-ci terminée, exécuter la tâche de *recherche de virus* comme tâche de déclenchement.

  Il faut sélectionner la tâche de déclenchement dans le tableau et l'état avec lequel cette tâche doit se terminer (**Terminée avec succès** ou **Échec**).

  Si nécessaire, vous pouvez rechercher, trier et filtrer les tâches dans le tableau comme suit :

  - Saisissez le nom de la tâche dans le champ de recherche pour rechercher une tâche par son nom.
  - Cliquez sur l'icône de tri pour trier les tâches par nom.

    Par défaut, les tâches sont triées par ordre alphabétique croissant.
  - Cliquez sur l'icône du filtre, et dans la fenêtre qui s'ouvre, filtrez les tâches par groupe, puis cliquez sur le bouton **Appliquer**.

- **Lancer les tâches non exécutées**

  Cette option détermine le comportement d'une tâche si un appareil client n'est pas visible sur le réseau quand la tâche est sur le point de démarrer.

  Si la case est Activé, lors du lancement suivant de l'application de Kaspersky sur cet appareil client, une tentative de lancement de la tâche sera faite. Si la programmation de la tâche est **Manuel**, **Une fois** ou **Immédiatement**, la tâche est immédiatement lancée dès que l'appareil apparaît sur le réseau ou immédiatement après l'inclusion de l'appareil dans la zone d'action de la tâche.

  Si cette option est désactivée, seules les tâches planifiées s'exécutent sur les appareils clients. Pour les planifications **Manuel**, **Une fois** et **Immédiatement**, les tâches s'exécutent uniquement sur les appareils clients qui sont visibles sur le réseau. Par exemple, vous pouvez désactiver cette option pour une tâche qui consomme des ressources que vous voulez exécuter uniquement en dehors des heures de bureau.

  Cette option est Inactif par défaut.

- **Adopter un décalage aléatoire automatique pour les lancements de tâche**

  Si cette option est activée, la tâche est lancée sur les appareils clients de manière aléatoire au cours d'un intervalle défini. C'est ce qu'on appelle un *lancement échelonné d'une tâche*. Un lancement échelonné de tâche permet d'éviter la communication simultanée d'un nombre important d'appareils clients avec le Serveur d'administration lors du lancement de la tâche programmée.

  Le temps du lancement aléatoire est automatiquement calculée lors de la création d'une tâche selon le nombre d'appareils clients sur lesquels la tâche est diffusée. Par la suite, la tâche démarre toujours à l'heure de lancement calculée. Toutefois, quand les paramètres de la tâche sont modifiés ou si la tâche est lancée manuellement, la valeur calculée de l'heure de lancement de la tâche est modifiée.

  Si la case n'est pas cochée, le lancement de la tâche sur les appareils clients s'opère selon la planification.

- **Décaler aléatoirement et automatiquement le lancement de la tâche dans un intervalle de**

  Si cette option est activée, la tâche est lancée sur les appareils clients de manière aléatoire au cours de l'intervalle défini. Un lancement échelonné de tâche permet d'éviter la communication simultanée d'un nombre important d'appareils clients avec le Serveur d'administration lors du lancement de la tâche programmée.

  Si la case n'est pas cochée, le lancement de la tâche sur les appareils clients s'opère selon la planification.

  Cette option est Inactif par défaut. Par défaut, la valeur de cet intervalle est de une minute.

- 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.

  - **Connexion.**

    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.

- **Distribuer aux Serveurs d'administration secondaires et virtuels**

  Lorsque cette option est activée, la tâche effective sur le Serveur d'administration principal est également appliquée sur les Serveurs d'administration secondaires (y compris virtuels). Si une tâche du même type existe déjà sur le Serveur d'administration secondaire, les deux tâches sont appliquées sur le Serveur d'administration secondaire, celui existant et celui hérité du Serveur d'administration principal.

  Cette option est disponible uniquement lorsque l'option **Distribuer aux sous-groupes** est activée.

  Cette option est Inactif par défaut.

- Paramètres de programmation avancés :

  - **Allumer les appareils en utilisant la fonctionnalité Wake-on-LAN avant le lancement de la tâche**

    Le système d'exploitation sur l'appareil démarre au délai indiqué avant le lancement de la tâche. Par défaut, la valeur de cet délai de est de une minute.

    Activez cette option si vous souhaitez que la tâche soit exécutée sur tous les appareils clients de la zone d'action de la tâche, y compris pour les appareils éteints alors que la tâche est sur le point de démarrer.

    Si vous souhaitez que l'appareil soit automatiquement éteint une fois la tâche terminée, activez l'option **Arrêter les appareils après la fin de la tâche**. Cette option se trouve dans la même fenêtre.

    Cette option est Inactif par défaut.

  - **Arrêter les appareils après la fin de la tâche**

    Par exemple, vous pouvez activer cette option pour une tâche d'installation de mise à jour qui installe les mises à jour sur les appareils client chaque vendredi après la fermeture des bureaux, puis éteint ces appareils pour le week-end.

    Cette option est Inactif par défaut.

  - **Arrêter la tâche si elle prend plus de**

    A l'issue du délai défini, la tâche s'arrêt automatiquement, qu'elle soit finie ou non.

    Activez cette option si vous souhaitez interrompre (ou arrêter) les tâches dont l'exécution dure trop longtemps.

    Cette option est Inactif par défaut. La durée d'exécution de la tâche par défaut est de 120 minutes.

- Paramètres des notifications :
  - Groupe **Sauvegarder le résultat** :
    - **Conserver dans la base de données du Serveur d'administration pendant (jours)**

      Les événements de l'application en rapport avec l'exécution de la tâche sur tous les appareils clients de la zone d'action de la tâche sont stockés sur le Serveur d'administration pendant le nombre de jours indiqué. A l'issue de cette période, les informations sont supprimées du Serveur d'administration.

      Cette option est activée par défaut.

    - **Stocker dans le journal des événements du système d'exploitation 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 au déroulement des tâches**

      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 **Gestion des ressources** → **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 que l'importation de la tâche d'application Kaspersky se fasse correctement, il est nécessaire d'installer le plug-in d'administration approprié.

Pour importer une tâche, procédez comme suit :

1. Dans le menu principal, accédez à **Gestion des ressources** → **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 de la 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 **En savoir plus** pour afficher les propriétés de la tâche.

Après une importation réussie, la tâche s'affiche dans la liste des tâches. Les paramètres et la planification de la tâche sont également importés. La tâche sera lancée conformément à sa planification.

Si la tâche importée porte le même nom qu'une tâche existante, le nom de la tâche importée est suivi de l'index **(<numéro de séquence suivant>)**, par exemple : **(1)**, **(2)**.

Démarrage de l'Assistant de modification du mot de passe des tâches

Pour une tâche non locale, vous pouvez spécifier un compte sous lequel la tâche doit être exécutée. Vous pouvez spécifier le compte lors de la création de la tâche ou dans les propriétés d'une tâche existante. Si le compte spécifié est utilisé conformément aux instructions de sécurité de l'organisation, ces instructions peuvent nécessiter périodiquement le changement du mot de passe du compte. Lorsque le mot de passe du compte expire et que vous en définissez un nouveau, les tâches ne démarrent pas tant que vous n'avez pas spécifié le nouveau mot de passe valide dans les propriétés de la tâche.

L'Assistant de modification du mot de passe des tâches vous permet de remplacer automatiquement l'ancien mot de passe par le nouveau dans toutes les tâches dans lesquelles le compte est spécifié. Vous pouvez également modifier ce mot de passe manuellement dans les propriétés de chaque tâche.

Pour démarrer l'Assistant de modification du mot de passe des tâches :

1. Dans le menu principal, accédez à **Gestion des ressources** → **Tâches**.

2. Cliquez sur **Administrer les informations d'identification des comptes pour les tâches de démarrage**.

   Suivez les étapes 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. Exécutez 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.

Pour consulter les résultats de l'exécution de la tâche, procédez comme suit :

Dans la fenêtre des propriétés de la tâche, accédez à l'onglet **Résultats**.

Pour consulter les résultats des tâches d'un Serveur d'administration secondaire, procédez comme suit :

1. Dans la fenêtre des propriétés de la tâche, sélectionnez la section **Général**.
2. Cliquez sur le lien **Résultats** pour ouvrir la fenêtre **Résultats de la tâche**.
3. Cliquez sur **Statistiques des Serveurs secondaires**.
4. Sélectionnez le Serveur secondaire pour lequel vous souhaitez afficher la fenêtre **Résultats de la tâche**.

Tags de l'application

Cette section décrit les tags de l'application et explique comment les créer et les modifier tout en indiquant également comment attribuer des tags à des applications tierces.

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 **Enregistrer** pour 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. Ensuite, 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.

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** → **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 sur les appareils administrés, ainsi que les comptes locaux sur l'appareil sur lequel le Serveur d'administration est installé.
- Comptes des utilisateurs internes de Kaspersky Security Center Linux. Vous pouvez créer des comptes d'utilisateurs internes. Ces comptes sont utilisés uniquement dans Kaspersky Security Center Linux.

Les comptes utilisateurs locaux et le groupe local kladmins du système d'exploitation Linux ne peuvent pas être utilisés 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. Les employés de l'entreprise pourront utiliser leurs comptes utilisateurs pour se connecter après avoir configuré l'authentification de domaine.

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.

Si le tableau des utilisateurs contient plus de 50 000 utilisateurs, seuls les 50 000 premiers utilisateurs sont affichés, et les autres utilisateurs ne sont pas affichés.

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 descriptions de poste différentes qui requièrent des paramètres de sécurité différents 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.

> Toutes les tâches, rapports, paramètres et paquets d'installation qui manquent dans le tableau appartiennent à la zone fonctionnelle **Fonctionnalités générales : Fonctionnalité de base**.

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

Zone fonctionnelle	Droit	Action utilisateur : droit requis pour exécuter l'action	Tâche	Rapport	Autres
Caractéristiques générales : **Accéder aux objets, quel que soit leur ACL**	**Lecture**	Obtenir un accès en lecture à tous les objets : **Lire**	Aucun	Aucun	La zone fonctionnelle **Fonctions générales : Accéder aux objets quel que soit leur ACL** est conçue à des fins d'audit. Une autorisation **Lecture** dans cette zone fonctionnelle accorde un accès complet en **Lecture** à tous les objets. Nous vous recommandons d'octroyer ces droits avec précaution et à un nombre limité d'utilisateurs qui en ont besoin pour l'accomplissement de leurs tâches officielles. L'accès est accordé indépendamment des autres droits, même s'ils interdisent l'accès 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** • Définir le certificat personnalisé du protocole mobile (LWNGT) : **Lire** • Définir le certificat personnalisé du protocole mobile (LWNGT) : **Écrire** • Obtenir la liste des réseaux définis par NLA : **Lire** • Ajouter, modifier ou supprimer une liste de réseaux définie par NLA : **Écrire** • Afficher la liste de contrôle d'accès des groupes : **Lire** • 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**	• " Télécharger les mises à jour dans le stockage du Serveur d'administration " • "Livrer des rapports" • "Diffusion du paquet d'installation" • "Installation des applications sur les Serveurs d'administration secondaires à distance"	• "Rapport sur l'état de la protection" • "Rapport sur les menaces" • "Rapport sur les appareils les plus infectés" • "Rapport sur l'état des bases antivirus" • "Rapport sur les erreurs" • "Rapport sur les attaques réseau" • "Rapport de synthèse sur les applications de sécurité des systèmes de messagerie installées" • " Rapport de synthèse sur les applications de sécurité des postes de travail et serveurs Windows installées " • "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"	Aucun

Zone fonctionnelle	Droit	Action utilisateur : droit requis pour exécuter l'action	Tâche	Rapport	Autres
				• "Rapport sur les problèmes de sécurité" • "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 vulnérabilités" • "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**	Aucun	Aucun	Paramètres : • Le nombre maximal d'événements stockés dans la base de données • Période de stockage des événements des appareils supprimés

Zone fonctionnelle	Droit	Action utilisateur : droit requis pour exécuter l'action	Tâche	Rapport	Autres
		paramètres de notification d'événements • Supprimer des événements : **Supprimer des événements**			
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 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**	• "Sauvegarde des données du Serveur d'administration" • "Maintenance de la base de données"	Aucun	Aucun

Zone fonctionnelle	Droit	Action utilisateur : droit requis pour exécuter l'action	Tâche	Rapport	Autres
		• 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** • Exécuter des rapports quel que soit leur ACL : **Lire**	Aucun	Aucun	Aucun
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**	Aucun	Aucun	Aucun

Zone fonctionnelle	Droit	Action utilisateur : droit requis pour exécuter l'action	Tâche	Rapport	Autres
		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**			
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

Zone fonctionnelle	Droit	Action utilisateur : droit requis pour exécuter l'action	Tâche	Rapport	Autres
Caractéristiques générales : **Gestion des clés de chiffrement**	**Écrire**	Importer les clés de chiffrement : **Écrire**	Aucun	Aucun	Aucun
Administration des appareils mobiles : **Généralités**	• **Connexion des nouveaux appareils** • **Envoyer uniquement des commandes d'information aux appareils mobiles** • **Envoi des commandes sur les appareils mobiles** • **Gérer les certificats** • **Lecture** • **Écrire**	• Obtenir les données de restauration du service de gestion des clés : **Lire** • Supprimer les certificats utilisateur : **Gérer les certificats** • Obtenir la partie publique du certificat utilisateur : **Lire** • Vérifier si l'infrastructure à clé publique est activée : **Lire** • Vérifier le compte d'infrastructure à clé publique : **Lire** • Obtenir des modèles d'infrastructure à clé publique : **Lire** • Obtenir des modèles d'infrastructure de clé publique par certificat d'utilisation de clé étendue : **Lire** • Vérifier si le certificat d'infrastructure à clé publique est révoqué : **Lire** • Mettre à jour les paramètres d'émission des certificats utilisateur : **Gérer les certificats** • Obtenir les paramètres d'émission de certificat utilisateur : **Lire** • Obtenir des paquets par nom d'application et par version : **Lire** • Définir ou annuler le certificat utilisateur : **Gérer les certificats** • Renouveler le certificat utilisateur : **Gérer les certificats**	Aucun	Aucun	Aucun

Zone fonctionnelle	Droit	Action utilisateur : droit requis pour exécuter l'action	Tâche	Rapport	Autres
		• Définir la balise de certificat utilisateur : **Gérer les certificats** • Exécuter la génération du paquet d'installation MDM ; annuler la génération du paquet d'installation MDM : **connecter de nouveaux appareils**			
Gestion du système : **Connectivité**	• **Démarrer des sessions RDP** • **Se Connecter aux sessions RDP existantes** • **Lancer le tunneling** • **Enregistrer les fichiers des appareils sur le poste de travail de l'administrateur** • **Lecture** • **Écrire** • **Exécuter** • **Effectuer des opérations sur les sélections d'appareils**	• Créer une session de partage de bureau : **Droit de créer une session de partage de bureau** • Créer une session RDP : **Se connecter aux sessions RDP existantes** • Créer un tunnel : **lancer le tunneling** • Enregistrer la liste des réseaux de contenu : **enregistrer les fichiers des appareils sur le poste de travail de l'administrateur**	Aucun	" Rapport sur les utilisateurs de l'appareil "	Aucun
Gestion du système : **Gestion des vulnérabilités et des correctifs**	• **Lecture** • **Écrire** • **Exécuter** • **Effectuer des opérations sur les sélections d'appareils**	• Afficher les propriétés des correctifs tiers : **Lire** • Modifier les propriétés des correctifs tiers : **Écrire**	• "Corriger les vulnérabilités" • "Installation des mises à jour requises et correction des vulnérabilités"	"Rapport sur les mises à jour des logiciels"	Aucun
Administration du système : **Exécuter des scripts à distance**	• **Lecture** • **Écrire** • **Exécuter** • **Effectuer des opérations sur les sélections d'appareils**	L'utilisateur peut consulter les propriétés de la tâche : **Lire** L'utilisateur peut créer, supprimer ou modifier un paquet d'installation : **Écrire** L'utilisateur peut exécuter une tâche : **Écrire**. Sur les appareils clients Linux, les scripts sont exécutés avec les privilèges root. L'utilisateur peut exécuter une tâche ou planifier son exécution : **Exécuter**	" Exécuter des scripts à distance "	Aucun	Aucun

Zone fonctionnelle	Droit	Action utilisateur : droit requis pour exécuter l'action	Tâche	Rapport	Autres
		L'utilisateur peut exécuter une tâche sur une sélection d'appareils : **Effectuer des opérations sur les sélections d'appareils**			

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. Lors de la création d'un nouveau rôle, 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	Autorise la consultation et l'exécution de toutes les tâches créées sur les appareils sélectionnés connectés au Serveur d'administration via l'Agent d'administration avec des privilèges d'administrateur local (root pour Linux). Nous recommandons d'attribuer ce rôle prudemment et à un nombre limité d'utilisateurs qui en ont besoin pour l'accomplissement de leurs tâches officielles.
Superviseur	Autorise toutes les opérations d'affichage, n'autorise pas les autres opérations. Vous pouvez attribuer ce rôle à un responsable de la sécurité et à d'autres responsables chargé de la sécurité de l'information dans votre organisation.
Responsable de la sécurité	Autorise toutes les informations de consultation, autorise la gestion des rapports, octroie des permissions restreintes dans les domaines **Administration du système** : **Connectivité**. Vous pouvez attribuer ce rôle à la personne chargée de la sécurité de l'information dans votre organisation.

Le tableau ci-dessous montre les droits d'accès attribués à chaque rôle d'utilisateur prédéfini.

Droits d'accès des rôles utilisateur prédéfinis

Rôle	Description

Administrateur du Serveur d'administration	Permet toutes les opérations dans les domaines fonctionnels suivants :
	• **Caractéristiques générales** :
	  • **Fonctionnalité de base**
	  • **Gestion des clés de chiffrement**
	  • **Traitement des événements**
	  • **Hiérarchie des Serveurs d'administration**
	  • **Serveurs d'administration virtuels**
	• **Administration du système :**
	  • **Connectivité**
	  • **Inventaire du matériel**
	  • **Inventaire des applications**

Rôle	Description

Opérateur du Serveur d'administration	Accorde les droits de **lecture** et d' **exécution** (le cas échéant) dans tous les domaines fonctionnels suivants :
	• **Caractéristiques générales** :
	  • **Fonctionnalité de base**
	  • **Gestion des clés de chiffrement**
	  • **Serveurs d'administration virtuels**
	• **Administration du système :**
	  • **Connectivité**
	  • **Inventaire du matériel**
	  • **Inventaire des applications**

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	Permet toutes les opérations dans les domaines fonctionnels suivants :
	• **Fonctions générales :**
	  • **Fonctionnalité de base**
	  • **Déploiement d'applications Kaspersky**
	  • **Gestion des clés de licence**
	• **Administration du système :**
	  • **Déploiement du système d'exploitation**
	  • **Gestion des vulnérabilités et des correctifs**
	  • **Installation à distance**
	  • **Inventaire des applications**
	Accorde les droits de **lecture** et d'**exécution** dans la zone fonctionnelle **Fonctionnalités générales : Serveurs d'administration virtuelle**.

Opérateur d'installation	Accorde les droits de **lecture** et d' **exécution** (le cas échéant) dans tous les domaines fonctionnels suivants :
	• **Fonctions générales :**
	  • **Fonctionnalité de base**
	  • **Déploiement de logiciels Kaspersky** (accorde également les **correctifs Manage Kaspersky** directement dans cette zone)
	  • **Serveurs d'administration virtuels**
	• **Administration du système :**
	  • **Déploiement du système d'exploitation**
	  • **Gestion des vulnérabilités et des correctifs**
	  • **Installation à distance**
	  • **Inventaire des applications**

Administrateur Kaspersky Endpoint Security	Permet toutes les opérations dans les domaines fonctionnels suivants : • **Caractéristiques générales : fonctionnalité de base** • **Caractéristiques générales : Gestion des clés de chiffrement** • Zone **Kaspersky Endpoint Security**, y compris toutes les fonctionnalités
Opérateur Kaspersky Endpoint Security	Accorde les droits de **lecture** et d' **exécution** (le cas échéant) dans tous les domaines fonctionnels suivants : • **Caractéristiques générales : fonctionnalité de base** • **Caractéristiques générales : Gestion des clés de chiffrement** • Zone **Kaspersky Endpoint Security**, y compris toutes les fonctionnalités
Administrateur général	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**

Rôle	Description

Opérateur principal	Accorde les droits de **lecture** et d' **exécution** (le cas échéant) dans tous les domaines fonctionnels suivants :
	• **Caractéristiques générales** :
	  • **Fonctionnalité de base**
	  • **Objets supprimés**
	  • **Gestion des clés de chiffrement**
	  • **Opérations avec le Serveur d'administration**
	  • **Tags de l'appareil**
	  • **Déploiement d'applications Kaspersky**
	  • **Intégration des applications**
	  • **Serveurs d'administration virtuels**
	• La zone **Administration des appareils mobiles**, y compris toutes les fonctions
	• **Gestion du système**, y compris toutes les fonctionnalités
	• Zone **Kaspersky Endpoint Security**, y compris toutes les fonctionnalités

Administrateur Administration des appareils mobiles	Permet toutes les opérations dans les domaines fonctionnels suivants : • **Caractéristiques générales : fonctionnalité de base** • La zone **Administration des appareils mobiles**, y compris toutes les fonctions Accorde le droit **Exporter le fichier clé** dans les **Fonctionnalités générales : gestion des clés de licence**. Accorde le droit de **lecture** dans **Gestion du système : Gestion des vulnérabilités et des correctifs**.
Opérateur Administration des appareils mobiles	Accorde les droits de **lecture** et d'**exécution** dans les **Fonctionnalités générales : Fonctionnalité de base**. Accorde les droits de **lecture** et **Envoyer uniquement les commandes d'informations aux appareils mobiles** dans **Gestion des appareils mobiles** : • **Commun** • **Self Service Portal**
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 suivants dans la zone fonctionnelle **Gestion du système : Connectivité** : **Lecture**, **Écriture**, **Exécution**, **Enregistrer les fichiers des appareils sur le poste de travail de l'administrateur** et **Exécuter les opérations sur les appareils sélectionnés**. 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**.
Superviseur	Accorde le droit de **lecture** dans les zones fonctionnelles **Fonctions générales** : **Accéder aux objets quelles que soient leurs ACL** et **Fonctions générales** : **Gestion imposée des rapports**. Vous pouvez attribuer ce rôle à un responsable de la sécurité et à d'autres responsables chargé de la sécurité de l'information dans votre organisation.
Administrateur de gestion des vulnérabilités et des correctifs	Permet toutes les opérations dans les zones fonctionnelles **Fonctionnalités générales** : **Fonctionnalité de base** et **Gestion du système** (y compris toutes les fonctionnalités, *sauf* la fonction **Exécuter les scripts à distance**).
Opérateur de gestion des vulnérabilités et des correctifs	Accorde les droits de **lecture** et d'**exécution** (le cas échéant) dans les zones fonctionnelles **Fonctionnalités générales** : **Fonctionnalité de base** et **Gestion du système** (y compris toutes les fonctionnalités, *sauf* la fonction **Exécuter les scripts à distance**).

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 :
   - **Gestion des ressources** → **Hiérarchie des groupes**
   - **Gestion des ressources** → **Tâches**
   - **Surveillance** → **Rapports**
   - **Gestion des ressources** → **Sélections d'appareils**
   - **Surveillance** → **Sélections d'événements**
2. Ouvrez les propriétés de l'objet pour lequel vous souhaitez configurer les droits d'accès.

   Pour ouvrir la fenêtre des propriétés d'un groupe d'administration ou d'une tâche, cliquez sur le nom de l'objet. Les propriétés d'autres objets peuvent être ouvertes à l'aide du bouton de la barre d'outils.
3. Dans la fenêtre des propriétés, ouvrez la section **Privilèges d'accès**.

   La liste des utilisateurs s'ouvre. Les utilisateurs et les groupes de sécurité répertoriés disposent de droits d'accès à l'objet. Par défaut, si vous utilisez une hiérarchie de groupes d'administration ou de Serveurs, la liste et les droits d'accès sont hérités du groupe d'administration parent ou du Serveur primaire.
4. Pour pouvoir modifier la liste, activez l'option **Utiliser des autorisations personnalisées**.
5. Configurez les droits d'accès :
   - Utilisez les boutons **Ajouter** et **Supprimer** pour modifier la liste.
   - Spécifiez les droits d'accès pour un utilisateur ou un groupe de sécurité. Exécutez une des actions suivantes :
     - Si vous souhaitez définir les droits d'accès manuellement, sélectionnez l'utilisateur ou le groupe de sécurité, cliquez sur le bouton **Privilèges d'accès**, puis indiquez les droits d'accès.
     - Si vous souhaitez attribuer un rôle utilisateur à l'utilisateur ou au groupe de sécurité, sélectionnez l'utilisateur ou le groupe de sécurité, cliquez sur le bouton **Rôles**, puis sélectionnez le rôle à attribuer.
6. Cliquez sur le bouton **Enregistrer**.

Les droits d'accès à l'objet sont configurés.

Attribution de droits d'accès aux utilisateurs et aux groupes de sécurité

Vous pouvez octroyer aux utilisateurs et aux groupes de sécurité des droits d'accès pour utiliser différentes fonctionnalités du Serveur d'administration, par exemple, Kaspersky Endpoint Security for Linux.

Pour attribuer des droits d'accès à un utilisateur ou à un groupe de sécurité :

1. Dans le menu principal, cliquez sur le nom du Serveur d'administration.

   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 sur le Serveur d'administration (uniquement dans la fenêtre des propriétés du Serveur d'administration)
  - Tags de l'appareil
  - Déploiement de l'application Kaspersky
  - Gestion des clés de licence
  - Intégration des applications

    - Administration des rapports mise en œuvre
    - Hiérarchie des Serveurs d'administration
    - Autorisations d'utilisateur
    - Serveurs d'administration virtuels
- Administration des appareils mobiles :
    - Général
    - Self Service Portal
- Administration du système
    - Connectivité
    - Exécuter des scripts à distance
    - Hardware inventory
    - 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 une permission, cette permission est considérée comme *non définie* : elle persiste tant qu'elle n'a pas été explicitement autorisée ou interdite pour l'utilisateur.

Les privilèges d'un utilisateur sont la somme des éléments suivants :

- Propres privilèges de l'utilisateur
- Privilèges de tous les rôles attribués à cet utilisateur
- Privilèges de tous les groupe de sécurité auxquels l'utilisateur appartient
- Les privilèges de tous les rôles attribués aux groupes de sécurité auxquels l'utilisateur appartient

Si au moins un de ces ensembles de privilèges a la valeur **Interdire** pour une permission, celle-ci n'est pas accordée à l'utilisateur, même si d'autres ensembles l'autorisent ou ne la définissent pas.

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'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.

Ajout d'un compte d'un utilisateur interne

Si vous souhaitez ajouter un compte utilisateur, assurez-vous que votre compte dispose du droit Modifier les ACL des objets dans la zone fonctionnelle Caractéristiques générales : Autorisations utilisateur.

Pour ajouter un nouveau compte d'utilisateur interne à Kaspersky Security Center 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 256 caractères.

     - Le mot de passe doit compter des caractères d'au moins trois des groupes ci-dessous :

       - Lettres majuscules (A–Z)

       - Lettre minuscules (a-z)

       - Chiffres (0–9)

       - Caractères spéciaux (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)

     - Le mot de passe ne doit contenir aucun caractère d'espacement, aucun caractère Unicode, ni la combinaison de "." et de "@" lorsque "." précède "@".

     Pour consulter le mot de passe saisi, cliquez sur 👁.

     Vous pouvez activer l'option **L'utilisateur doit changer son mot de passe lors de la première connexion** pour forcer la modification du mot de passe lors de la première authentification de l'utilisateur.

4. Enregistrez les modifications pour terminer la création d'un compte utilisateur.

Un nouveau compte utilisateur est ajouté à la liste des utilisateurs.

Pour vous connecter à Kaspersky Security Center Web Console via un compte utilisateur interne créé, vous devez attribuer un rôle à ce compte. Avant de vous connecter, assurez-vous que le compte utilisateur interne dispose d'un rôle. Dans le cas contraire, une erreur de connexion se produira.

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 de groupe**

   - **Description**

4. Cliquez sur **Enregistrer** pour enregistrer les modifications.

Un nouveau groupe de sécurité est ajouté à la liste des groupes.

Modification d'un compte d'un utilisateur interne

Si vous souhaitez modifier un compte utilisateur, assurez-vous que votre compte dispose du droit Modifier les ACL des objets dans la zone fonctionnelle Caractéristiques générales : Autorisations utilisateur.

Pour modifier le compte d'un utilisateur interne dans Kaspersky Security Center 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 :

   - **Compte utilisateur**

     Le cas échéant, placez le commutateur en position **Désactivée** 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.

   - Description

   - **Nom complet**

   - **Adresse email**

   - **Téléphone principal**

- **Mot de passe**

  En cas de nécessité, vous pouvez définir un nouveau mot de passe pour la connexion de l'utilisateur à Kaspersky Security Center Linux comme suit :

  a. Cliquez sur le bouton **Modifier le mot de passe**, puis définissez un nouveau mot de passe pour le compte utilisateur.

     Le mot de passe doit remplir les conditions suivantes :

     - Le mot de passe doit compter entre 8 et 256 caractères.
     - Le mot de passe doit compter des caractères d'au moins trois des groupes ci-dessous :
       - Lettres majuscules (A–Z)
       - Lettre minuscules (a-z)
       - Chiffres (0–9)
       - Caractères spéciaux (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
     - Le mot de passe ne doit contenir aucun caractère d'espacement, aucun caractère Unicode, ni la combinaison de "." et de "@" lorsque "." précède "@".

     Pour consulter le mot de passe saisi, cliquez sur 👁.

  b. Si nécessaire, vous pouvez activer l'option **L'utilisateur doit changer son mot de passe lors de la première connexion** pour forcer la modification du mot de passe lors de l'authentification de l'utilisateur suivante.

  c. Si le compte utilisateur est protégé contre les modifications non autorisées, vous devez confirmer que vous avez les autorisations pour modifier le compte en question. Dans la fenêtre **Protection du compte**, indiquez les identifiants du compte disposant du droit Modifier les ACL des objets dans la zone fonctionnelle Caractéristiques générales : Autorisations utilisateur.

4. Dans l'onglet **Authentification à deux facteurs**, vous pouvez spécifier les paramètres de sécurité de ce compte.

5. Sous l'onglet **Groupes**, vous pouvez ajouter l'utilisateur à des groupes de sécurité.

6. Sous l'onglet **Appareils**, vous pouvez attribuer des appareils à l'utilisateur.

7. Sous l'onglet **Rôles**, vous pouvez attribuer des rôles à l'utilisateur.

8. Enregistrez les modifications pour terminer la modification du compte utilisateur.

Le compte utilisateur mis à jour apparaît dans la liste des utilisateurs.

Modification d'un groupe de sécurité

Pour modifier un groupe de sécurité, procédez comme suit :

1. Dans le menu principal, accédez à **Utilisateurs et rôles** → **Utilisateurs et groupes**, puis sélectionnez l'onglet **Groupes**.

2. Cliquez sur le nom du groupe de sécurité que vous souhaitez modifier.

3. Dans la fenêtre des paramètres de groupe qui s'ouvre, modifiez les paramètres du groupe de sécurité :

   - Sous l'onglet **Général**, vous pouvez modifier les paramètres **Nom** et **Description**. Ces paramètres sont disponibles uniquement pour les groupes de sécurité internes.

   - L'onglet **Utilisateurs** permet d'ajouter des utilisateurs au groupe de sécurité. Ce paramètre est disponible uniquement pour les utilisateurs internes et les groupes de sécurité internes.

   - Sous l'onglet **Rôles**, vous pouvez attribuer le rôle au groupe de sécurité.

4. Cliquez sur **Enregistrer** pour 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 Secure Mobility Management.

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**.

   La liste des 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 **Gestion des ressources** → **Ressources (Appareils)**, en cliquant sur le nom de l'appareil que vous voulez attribuer, puis en cliquant sur le lien **Administrer le propriétaire de l'appareil**.

Désignation d'un utilisateur en tant que propriétaire de l'appareil pendant l'installation de l'Agent d'administration

Pour désigner un utilisateur en tant que propriétaire de l'appareil lors de l'installation de l'Agent d'administration via un paquet d'installation, ajoutez les variables spécifiées dans le tableau ci-dessous aux paramètres du paquet d'installation de l'Agent d'administration.

Nom de la variable	Requis	Description	Valeurs possibles
KLNAGENT_DEVICEOWNER_REGISTRATION_START	Non	Permet d'exécuter l'utilitaire d'enregistrement de l'utilisateur en tant que propriétaire de l'appareil après l'installation de l'Agent d'administration. Si cette option est désactivée, l'enregistrement en tant que propriétaire de l'appareil n'est pas disponible pour l'utilisateur.	1 : l'utilitaire d'enregistrement de l'utilisateur en tant que propriétaire de l'appareil démarrera après l'installation de l'Agent d'administration. Autre : l'utilitaire n'est pas disponible.
KLNAGENT_DEVICEOWNER_LOGIN	Non Oui, si vous saisissez le mot de passe	Contient l'identifiant de l'utilisateur qui sera enregistré en tant que propriétaire de l'appareil.	Identifiant de l'utilisateur tel qu'il est indiqué dans la liste des utilisateurs de Kaspersky Security Center Linux.
KLNAGENT_DEVICEOWNER_PASSWORD	Non Oui, si vous saisissez l'identifiant	Contient le mot de passe chiffré de l'utilisateur qui sera enregistré en tant que propriétaire de l'appareil.	Le mot de passe de l'utilisateur.

L'Agent d'administration déchiffrera l'identifiant et le mot de passe indiqués pendant l'installation de Kaspersky Security Center Linux et l'utilisateur sera enregistré en tant que propriétaire de l'appareil.

Vous pouvez également désigner un utilisateur en tant que propriétaire de l'appareil lors de l'installation de l'Agent d'administration en mode silencieux avec un fichier de réponses.

Pour désigner un utilisateur en tant que propriétaire de l'appareil lors de l'installation de l'Agent d'administration en mode silencieux avec un fichier de réponses, procédez comme suit :

1. Ajoutez le paramètre KLNAGENT_DEVICEOWNER_REGISTRATION_START au fichier de réponses et définissez-le sur 1.

   L'utilitaire d'enregistrement de l'utilisateur en tant que propriétaire de l'appareil démarrera après l'installation de l'Agent d'administration.

2. Saisissez l'identifiant et le mot de passe dans la ligne de commande de l'appareil client.

   L'utilisateur sera désigné comme propriétaire de l'appareil.

Si l'utilisateur fait partie d'un groupe de sécurité interne, le nom d'utilisateur doit figurer dans l'identifiant.

Si l'utilisateur fait partie d'un groupe de sécurité Active Directory, le nom d'utilisateur et le nom de domaine doivent figurer dans l'identifiant.

Pour l'authentification à deux facteurs, vous devez saisir le mot de passe à usage unique basé sur le temps (TOTP) depuis l'application.

Désignation d'un utilisateur en tant que propriétaire de l'appareil Linux après l'installation de l'Agent d'administration

Pour autoriser l'enregistrement de l'utilisateur en tant que propriétaire de l'appareil Linux, procédez comme suit :

1. Dans Kaspersky Security Center Web Console, accédez à **Découverte et déploiement** → **Déploiement et attribution** → **Paquets d'installation**.

   La liste des paquets d'installation s'ouvre.

2. Cliquez sur le paquet d'installation de l'Agent d'administration.

   La fenêtre des propriétés du paquet d'installation s'ouvre.

3. Dans la fenêtre des propriétés du paquet d'installation, cliquez sur **Paramètres** → **Avancé**.

4. Dans la section **Enregistrement de l'utilisateur en tant que propriétaire de l'appareil (Linux uniquement)**, activez l'option **Autoriser l'exécution de l'utilitaire d'enregistrement des utilisateurs après l'installation de l'Agent d'administration** et cliquez sur le bouton **Enregistrer**.

L'utilitaire d'enregistrement de l'utilisateur en tant que propriétaire de l'appareil peut être lancé via la ligne de commande sur l'appareil client.

Pour enregistrer un utilisateur en tant que propriétaire de l'appareil client Linux, procédez comme suit :

1. Exécutez la commande suivante dans la ligne de commande sur l'appareil client :
   ```
   $ /opt/kaspersky/klnagent64/bin/nagregister -set_owner
   ```

2. Saisissez l'identifiant et le mot de passe, si vous y êtes invité(e).

   Si l'identifiant et le mot de passe se trouvent dans le fichier de réponses ou dans le paquet d'installation de l'Agent d'administration, exécutez la commande suivante sur l'appareil client dans la ligne de commande :
   ```
   $ /opt/kaspersky/klnagent64/bin/nagregister -set_owner -unattended
   ```

Si l'utilisateur fait partie d'un groupe de sécurité interne, le nom d'utilisateur doit figurer dans l'identifiant.

Si l'utilisateur fait partie d'un groupe de sécurité Active Directory, le nom d'utilisateur et le nom de domaine doivent figurer dans l'identifiant.

Pour l'authentification à deux facteurs, vous devez saisir le mot de passe à usage unique basé sur le temps (TOTP) depuis l'application.

L'utilisateur sera enregistré en tant que propriétaire de l'appareil.

Suppression d'un utilisateur en tant que propriétaire de l'appareil

Pour supprimer un utilisateur en tant que propriétaire de l'appareil sur l'appareil client, procédez comme suit :

1. Exécutez la commande suivante dans la ligne de commande de l'appareil client :

   ```
   $ /opt/kaspersky/klnagent64/bin/nagregister -remove_owner
   ```

2. Saisissez le nom d'utilisateur et le mot de passe.

Si l'utilisateur fait partie d'un groupe de sécurité interne, le nom d'utilisateur doit figurer dans l'identifiant.

Si l'utilisateur fait partie d'un groupe de sécurité Active Directory, le nom d'utilisateur et le nom de domaine doivent figurer dans l'identifiant.

Pour l'authentification à deux facteurs, vous devez saisir le mot de passe à usage unique basé sur le temps (TOTP) depuis l'application.

L'utilisateur sera supprimé en tant que 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 **Authentification à deux facteurs**.

4. Sous l'onglet **Authentification à deux facteurs**, sélectionnez l'option **Demander une authentification pour vérifier l'autorisation de modifier les comptes utilisateurs** si vous souhaitez demander les identifiants et un code de sécurité à usage unique pour l'authentification à deux facteurs chaque fois que les paramètres du compte sont modifiés. Dans le cas contraire, sélectionnez l'option **Autoriser les utilisateurs à modifier ce compte sans authentification supplémentaire**.

5. Enregistrez vos modifications.

Configuration de l'authentification à deux facteurs

À partir de la version 16.1 du Serveur d'administration, l'authentification à deux facteurs est activée automatiquement. L'option générale permettant de désactiver l'authentification à deux facteurs n'est pas prise en charge. Ce scénario décrit les étapes à suivre pour configurer l'authentification en deux étapes lors de la première connexion, ainsi que les paramètres de l'authentification à deux facteurs sur le Serveur d'administration.

Étapes

La configuration de l'authentification à deux facteurs comporte plusieurs 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
   - Bitrix24 OTP
   - Yandex ID
   - Authentificateur Avanpost
   - Aladdin 2FA
   - Rutoken OTP

   Pour vérifier si Kaspersky Security Center Linux prend en charge l'application d'authentification que vous souhaitez utiliser, activez l'authentification à deux facteurs 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 le Serveur d'administration est géré.

2. **Synchronisation de l'heure de l'appareil avec l'application d'authentification 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. Pour une meilleure précision, nous vous recommandons d'utiliser les mêmes serveurs NTP dans toute votre infrastructure. Sinon, des échecs peuvent se produire lors de la configuration de l'authentification à deux facteurs.

3. **Configuration de l'authentification à deux facteurs pour les comptes utilisateur lors de la connexion à la Web Console**

   Connectez-vous à la Web Console et configurez l'authentification à deux facteurs.

   Si vous n'avez pas accès à la configuration de l'authentification à deux facteurs, contactez un utilisateur disposant du droit Modifier les ACL des objets dans la zone fonctionnelle **Fonctionnalités générales : Autorisations utilisateur** et possédant un compte sur lequel l'authentification à deux facteurs est configurée afin qu'il ajoute votre compte à la liste d'autorisation pour l'authentification à deux facteurs.

4. **Configuration des paramètres de l'authentification à deux facteurs sur le Serveur d'administration**

   Si vous avez configuré l'authentification à deux facteurs et que vous disposez du droit Modifier les ACL des objets dans la zone fonctionnelle **Fonctions générales** : **Autorisations d'utilisateur**, vous pouvez configurer les paramètres de l'authentification à deux facteurs sur le Serveur d'administration comme suit :

   1. Vérification de la liste des utilisateurs qui peuvent configurer l'authentification en deux étapes lors de la connexion :

      - Pour installer le Serveur d'administration version 16.1 à partir de zéro : ajoutez les utilisateurs requis à la liste d'autorisation pour l'authentification à deux facteurs afin de leur permettre de configurer l'authentification à deux facteurs lors de leur première connexion.

      - Pour mettre à niveau ou restaurer le Serveur d'administration version 16.1 : consultez la liste d'autorisation pour l'authentification à deux facteurs et supprimez les comptes qui ne doivent pas avoir accès au Serveur d'administration.

   2. Exclusion des comptes utilisateur pour lesquels vous n'avez pas besoin d'activer l'authentification à deux facteurs (facultatif)

      Excluez des comptes utilisateur de l'authentification à deux facteurs pour leur permettre de se connecter au Serveur d'administration même s'ils n'ont pas configuré l'authentification à deux facteurs. L'exclusion des comptes de l'authentification à deux facteurs peut être nécessaire pour les comptes d'intégration qui ne peuvent pas fournir le code de sécurité lors de l'authentification. Les comptes d'intégration sont utilisés pour exécuter des scripts via OpenAPI.

   3. Réinitialisation ou suppression d'une clé secrète d'authentification à deux facteurs (facultatif)

      Vous pouvez réinitialiser une clé secrète d'authentification à deux facteurs lorsqu'un utilisateur perd l'accès à l'appareil sur lequel il utilise l'authentification à deux facteurs ou doit configurer l'authentification à deux facteurs sur un nouvel appareil. Vous pouvez également réinitialiser une clé secrète pour votre propre compte.

      Vous pouvez supprimer une clé secrète pour empêcher complètement un utilisateur de se connecter à la Web Console et pour empêcher cet utilisateur d'accéder au Serveur d'administration.

   4. Modification du nom d'un émetteur de code de sécurité (facultatif)

      Si vous disposez de plusieurs Serveurs d'administration avec des noms semblables, vous devrez peut-être modifier les noms des émetteurs de codes de sécurité afin de mieux reconnaître les différents Serveurs d'administration.

Résultats

À la fin de ce scénario :

- L'authentification à deux facteurs est configurée pour votre propre compte et pour un autre compte utilisateur qui doit accéder au Serveur d'administration.
- Les comptes d'intégration sont exclus de l'authentification à deux facteurs.

À propos de l'authentification à deux facteurs pour un compte

Kaspersky Security Center Linux propose une authentification à deux facteurs aux utilisateurs de Kaspersky Security Center Web Console. L'authentification à deux facteurs repose sur la norme RFC 6238 (TOTP : algorithme de mot de passe à usage unique basé sur le temps).

Chaque fois que vous vous connectez à Kaspersky Security Center Web Console, vous saisissez votre nom d'utilisateur et votre mot de passe, ainsi qu'un code de sécurité à usage unique. Pour recevoir un code de sécurité à usage unique, vous devez disposer d'une application d'authentification sur votre appareil mobile ou votre ordinateur.

Tout logiciel d'authentification prenant en charge l'algorithme TOTP (algorithme de mot de passe unique calculé en fonction du temps) peut être utilisé comme application d'authentification, par exemple, Google Authenticator. Pour générer le code de sécurité à usage unique, vous devez synchroniser l'heure définie sur l'appareil avec l'application d'authentification et l'heure définie sur l'appareil du Serveur d'administration. Pour une meilleure précision, nous vous recommandons d'utiliser les mêmes serveurs NTP dans toute votre infrastructure.

Pour vérifier si Kaspersky Security Center Linux prend en charge l'application d'authentification que vous souhaitez utiliser, essayez de configurer l'authentification à deux facteurs avec cette application d'authentification.

L'une des étapes propose d'indiquer le code de sécurité à usage unique généré par l'application d'authentification. Si l'opération réussit, Kaspersky Security Center Linux prend en charge l'authentificateur sélectionné.

Génération d'un code secret à l'aide d'une application d'authentification

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.

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. Un nouveau nom d'émetteur de code de sécurité est attribué au Serveur d'administration après la connexion suivante. Un code de sécurité est à usage unique et valide jusqu'à 30 secondes (la durée exacte peut varier).

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 sur lequel est installée l'application d'authentification.

L'authentification à deux facteurs présente les caractéristiques suivantes :

- Depuis la version 16.1 du Serveur d'administration, l'authentification à deux facteurs est activée automatiquement, et l'option permettant de configurer l'authentification à deux facteurs lors de la connexion est désactivée par défaut. La configuration de l'authentification à deux facteurs lors de la connexion est disponible uniquement pour les utilisateurs figurant dans la liste d'autorisation pour l'authentification à deux facteurs.
- Un utilisateur peut configurer l'authentification à deux facteurs uniquement pour son propre compte.
- Un utilisateur peut exclure des comptes de l'authentification à deux facteurs. Cela peut être nécessaire pour les comptes d'intégration qui ne peuvent pas recevoir de code de sécurité à usage unique pour l'authentification. Les comptes d'intégration sont utilisés pour exécuter des scripts via OpenAPI.
- Pour régénérer une clé secrète d'authentification à deux facteurs, l'utilisateur doit réinitialiser la clé secrète pour son propre compte.
- Pour réinitialiser ou supprimer une clé secrète d'authentification à deux facteurs pour le compte d'un autre utilisateur, l'utilisateur doit posséder un compte sur lequel l'authentification à deux facteurs est configurée et disposant du droit Modifier les ACL des objets dans la zone fonctionnelle **Fonctions générales** : **Autorisations d'utilisateur**.
- Pour exclure des comptes d'autres utilisateurs de l'authentification à deux facteurs ou pour modifier la liste d'autorisation pour l'authentification à deux facteurs, l'utilisateur doit posséder un compte sur lequel l'authentification à deux facteurs est configurée et disposant du droit Modifier les ACL des objets dans la zone fonctionnelle **Fonctions générales** : **Autorisations d'utilisateur**.
- L'authentification à deux facteurs doit toujours être configurée pour au moins un utilisateur, afin que celui-ci puisse gérer la liste d'autorisation et la liste d'exclusion de l'authentification à deux facteurs.
- L'authentification à deux facteurs est activée automatiquement uniquement pour le Serveur d'administration version 16.1. Si d'autres Serveurs d'administration principaux ou secondaires exécutent la version 16 ou une version antérieure, leurs paramètres d'authentification à deux facteurs resteront inchangés.

- Un Serveur d'administration virtuel hérite les paramètres de l'authentification à deux facteurs du Serveur d'administration physique, de sorte que, si l'authentification à deux facteurs est activée sur le Serveur d'administration physique, elle est également activée sur un Serveur d'administration virtuel. Vous ne pouvez pas configurer les paramètres de l'authentification à deux facteurs sur un Serveur d'administration virtuel.

- Pour que l'authentification à deux facteurs fonctionne correctement, vous devez mettre à niveau le Serveur d'administration et la Web Console vers la version 16.1 ou ultérieure.

Pour garantir une protection complète à l'aide de l'authentification à deux facteurs, il est nécessaire de sécuriser non seulement le Serveur d'administration, mais également l'appareil sur lequel il est installé. Pour ce faire, tenez compte des recommandations du Guide de renforcement.

Configuration d'une clé secrète d'authentification à deux facteurs pour Kaspersky Security Center Web Console

La fenêtre de configuration de l'authentification à deux facteurs s'ouvre lorsque vous vous connectez pour la première fois à Kaspersky Security Center Linux 16.1 ou version ultérieure.

Pour configurer l'authentification à deux facteurs pour votre compte, procédez comme suit :

1. Installez toute application prenant en charge l'algorithme de mot de passe unique calculé en fonction du temps (TOTP) sur l'appareil mobile ou l'ordinateur.

   Disponible en Russie :

   - Bitrix24 OTP
   - Yandex ID
   - Authentificateur Avanpost
   - Aladdin 2FA
   - Rutoken OTP

   Disponible dans le monde entier (y compris en Russie) :

   - Authentificateur Google
   - Authentification Microsoft

   Il est fortement déconseillé d'installer l'application d'authentification sur l'appareil à partir duquel le Serveur d'administration est géré.

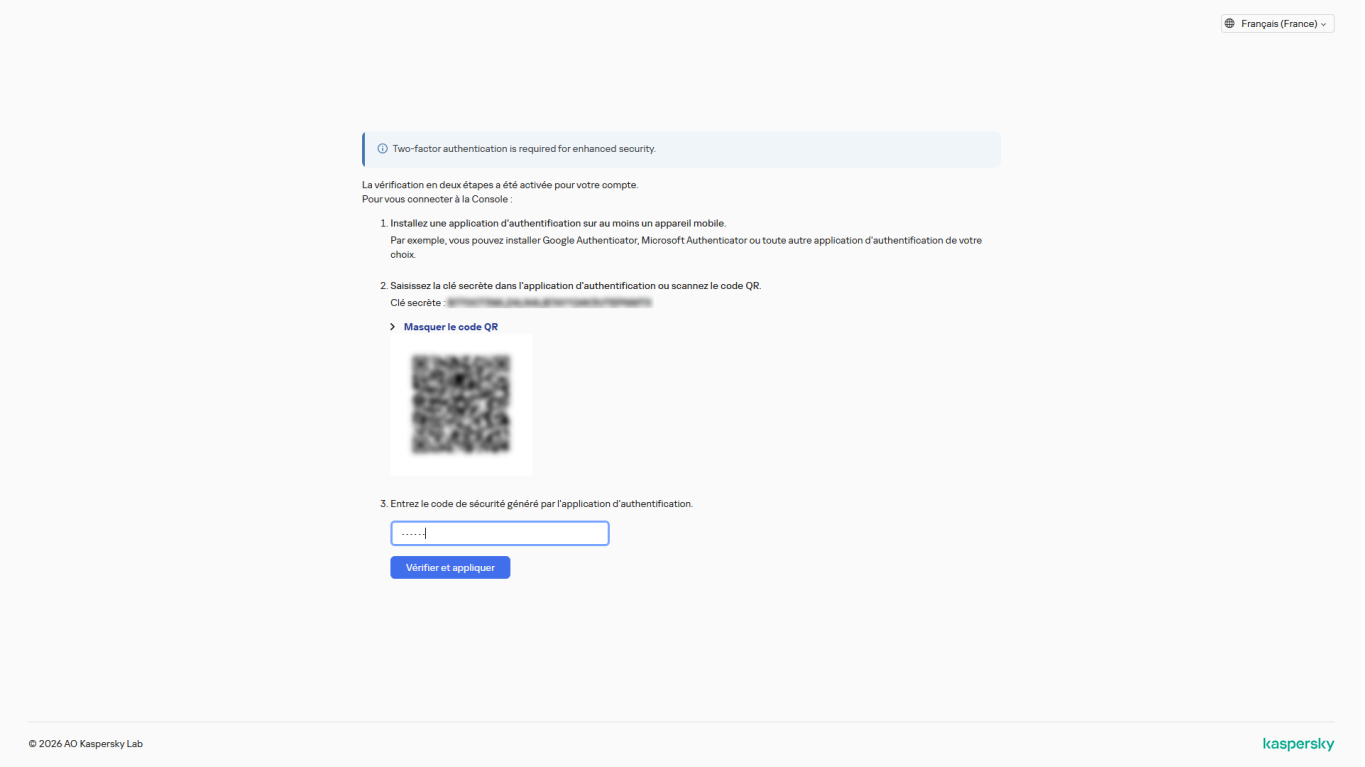
2. Assurez-vous que l'heure de l'appareil avec l'application d'authentification et l'heure de l'appareil avec le Serveur d'administration sont synchronisées au format UTC. Pour une meilleure précision, nous vous recommandons d'utiliser les mêmes serveurs NTP dans toute votre infrastructure.

3. Générez un code de sécurité à usage unique à l'aide de l'application d'authentification de l'appareil mobile ou de l'ordinateur. Pour ce faire, effectuez l'une des opérations suivantes :

   - Saisissez manuellement la clé secrète d'authentification à deux facteurs 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 à usage unique à 6 chiffres s'affichera sur l'appareil mobile.



Configuration d'une clé secrète d'authentification à deux facteurs pour Kaspersky Security Center Web Console

4. Dans la fenêtre d'**Authentification à deux facteurs**, indiquez le code de sécurité à usage unique généré par l'application d'authentification, puis cliquez sur le bouton **Vérifier et appliquer**.

   Configuration de Rutoken OTP

   Si vous utilisez Rutoken OTP, vous devez disposer d'un appareil mobile Android sur lequel l'application Rutoken OTP est installée. L'appareil mobile Android doit répondre aux exigences suivantes :

   - Système d'exploitation Android 7 ou plus récent.

   - Module NFC disponible et activé.

   Dans l'application Rutoken OTP, il faut configurer les paramètres suivants :

   - Scannez le code QR affiché dans l'assistant de configuration en deux étapes.

   - Réglez l'intervalle sur 30 secondes.

   - Sélectionnez SHA1 comme algorithme.

Pour configurer Rutoken OTP, procédez comme suit :

1. Placez l'appareil Rutoken OTP à côté de l'appareil mobile doté du module NFC.
2. Dans l'application Rutoken OTP, appuyez sur **Connecter le jeton**.
3. Dans l'application Rutoken OTP, appuyez sur **Configurer les paramètres**, puis sur **Enregistrer la clé secrète**.

   Si le jeton est correctement connecté à l'appareil mobile, l'application Rutoken OTP affiche les messages d'état suivants :

   - **Le jeton est connecté.**
   - **Les paramètres sont configurés.**
   - **La clé secrète est enregistrée.**
4. Sur l'appareil Rutoken OTP, appuyez sur le bouton.

   Un code de sécurité s'affiche sur l'appareil.
5. Dans Kaspersky Security Center Web Console, saisissez le code de sécurité dans la fenêtre de vérification en deux étapes.

L'authentification à deux facteurs est configurée pour votre compte. Vous pouvez accéder au Serveur d'administration conformément à vos privilèges.

Si vous n'avez pas accès à la configuration de l'authentification à deux facteurs, contactez un utilisateur disposant du droit Modifier les ACL des objets dans la zone fonctionnelle **Fonctions générales** : **Autorisations d'utilisateur** et de l'authentification à deux facteurs configurée pour ajouter votre compte à la liste d'autorisation pour l'authentification à deux facteurs.

Autorisation des utilisateurs à configurer l'authentification à deux facteurs

La liste d'autorisation pour l'authentification à deux facteurs est une liste d'utilisateurs qui sont autorisés à configurer initialement l'authentification à deux facteurs lorsqu'ils se connectent à la Web Console. Cette liste contient les comptes utilisateur sans authentification à deux facteurs configurée. Par défaut, les nouveaux comptes utilisateur ne sont pas inclus dans la liste d'autorisation pour l'authentification à deux facteurs et doivent être ajoutés à la liste par un administrateur. Si un nouveau compte est un compte d'intégration utilisé pour exécuter des scripts OpenAPI, il doit être exclu de l'authentification à deux facteurs.

Un compte utilisateur est automatiquement supprimé de la liste d'autorisation pour l'authentification à deux facteurs lorsque l'authentification à deux facteurs est configurée sur ce compte ou lorsque celui-ci est exclu de l'authentification à deux facteurs.

La modification manuelle de la liste d'autorisation pour l'authentification à deux facteurs est disponible pour les comptes sur lesquels l'authentification à deux facteurs est configurée et disposant du droit Modifier les ACL des objets dans la zone fonctionnelle **Fonctions générales** : **Autorisations d'utilisateur**.

Pour ajouter manuellement un compte utilisateur à la liste d'autorisation pour l'authentification à deux facteurs :

1. Dans le menu principal, cliquez sur le nom du Serveur d'administration.

   La fenêtre des propriétés du Serveur d'administration s'ouvre.

2. Sous l'onglet **Authentification à deux facteurs** de la fenêtre Propriétés, dans le tableau **Utilisateurs autorisés à générer des clés secrètes**, cliquez sur le bouton **Ajouter**.

3. Dans la fenêtre qui s'ouvre :

   a. Sélectionnez le compte utilisateur que vous voulez ajouter.

      Seuls les utilisateurs qui ne sont pas exclus de l'authentification à deux facteurs et qui ne possèdent pas de clé secrète d'authentification à deux facteurs peuvent être ajoutés à la liste d'autorisation pour l'authentification à deux facteurs.

   b. Si le compte est protégé contre les modifications non autorisées, vous devez confirmer que vous avez les autorisations pour modifier le compte en question. Dans la fenêtre **Protection du compte**, spécifiez les identifiants de votre propre compte et le code de sécurité à usage unique pour l'authentification à deux facteurs.

   c. Enregistrez vos modifications.

   Le compte utilisateur sélectionné est ajouté à la liste d'autorisation pour l'authentification à deux facteurs. Lors de la connexion suivante, l'utilisateur sera en mesure de générer une clé secrète.

Un compte utilisateur peut être supprimé de la liste d'autorisation pour l'authentification à deux facteurs jusqu'à ce que l'authentification à deux facteurs soit configurée pour ce compte.

Pour supprimer manuellement des comptes utilisateur de la liste d'autorisation pour l'authentification à deux facteurs, procédez comme suit :

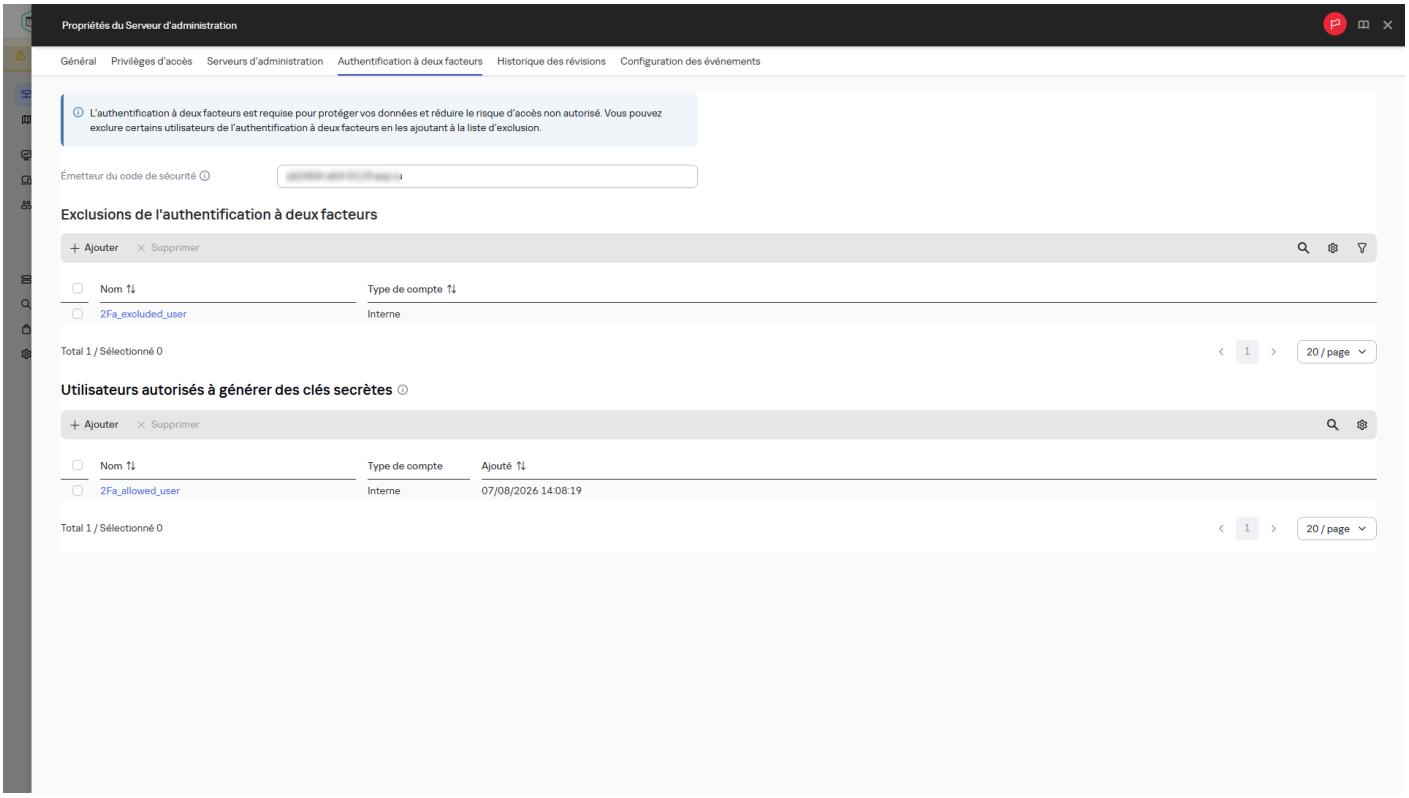
1. Dans le menu principal, cliquez sur le nom du Serveur d'administration.

   La fenêtre des propriétés du Serveur d'administration s'ouvre.

2. Sous l'onglet **Authentification à deux facteurs** de la fenêtre Propriétés, dans le tableau **Utilisateurs autorisés à générer des clés secrètes**, sélectionnez les comptes utilisateur que vous souhaitez supprimer, puis cliquez sur **Supprimer**.

3. Si le compte est protégé contre les modifications non autorisées, vous devez confirmer que vous avez les autorisations pour modifier le compte en question. Dans la fenêtre **Protection du compte**, spécifiez les identifiants de votre propre compte et le code de sécurité à usage unique pour l'authentification à deux facteurs.

Les comptes utilisateurs sélectionnés sont supprimés de la liste d'autorisation pour l'authentification à deux facteurs.



Configuration de la liste d'autorisation pour l'authentification à deux facteurs

Si, au cours d'une session active sur le Serveur d'administration, votre clé secrète d'authentification à deux facteurs est supprimée par un autre utilisateur, ou si vous réinitialisez vous-même la clé sans en créer une autre, la possibilité de modifier la liste d'autorisation pour l'authentification à deux facteurs est bloquée.

Des comptes utilisateur peuvent également être ajoutés et supprimés automatiquement de la liste d'autorisation pour l'authentification à deux facteurs.

Lorsque vous réinitialisez une clé secrète pour l'authentification à deux facteurs pour d'autres comptes, les comptes correspondants sont automatiquement ajoutés à la liste d'autorisation pour l'authentification à deux facteurs afin qu'ils puissent générer une nouvelle clé secrète.

Lors de la mise à niveau du Serveur d'administration depuis la version 16 ou antérieure vers la version 16.1 ou ultérieure, ainsi que lorsque vous créez une sauvegarde des données sur le Serveur d'administration version 16 ou antérieure et que vous la restaurez sur le Serveur d'administration version 16.1 ou ultérieure, les comptes utilisateur sont automatiquement ajoutés à la liste d'autorisation pour l'authentification à deux facteurs si toutes les conditions suivantes sont remplies :

- L'utilisateur dispose de l'autorisation de lecture dans la zone fonctionnelle *Fonctions générales : Fonctionnalité de base* attribuée directement à l'utilisateur (et non par l'intermédiaire d'un groupe de sécurité). La portée du rôle utilisateur disposant de cette autorisation doit inclure tous les appareils administrés et non attribués et doit être définie au niveau du Serveur d'administration.
- L'utilisateur n'est pas exclu de l'authentification à deux facteurs.
- L'utilisateur ne dispose pas de clé secrète pour l'authentification à deux facteurs.
- L'authentification à deux facteurs n'était pas activée pour tous les utilisateurs sur le Serveur d'administration de la version précédente.

Si une seule condition n'est pas remplie, l'utilisateur ne sera pas ajouté à la liste d'autorisation pour l'authentification à deux facteurs.

> Après une mise à niveau ou une restauration, nous vous recommandons de veiller à ce que la liste d'autorisation pour l'authentification à deux facteurs ne contienne que les comptes utilisateur qui doivent avoir accès au Serveur d'administration. Vérifiez la liste d'autorisation pour l'authentification à deux facteurs et supprimez tout autre compte. Ajoutez les comptes d'intégration utilisés pour exécuter des scripts via OpenAPI à la liste des exclusions pour éviter l'échec des scripts.

Les comptes des utilisateurs perdront l'accès au Serveur d'administration après une mise à niveau ou une restauration si toutes les conditions suivantes sont remplies :

- L'utilisateur dispose de l'autorisation de lecture dans la zone fonctionnelle *Fonctions générales : Fonctionnalité de base* attribuée par l'intermédiaire d'un groupe de sécurité (et non directement à l'utilisateur) ou ne dispose pas du tout de cette autorisation.
- L'utilisateur n'est pas exclu de l'authentification à deux facteurs.
- L'utilisateur ne dispose pas de clé secrète pour l'authentification à deux facteurs.
- L'authentification à deux facteurs n'était pas activée pour tous les utilisateurs sur le Serveur d'administration de la version précédente.

Si nécessaire, ces comptes peuvent être ajoutés manuellement à la liste d'autorisation pour l'authentification à deux facteurs.

Réinitialisation et suppression d'une clé secrète d'authentification à deux facteurs

Vous pouvez réinitialiser une clé secrète lorsqu'un utilisateur perd l'accès à l'appareil sur lequel il utilise l'authentification à deux facteurs ou doit configurer l'authentification à deux facteurs sur un nouvel appareil. La réinitialisation de la clé secrète permet à l'utilisateur de se connecter de nouveau à la Web Console et de générer une nouvelle clé secrète.

Vous pouvez réinitialiser ou supprimer une clé secrète d'authentification à deux facteurs pour les comptes d'autres utilisateurs uniquement si vous avez configuré la clé secrète d'authentification à deux facteurs et si vous disposez du droit Modifier les ACL des objets dans la zone fonctionnelle **Fonctions générales** : **Autorisations d'utilisateur**. Vous pouvez également régénérer votre propre clé secrète.

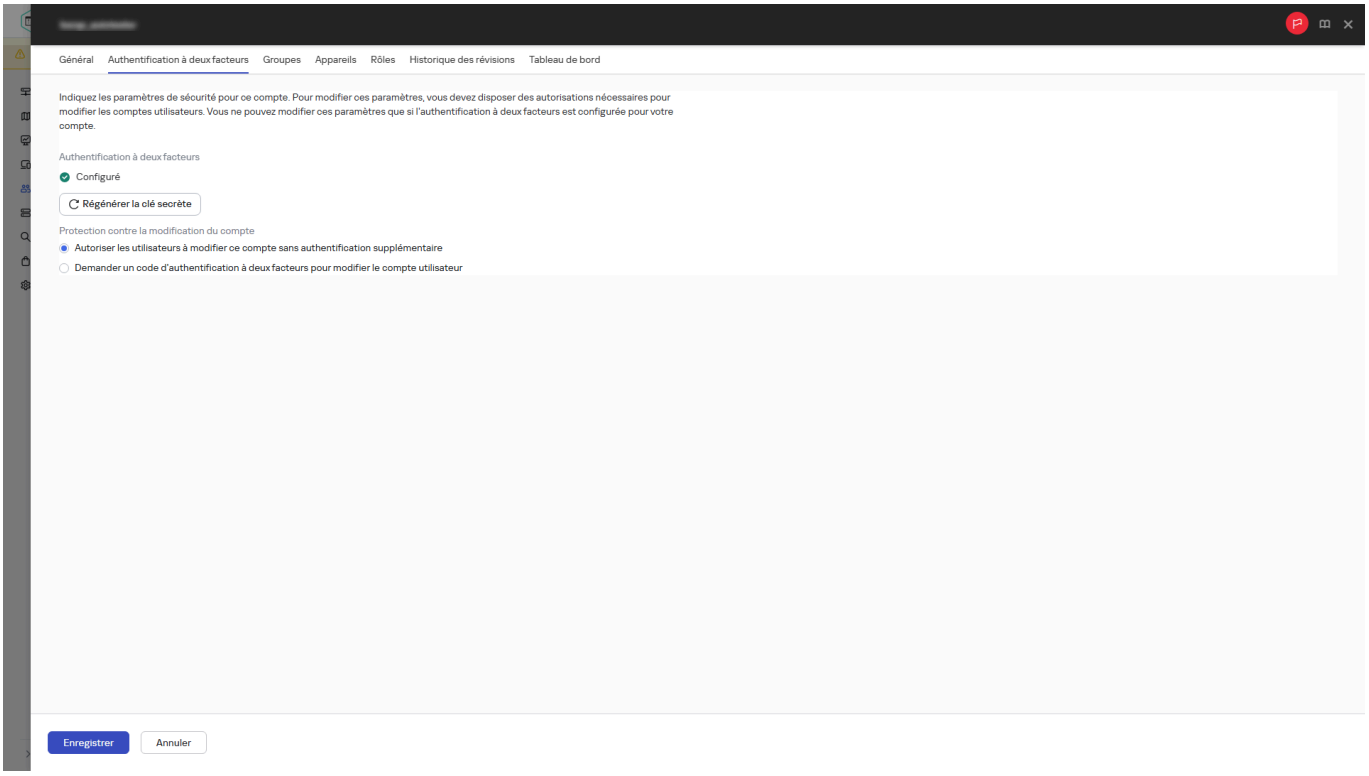
Pour réinitialiser une clé secrète pour un compte, procédez comme suit :

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 réinitialiser une clé secrète.

3. Si vous souhaitez réinitialiser une clé secrète pour votre compte, procédez comme suit :

   a. Sous l'onglet **Authentification à deux facteurs**, cliquez sur le bouton **Régénérer la clé secrète**.

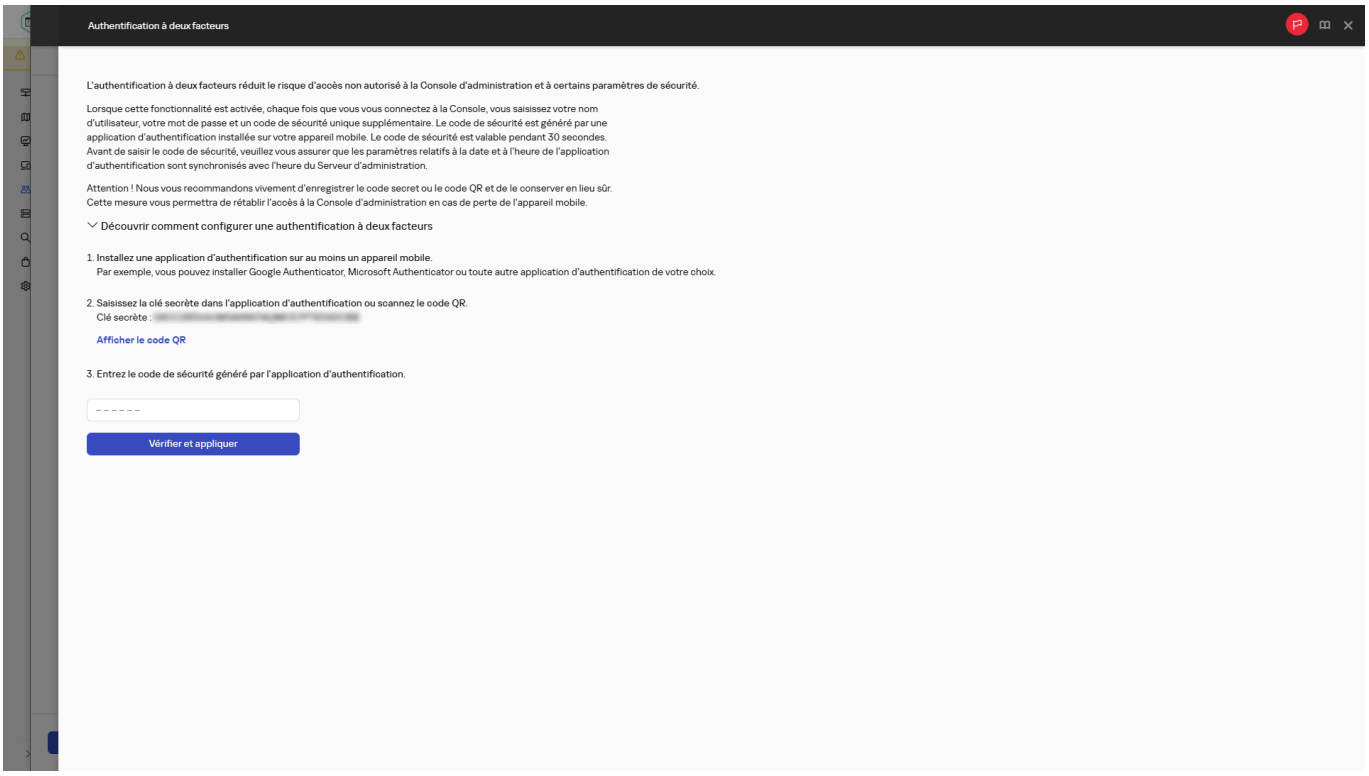


Régénération de la clé secrète d'authentification à deux facteurs pour le compte utilisateur actuel

   a. Si votre compte est protégé contre les modifications non autorisées, vous devez confirmer que vous avez les autorisations pour modifier le compte en question. Dans la fenêtre **Protection du compte**, spécifiez les identifiants de votre propre compte et le code pour l'authentification à deux facteurs.

   b. Dans la fenêtre d'**Authentification à deux facteurs**, cliquez sur **Découvrir comment configurer une authentification à deux facteurs**, puis cliquez sur **Afficher le code QR**.

   c. Utilisez l'application d'authentification sur l'appareil mobile pour scanner le QR code et recevoir un code de sécurité à usage unique.



Configuration d'une nouvelle clé secrète d'authentification à deux facteurs pour le compte utilisateur actuel

a. Dans la fenêtre d'**Authentification à deux facteurs**, indiquez le code de sécurité généré par l'application d'authentification, cliquez sur le bouton **Vérifier et appliquer**, puis enregistrez les modifications.

Configuration de Rutoken OTP

Si vous utilisez Rutoken OTP, vous devez disposer d'un appareil mobile Android sur lequel l'application Rutoken OTP est installée. L'appareil mobile Android doit répondre aux exigences suivantes :

- Système d'exploitation Android 7 ou plus récent.
- Module NFC disponible et activé.

Dans l'application Rutoken OTP, il faut configurer les paramètres suivants :

- Scannez le code QR affiché dans l'assistant de configuration en deux étapes.
- Réglez l'intervalle sur 30 secondes.
- Sélectionnez SHA1 comme algorithme.

Pour configurer Rutoken OTP, procédez comme suit :

1. Placez l'appareil Rutoken OTP à côté de l'appareil mobile doté du module NFC.
2. Dans l'application Rutoken OTP, appuyez sur **Connecter le jeton**.
3. Dans l'application Rutoken OTP, appuyez sur **Configurer les paramètres**, puis sur **Enregistrer la clé secrète**.

Si le jeton est correctement connecté à l'appareil mobile, l'application Rutoken OTP affiche les messages d'état suivants :

- **Le jeton est connecté.**
- **Les paramètres sont configurés.**
- **La clé secrète est enregistrée.**

4. Sur l'appareil Rutoken OTP, appuyez sur le bouton.

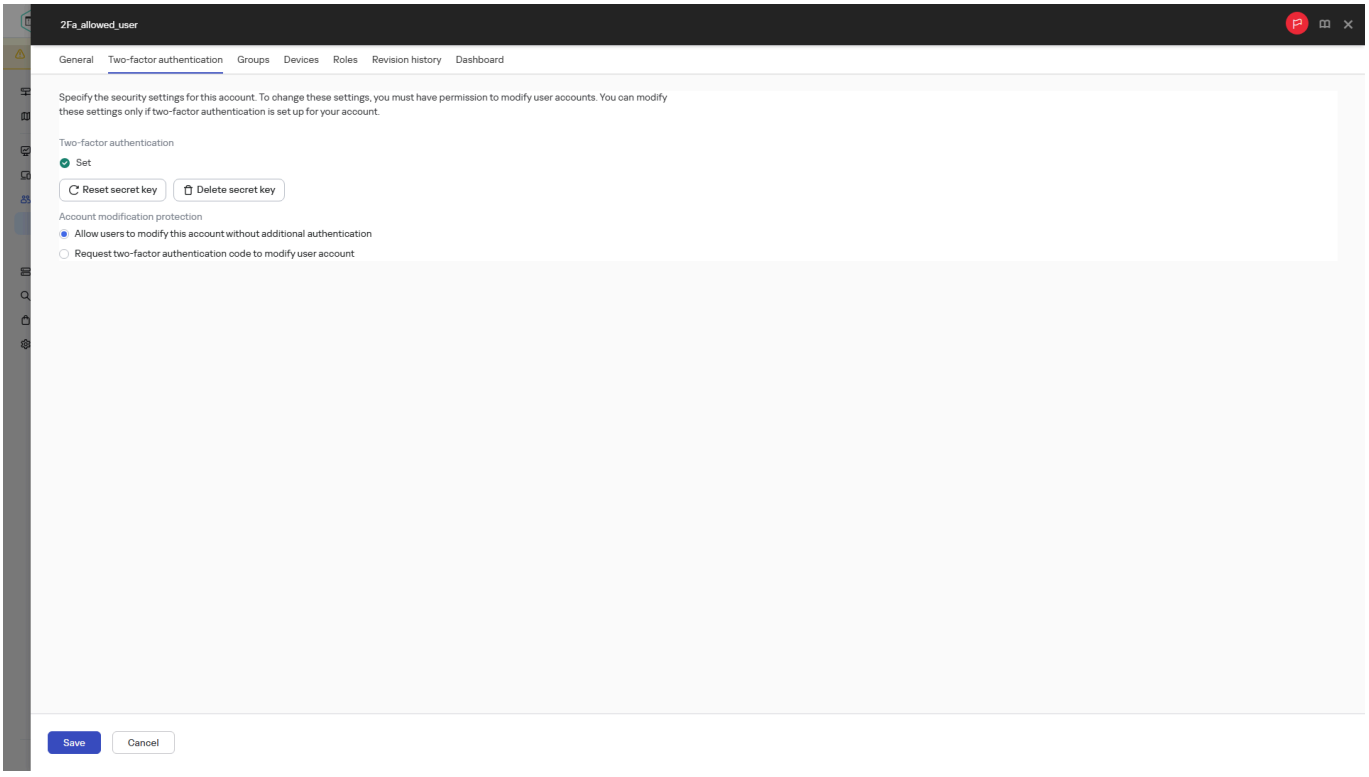
   Un code de sécurité s'affiche sur l'appareil.

5. Dans Kaspersky Security Center Web Console, saisissez le code de sécurité dans la fenêtre de vérification en deux étapes.

La clé secrète pour votre compte a été modifiée.

4. Si vous souhaitez réinitialiser une clé secrète pour un autre compte, procédez comme suit :

   a. Sous l'onglet **Authentification à deux facteurs**, cliquez sur le bouton **Réinitialiser la clé secrète**.



Réinitialisation de la clé secrète d'authentification à deux facteurs pour un autre compte utilisateur

   a. Si le compte est protégé contre les modifications non autorisées, vous devez confirmer que vous avez les autorisations pour modifier le compte en question. Dans la fenêtre **Protection du compte**, spécifiez les identifiants de votre propre compte et le code de sécurité à usage unique pour l'authentification à deux facteurs.

   b. Confirmez la réinitialisation de la clé secrète, puis enregistrez les modifications.

Lorsque vous réinitialisez une clé secrète pour un autre compte, la clé secrète existante est supprimée, et le compte utilisateur est ajouté à la liste d'autorisation pour l'authentification à deux facteurs dans les propriétés du Serveur d'administration. Lors de la connexion suivante, l'utilisateur sera en mesure de générer une nouvelle clé secrète.

La clé secrète d'un compte utilisateur est réinitialisée.

Vous pouvez supprimer une clé secrète pour empêcher complètement un utilisateur de se connecter à la Web Console et pour empêcher cet utilisateur d'accéder au Serveur d'administration.

Pour supprimer une clé secrète, 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 supprimer une clé secrète.

   Vous ne pouvez pas supprimer une clé secrète pour votre propre compte.

3. Sous l'onglet **Authentification à deux facteurs**, cliquez sur le bouton **Supprimer la clé secrète**.

4. Si le compte est protégé contre les modifications non autorisées, vous devez confirmer que vous avez les autorisations pour modifier le compte en question. Dans la fenêtre **Protection du compte**, spécifiez les identifiants de votre propre compte et le code de sécurité à usage unique pour l'authentification à deux facteurs.

5. Confirmez la suppression de la clé secrète, puis enregistrez les modifications.

La clé secrète d'un compte utilisateur est supprimée.

Vous pouvez rétablir l'accès en ajoutant l'utilisateur à la liste d'autorisation pour l'authentification à deux facteurs dans les propriétés du Serveur d'administration. Dans ce cas, lors de la connexion suivante, l'utilisateur sera en mesure de générer une nouvelle clé secrète.

Exclusion de comptes de l'authentification à deux facteurs

Vous pouvez exclure des comptes utilisateur de l'authentification à deux facteurs pour leur permettre de se connecter au Serveur d'administration même s'ils n'ont pas configuré l'authentification à deux facteurs. L'exclusion des comptes de l'authentification à deux facteurs peut être nécessaire pour les comptes d'intégration qui ne peuvent pas fournir le code de sécurité à usage unique lors de l'authentification. Les comptes d'intégration sont utilisés pour exécuter des scripts via OpenAPI.

Vous pouvez modifier la liste des exclusions si l'authentification à deux facteurs est configurée pour votre compte et si vous disposez du droit Modifier les ACL des objets dans la zone fonctionnelle **Fonctions générales** : **Autorisations d'utilisateur**.

Pour exclure un compte utilisateur de l'authentification à deux facteurs, procédez comme suit :

1. Dans le menu principal, cliquez sur le nom du Serveur d'administration.

   La fenêtre des propriétés du Serveur d'administration s'ouvre.

2. Sous l'onglet **Authentification à deux facteurs** de la fenêtre Propriétés, dans le tableau **Exclusions de l'authentification à deux facteurs**, cliquez sur le bouton **Ajouter**.

3. Dans la fenêtre qui s'ouvre :

   a. Sélectionnez le compte utilisateur que vous voulez exclure.

   b. Si le compte est protégé contre les modifications non autorisées, vous devez confirmer que vous avez les autorisations pour modifier le compte en question. Dans la fenêtre **Protection du compte**, spécifiez les identifiants de votre propre compte et le code de sécurité à usage unique pour l'authentification à deux facteurs.

   c. Enregistrez vos modifications.

   Les comptes utilisateur sélectionnés sont exclus de l'authentification à deux facteurs, et leurs clés secrètes, si elles existent, sont supprimées. La liste des comptes exclus n'est pas modifiée lorsque vous restaurez une sauvegarde sur le Serveur d'administration 16.1, ou lorsque vous mettez à niveau le Serveur d'administration vers la version 16.1 ou ultérieure. Si les comptes figurant dans la liste des exclusions contenaient des clés secrètes dans la version précédente du Serveur d'administration, ces clés secrètes seront supprimées dans la version 16.1.

Vous pouvez supprimer des comptes utilisateur de la liste des exclusions pour empêcher complètement les utilisateurs de se connecter à la Web Console et d'accéder au Serveur d'administration.

Pour supprimer des comptes utilisateur de la liste des exclusions :

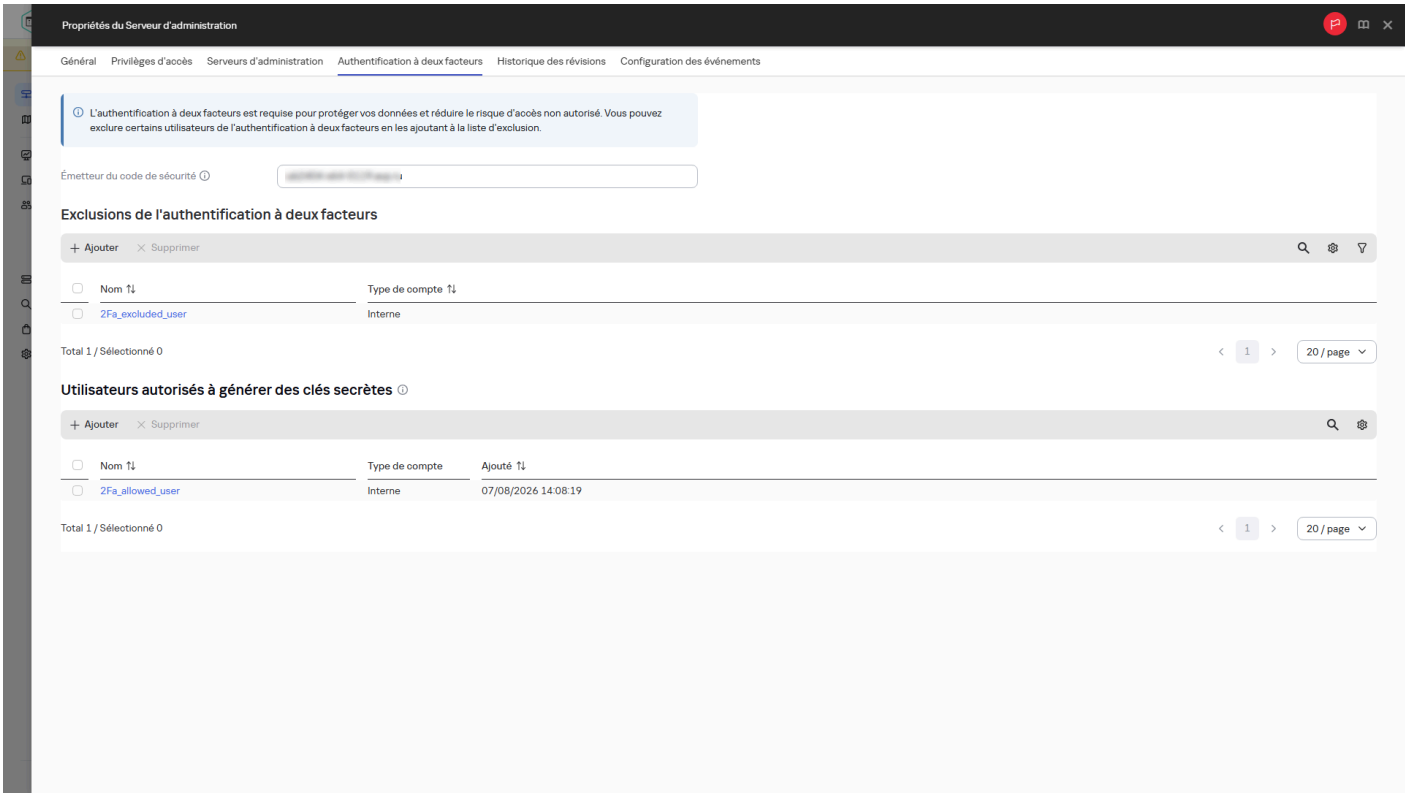
1. Dans le menu principal, cliquez sur le nom du Serveur d'administration.

   La fenêtre des propriétés du Serveur d'administration s'ouvre.

2. Sous l'onglet **Authentification à deux facteurs** de la fenêtre Propriétés, dans le tableau **Exclusions de l'authentification à deux facteurs**, sélectionnez les comptes utilisateur que vous souhaitez supprimer, puis cliquez sur **Supprimer**.

3. Si le compte est protégé contre les modifications non autorisées, vous devez confirmer que vous avez les autorisations pour modifier le compte en question. Dans la fenêtre **Protection du compte**, spécifiez les identifiants de votre propre compte et le code de sécurité à usage unique pour l'authentification à deux facteurs.

Les comptes utilisateur sélectionnés sont supprimés de la liste d'exclusions.



Configuration de la liste d'exclusion de l'authentification à deux facteurs

Modification du nom d'un émetteur de code de sécurité

Vous pouvez avoir plusieurs identifiants (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.

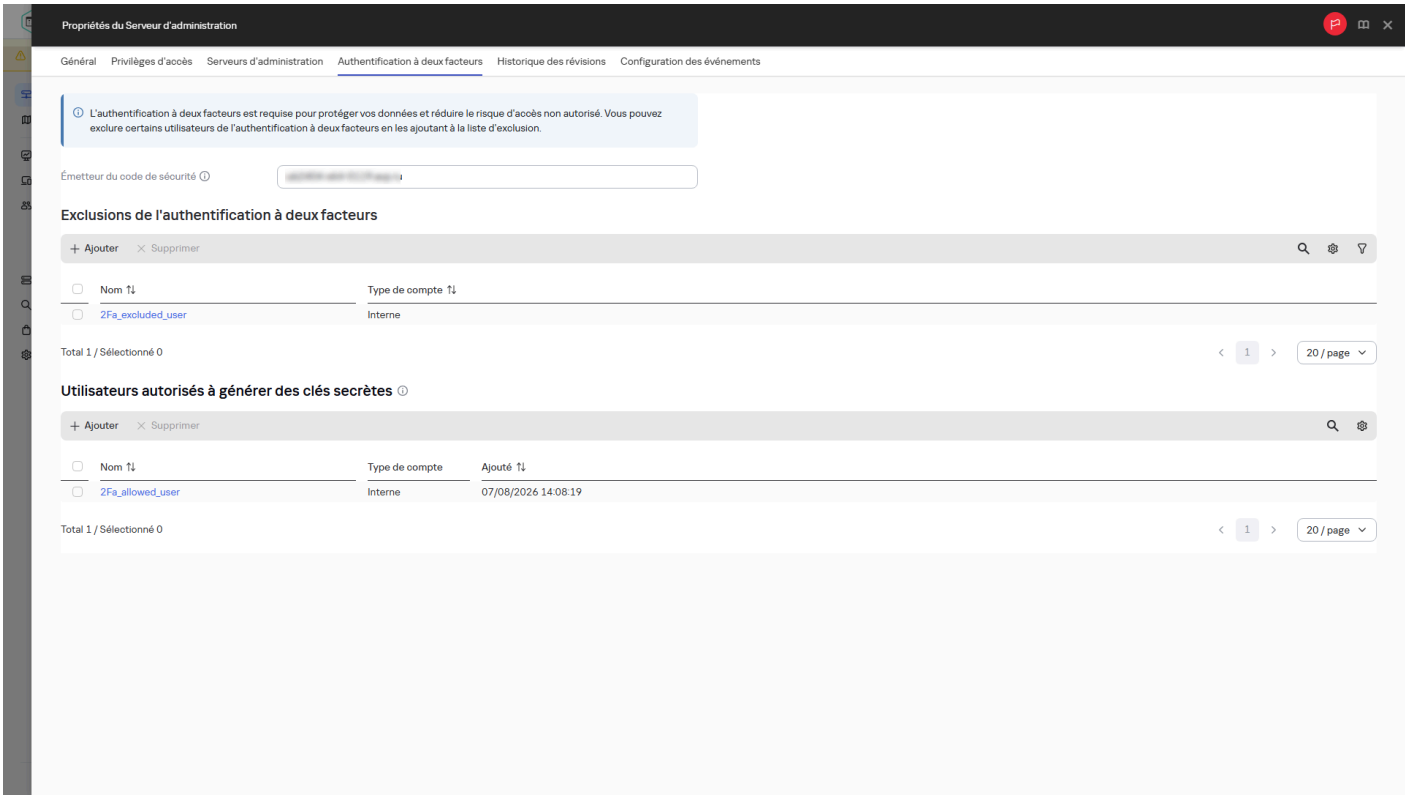
Pour spécifier un nouveau nom d'émetteur du code de sécurité :

1. Dans le menu principal, cliquez sur le nom du Serveur d'administration.

   La fenêtre des propriétés du Serveur d'administration s'ouvre.

2. Sous l'onglet **Authentification à deux facteurs** de la fenêtre Propriétés, saisissez un nouveau nom dans le champ **Émetteur du code de sécurité**, puis enregistrez les modifications.

Un nouveau nom d'émetteur de code de sécurité est attribué au Serveur d'administration après la connexion suivante.



Spécification du nom d'un émetteur de code de sécurité

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 de saisie du mot de passe autorisées est égal à 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.

   L'authentification à deux facteurs doit toujours être configurée pour au moins un utilisateur, afin que celui-ci puisse gérer la liste d'autorisation et la liste d'exclusion de l'authentification à deux facteurs.

3. Cliquez sur le bouton **Supprimer**.

4. Dans la fenêtre qui s'ouvre, cliquez sur **OK**.

L'utilisateur ou le groupe de sécurité est supprimé.

Modification du mot de passe d'un compte utilisateur

Vous devrez peut-être modifier le mot de passe de votre propre compte ou de celui d'un autre utilisateur si le mot de passe actuel est sur le point d'expirer ou si vous souhaitez le remplacer par un mot de passe plus sécurisé.

Le mot de passe doit remplir les conditions suivantes :

- Le mot de passe doit compter entre 8 et 256 caractères.
- Le mot de passe doit compter des caractères d'au moins trois des groupes ci-dessous :
  - Lettres majuscules (A–Z)
  - Lettre minuscules (a-z)

- Chiffres (0–9)
- Caractères spéciaux (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)

- Le mot de passe ne doit contenir aucun caractère d'espacement, aucun caractère Unicode, ni la combinaison de "." et de "@" lorsque "." précède "@".

Modification du mot de passe de votre compte

Pour modifier le mot de passe de votre compte, procédez comme suit :

1. Dans le volet supérieur, accédez au menu de votre compte en cliquant sur le nom de votre compte.
2. Dans la liste déroulante, sélectionnez **Modifier le mot de passe**.
3. Dans le volet droit qui s'ouvre, saisissez le mot de passe actuel, puis indiquez le nouveau mot de passe pour la connexion à Kaspersky Security Center Linux.

   Pour consulter le mot de passe saisi, cliquez sur 👁.
4. Si votre compte est protégé contre les modifications non autorisées, vous devez confirmer que vous avez les autorisations pour modifier le compte en question. Dans la fenêtre **Protection du compte**, indiquez les identifiants de votre propre compte ou du compte disposant du droit Modifier les ACL des objets dans la zone fonctionnelle **Fonctions générales** : **Autorisations d'utilisateur**.
5. Saisissez un code de sécurité à usage unique généré à l'aide de l'application d'authentification de l'appareil mobile.

Modification du mot de passe d'un compte utilisateur interne

Pour modifier le mot de passe d'un compte utilisateur interne, procédez comme suit :

1. Dans le menu principal, accédez à **Utilisateurs et rôles** → **Utilisateurs et groupes**, puis sélectionnez l'onglet **Utilisateurs**.
2. Cliquez sur le nom du compte utilisateur que vous souhaitez modifier.
3. Dans la fenêtre des paramètres utilisateur qui s'ouvre, sous l'onglet **Général**, cliquez sur le bouton **Modifier le mot de passe**.
4. Définissez un nouveau mot de passe pour connecter l'utilisateur à Kaspersky Security Center Linux.

   Pour consulter le mot de passe saisi, cliquez sur 👁.
5. Si nécessaire, vous pouvez activer l'option **L'utilisateur doit changer son mot de passe lors de la première connexion** pour forcer la modification du mot de passe lors de l'authentification de l'utilisateur suivante.

6. Si le compte est protégé contre les modifications non autorisées, vous devez confirmer que vous avez les autorisations pour modifier le compte en question. Dans la fenêtre **Protection du compte**, indiquez les identifiants du compte disposant du droit Modifier les ACL des objets dans la zone fonctionnelle **Fonctions générales** : **Autorisations d'utilisateur**.

7. Saisissez un code de sécurité à usage unique généré à l'aide de l'application d'authentification de l'appareil mobile.

Configuration des options de modification du mot de passe à l'aide d'indicateurs du serveur

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 l'Agent d'administration est installé. Le répertoire d'installation par défaut est `/opt/kaspersky/ksc64/sbin`. Exécutez les commande suivantes :

- Configuration de la période de rotation des mots de passe (l'indicateur `LP_SplPwdChangePeriodDays`)

  ```
  ./klscflag -fset -pv .core/.independent -s KLLIM -n LP_SplPwdChangePeriodDays -t d -v
  < rotation_period >
  ```

  Où `< période_de_rotation >` est une période en jours après laquelle le mot de passe de l'utilisateur expire. Valeurs possibles : 0–730. Si la valeur du paramètre est 0, la rotation du mot de passe est désactivée.

- Configuration de l'heure de l'avertissement préliminaire sur la nécessité de modifier le mot de passe (indicateur `LP_SplPwdChangeNotificationHours`)

  ```
  ./klscflag -fset -pv .core/.independent -s KLLIM -n LP_SplPwdChangeNotificationHours -
  t d -v < warning_time >
  ```

  Où `< temps_d'avertissement >` est une période en heures avant l'expiration du mot de passe de l'utilisateur. Pendant ce temps, la notification indiquant le besoin de modifier le mot de passe s'affiche. Valeurs possibles : 0–17520. Si la valeur du paramètre est 0, la durée d'avertissement est égale à 25 % de la période de rotation du mot de passe.

- Précision de la valeur par défaut de l'option **L'utilisateur doit changer son mot de passe lors de la première connexion** (l'indicateur `LP_SplPwdForceChange`)

  ```
  ./klscflag -fset -pv .core/.independent -s KLLIM -n LP_SplPwdForceChange -t d -v
  < value >
  ```

  Où les valeurs possibles du paramètre `< valeur >` sont :

  `1` : l'option **L'utilisateur doit changer son mot de passe lors de la première connexion** est activée.

  `0` : l'option **L'utilisateur doit changer son mot de passe lors de la première connexion** est désactivée.

Pour consulter la valeur actuelle de l'indicateur, exécutez la commande suivante :

```
./klscflag -fget -pv .core/.independent -s KLLIM -n < drapeau > -t d
```

Où `< indicateur >` est l'indicateur `LP_SplPwdChangePeriodDays`, `LP_SplPwdChangeNotificationHours` ou `LP_SplPwdForceChange`.

Création d'un rôle d'utilisateur

Pour créer un rôle d'utilisateur, procédez comme suit :

1. Dans le menu principal, accédez à **Utilisateurs et rôles** → **Rôles**.
2. Cliquez sur **Ajouter**.
3. Dans la fenêtre **Nom du nouveau rôle** qui s'ouvre, saisissez le nom du nouveau rôle.
4. Cliquez sur le bouton **OK** pour appliquer les modifications.
5. Dans la fenêtre des propriétés du rôle qui s'ouvre, modifiez les paramètres du rôle :
   - Sous l'onglet **Général**, modifiez le nom du rôle.
     Il est impossible de modifier le nom d'un rôle système.
   - Sous l'onglet **Configuration**, 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 **Enregistrer** pour 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 **Configuration**, 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 **Enregistrer** pour 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 **Configuration**.

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 le nom du Serveur d'administration.

   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 le bouton **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 **Configuration** et passez à la section **Stratégies**.
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 le nom du Serveur d'administration.

   La fenêtre des propriétés du Serveur d'administration s'ouvre avec l'onglet **Général** sélectionné.

2. Passez à la section **Hiérarchie des Serveurs d'administration**.

3. Activez l'option **Relayer la liste des rôles aux Serveurs d'administration secondaires**, puis cliquez sur le bouton **Enregistrer**.

L'application copie les rôles d'utilisateurs du Serveur d'administration principal sur les Serveurs d'administration secondaires.

Quand l'option **Relayer la liste des rôles aux Serveurs d'administration secondaires** est activée et que les rôles d'utilisateurs sont propagés, ces rôles ne peuvent être ni modifiés, ni supprimés sur les Serveurs d'administration secondaires. Quand vous créez un rôle ou modifiez un rôle existant sur le Serveur d'administration principal, les modifications sont appliquées automatiquement aux Serveurs d'administration secondaires. Quand vous supprimez un rôle d'utilisateur sur le Serveur d'administration principal, ce rôle demeure sur les Serveurs d'administration secondaires, mais il peut alors modifié ou supprimé.

Les rôles propagés sur le Serveur d'administration secondaire depuis le Serveur d'administration primaire sont accompagnés de coches vertes (✓). Il est impossible de modifier ces rôles sur le Serveur d'administration secondaire.

Si vous créez un rôle sur le Serveur d'administration principal et s'il existe un rôle portant ce nom sur son Serveur d'administration secondaire, le nouveau rôle est copié sur ce Serveur d'administration secondaire avec un index ajouté à son nom, par exemple ~~1, ~~2 (l'index peut être aléatoire).

Quand vous désactivez l'option **Relayer la liste des rôles aux Serveurs d'administration secondaires**, tous les rôles d'utilisateurs demeurent sur les Serveurs d'administration secondaires, mais deviennent indépendants des rôles sur le Serveur d'administration principal. Une fois qu'ils sont devenus indépendants, ces rôles d'utilisateurs sur les Serveurs d'administration secondaires peuvent être modifiés ou supprimés.

Modification du mot de passe d'un compte

Vous pouvez modifier le mot de passe du compte local, par exemple, si l'utilisateur oublie le mot de passe du compte local ou pour effectuer une modification planifiée du mot de passe.

La modification du mot de passe s'appliquera même si l'utilisateur ne s'est pas connecté au compte. Vous pouvez également modifier le mot de passe du compte root local.

Cette tâche peut être exécutée uniquement sur les appareils Linux.

Pour modifier le mot de passe du compte local sur des appareils en particulier, procédez comme suit :

1. Dans le menu principal, accédez à **Gestion des ressources** → **Tâches**.

2. Cliquez sur **Ajouter**.

   Ceci permet de lancer l'Assistant de création d'une tâche.

3. Dans le champ **Type de tâche**, sélectionnez l'option **Modifier le mot de passe du compte (Linux uniquement)**.

4. Sélectionnez l'une des options ci-dessous :

   - **Attribuer la tâche à un groupe d'administration**

     La tâche est affectée aux appareils qui appartiennent à un groupe d'administration. Vous pouvez renseigner un des groupes existants ou en créer un.

     Par exemple, vous pourriez souhaiter utiliser cette option pour exécuter une tâche d'envoi de messages pour les utilisateurs si le message est particulier pour les appareils repris dans un groupe d'administration spécifique.

     Si une tâche est attribuée à un groupe d'administration, l'onglet **Sécurité** ne s'affiche pas dans la fenêtre des propriétés de la tâche, car les tâches de groupe sont soumises aux paramètres de sécurité des groupes auxquels elles s'appliquent.

   - **Définir les adresses des appareils manuellement ou les importer à partir de la 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 *Modifier le mot de passe du compte (Linux uniquement)* est créée pour les appareils spécifiés. Si vous avez sélectionné l'option **Attribuer la tâche à un groupe d'administration**, la tâche est de groupe.

5. À l'étape Zone d' **Zone d'action d'une tâche**, indiquez un groupe d'administration, des appareils avec des adresses spécifiques ou une sélection d'appareils.

   Les paramètres disponibles dépendent de l'option sélectionnée à l'étape précédente.

6. À l'étape **Saisissez le nom du compte et le nouveau mot de passe**, configurez les paramètres suivants :

   - Dans le champ **Nom du compte utilisateur**, indiquez le nom du compte dont vous souhaitez modifier le mot de passe.

   - Dans le champ **Nouveau mot de passe**, indiquez le mot de passe qui sera défini pour le compte indiqué dans le champ précédent.

     Pour afficher les caractères que vous avez entrés, cliquez sur le bouton **Afficher** et maintenez-le enfoncé.

- Si nécessaire, cochez la case **Définir comme mot de passe à usage unique (l'utilisateur doit modifier le mot de passe après la première connexion)**.

  - **Définir comme mot de passe à usage unique (l'utilisateur doit modifier le mot de passe après la première connexion)**

    Si la case est cochée, l'utilisateur sera invité à définir un nouveau mot de passe après la première connexion.

    Si la case est décochée, l'utilisateur ne sera plus invité à définir un nouveau mot de passe après la première connexion.

    Celle-ci est décochée par défaut.

7. À l'étape **Fin de la création de la tâche**, cliquez sur le bouton **Terminer** pour créer la tâche et fermer l'Assistant.

   Si vous avez activé l'option **Ouvrir les détails de la tâche à la fin de la création**, la fenêtre des paramètres de la tâche s'ouvre. Dans cette fenêtre, vous pouvez vérifier les paramètres de la tâche, les modifier ou configurer une planification de lancement de la tâche, si nécessaire.

8. Dans la liste des tâches, sélectionnez la tâche que vous avez créée, puis cliquez sur **Démarrer**.

   Vous pouvez également attendre que la tâche se lance conformément à la planification que vous avez spécifiée dans les paramètres de la tâche.

Une fois que la tâche de modification du mot de passe du compte est terminée, le mot de passe du compte local indiqué est modifié sur les appareils indiqués.

Pour garantir le bon fonctionnement des tâches de modification du mot de passe du compte, SELinux doit être désactivé sur l'appareil de l'utilisateur.

Révocation des droits d'administrateur local

Vous pouvez révoquer les droits d'administrateur local des comptes. Cela vous offre un niveau de contrôle supplémentaire sur les comptes utilisateurs. Par exemple, vous pouvez révoquer les droits d'administrateur local à l'issue d'une attribution à usage unique.

Suite à l'exécution de cette tâche, le compte local indiqué vérifie s'il appartient aux groupes d'administrateurs locaux. Ces groupes sont définis dans les paramètres de la stratégie de l'Agent d'administration. Vous pouvez personnaliser la liste des groupes d'administrateurs locaux dans les paramètres de la stratégie de l'Agent d'administration. Vous pouvez également consulter la liste des comptes utilisateurs à privilèges à l'aide du **Rapport sur les utilisateurs d'appareils à privilèges (Linux uniquement)**.

Cette tâche peut être exécutée uniquement sur les appareils Linux.

Pour révoquer les droits d'administrateur local sur des appareils en particulier, procédez comme suit :

1. Dans le menu principal, accédez à **Gestion des ressources** → **Tâches**.

2. Cliquez sur **Ajouter**.

   Ceci permet de lancer l'Assistant de création d'une tâche.

3. Dans le champ **Type de tâche**, sélectionnez l'option **Révoquer les autorisations d'administrateur local (Linux uniquement)**.

4. Sélectionnez l'une des options ci-dessous :

   - **Attribuer la tâche à un groupe d'administration**

     La tâche est affectée aux appareils qui appartiennent à un groupe d'administration. Vous pouvez renseigner un des groupes existants ou en créer un.

     Par exemple, vous pourriez souhaiter utiliser cette option pour exécuter une tâche d'envoi de messages pour les utilisateurs si le message est particulier pour les appareils repris dans un groupe d'administration spécifique.

     Si une tâche est attribuée à un groupe d'administration, l'onglet **Sécurité** ne s'affiche pas dans la fenêtre des propriétés de la tâche, car les tâches de groupe sont soumises aux paramètres de sécurité des groupes auxquels elles s'appliquent.

   - **Définir les adresses des appareils manuellement ou les importer à partir de la 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 *Révoquer les droits d'administrateur local (Linux uniquement)* est créée pour les appareils indiqués. Si vous avez sélectionné l'option **Attribuer la tâche à un groupe d'administration**, la tâche est de groupe.

5. À l'étape Zone d' **Zone d'action d'une tâche**, indiquez un groupe d'administration, des appareils avec des adresses spécifiques ou une sélection d'appareils.

   Les paramètres disponibles dépendent de l'option sélectionnée à l'étape précédente.

6. À cette étape de l'Assistant, définissez les paramètres suivants :

   - Dans le groupe de paramètres **Mode de fonctionnement**, sélectionnez le mode de fonctionnement :

     - **Révoquer les privilèges d'administrateur local des comptes répertoriés**

       Si cette option a été sélectionnée, les droits d'administrateur local des comptes locaux indiqués seront révoqués.

       Cette option est sélectionnée par défaut.

- **Exclure les comptes mentionnés de la révocation des privilèges d'administrateur local**

  Si cette option a été sélectionnée, les droits d'administrateur local seront révoqués pour tous les comptes locaux, sauf les comptes indiqués.

  Par défaut, cette option n'est pas sélectionnée.

- Indiquez les comptes locaux :
  - Cliquez sur le bouton **Ajouter**.
  - Dans la fenêtre qui s'ouvre, réalisez une des opérations suivantes :
    - Dans le champ **Nom du compte utilisateur**, indiquez le nom du compte local.
    - Dans le groupe de paramètres **Action du compte** (disponible uniquement si l'option **Révoquer les privilèges d'administrateur local des comptes répertoriés** est sélectionnée), sélectionnez l'action.
    - **Garder le compte**

      Si cette option a été sélectionnée, le compte local n'est pas supprimé après la révocation des droits d'administrateur local.

      Cette option est sélectionnée par défaut.

    - **Supprimer le compte**

      Si cette option a été sélectionnée, le compte local sera supprimé, qu'il dispose ou non des droits d'administrateur local.

      Par défaut, cette option n'est pas sélectionnée.

7. À l'étape **Fin de la création de la tâche**, cliquez sur le bouton **Terminer** pour créer la tâche et fermer l'Assistant.

   Si vous avez activé l'option **Ouvrir les détails de la tâche à la fin de la création**, la fenêtre des paramètres de la tâche s'ouvre. Dans cette fenêtre, vous pouvez vérifier les paramètres de la tâche, les modifier ou configurer une planification de lancement de la tâche, si nécessaire.

8. Dans la liste des tâches, sélectionnez la tâche que vous avez créée, puis cliquez sur **Démarrer**.

   Vous pouvez également attendre que la tâche se lance conformément à la planification que vous avez spécifiée dans les paramètres de la tâche.

Lorsque la tâche de révocation des droits d'administrateur local est terminée, les droits d'administrateur local sont révoqués pour les comptes locaux définis sur les appareils en question.

Configuration de l'authentification de domaine Kerberos

Kaspersky Security Center Linux vous permet d'utiliser l'authentification de domaine via le protocole Kerberos. L'authentification par domaine vous permet d'activer l'authentification sécurisée dans Kaspersky Security Center Web Console sans avoir à saisir à nouveau le mot de passe sur le réseau d'entreprise (authentification unique).

Vous devez d'abord configurer votre contrôleur de domaine pour utiliser Kerberos et générer un fichier keytab. Pour en savoir plus, consultez la documentation de votre contrôleur de domaine.

SCRIL (Carte à puce requise pour l'ouverture de session interactive) est pris en charge pour Microsoft Active Directory.

Génération d'un fichier keytab pour FreeIPA et AldPro

Pour générer un fichier keytab :

1. Créez un compte utilisateur qui sera utilisé par IAM pour accéder au contrôleur de domaine.

2. Si le Serveur d'administration se trouve en dehors du domaine FreeIPA/AldPro, ajoutez l'entrée DNS et l'entrée hôte :

   ```
   ipa dnsrecord-add <zoneName> <recordName> --a-rec < Adresse IP du Serveur d'administration >
   ```

   ```
   ipa host-add --password=<password> < Adresse de l'hôte du Serveur d'administration >
   ```

3. Lors de la création du service HTTP pour le Serveur d'administration, précisez le type de PAC :

   ```
   ipa service-add HTTP/< FQDN de l'hôte du Serveur d'administration >@< DOMAINE ÉCRIT EN MAJUSCULES > --ok-to-auth-as-delegate=true --pac-type PAD
   ```

4. Spécifiez le compte utilisateur pour l'authentification :

   ```
   ipa service-allow-retrieve-keytab HTTP/< Adresse de l'hôte du Serveur d'administration >@< DOMAINE ÉCRIT EN MAJUSCULES > --user=<user>
   ```

5. Exportez le fichier keytab :

   ```
   ipa-getkeytab -s < Adresse du contrôleur de domaine > -p HTTP/< Adresse de l'hôte du Serveur d'administration >@< DOMAINE ÉCRIT EN MAJUSCULES > -k /tmp/h.keytab
   ```

Génération d'un fichier keytab pour Microsoft Active Directory

Pour générer un fichier keytab :

1. Créez un compte utilisateur qui sera utilisé par IAM pour communiquer avec le contrôleur de domaine.

2. Activez les options suivantes pour le compte utilisateur :

   - **L'utilisateur ne peut pas modifier le mot de passe**

   - **Chiffrement Kerberos AES 256 bits**

   Vous pouvez activer l'option **Le mot de passe n'expire jamais** pour éviter de devoir réémettre le fichier keytab à chaque expiration du mot de passe.

3. Ajoutez un nom principal de service (SPN) au compte utilisateur :

   ```
   setspn -S HTTP/< FQDN de l'hôte du Serveur d'administration > < DOMAINE ÉCRIT EN MAJUSCULES >\<user>
   ```

4. Exportez le fichier keytab :

```
ktpass -out C:\<folder>\< Nom du fichier keytab > -princ HTTP/< FQDN de l'hôte du
Serveur d'administration >@< DOMAINE ÉCRIT EN MAJUSCULES > -mapuser < DOMAINE ÉCRIT EN
MAJUSCULES >\<user> -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass <password> -
mapop set
```

Génération d'un fichier keytab pour Samba

Pour générer un fichier keytab :

1. Créez un compte utilisateur qui sera utilisé par IAM pour communiquer avec le contrôleur de domaine :

```
samba-tool user add <user>
```

2. Ajoutez le SPN au compte utilisateur :

```
samba-tool spn add HTTP/< FQDN de l'hôte du Serveur d'administration > <user>
```

3. Exportez le fichier keytab :

```
samba-tool domain exportkeytab /tmp/file.keytab --principal=HTTP/< FQDN de l'hôte du
Serveur d'administration >
```

Activation de l'authentification de domaine Kerberos

Pour activer l'authentification de domaine Kerberos, procédez comme suit :

1. effectuez un sondage du contrôleur de domaine.
2. Dans le menu principal, accédez à la section **Paramètres** → **Authentification unique**.
3. Activez l'option **Authentification Kerberos**.
4. Chargez le fichier keytab.
5. Attribuez aux utilisateurs du domaine un rôle qui autorise l'accès à Kaspersky Security Center Web Console.

   L'authentification du domaine Kerberos est activée pour les utilisateurs du domaine.

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 **Activé** 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 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.

7. **Approbation et refus des mises à jour des applications administrées par Kaspersky**

   Par défaut, les mises à jour logicielles téléchargées sont à l'état *Non défini*. Vous pouvez modifier l'état en *Approuvée* ou *Rejetée*. Les mises à jour confirmées sont toujours installées. Si la mise à jour d'une application gérée par Kaspersky nécessite une révision et l'acceptation des termes du Contrat de licence utilisateur final, vous devez d'abord les accepter. Ensuite, la mise à jour peut être propagée sur les appareils administrés. Les mises à jour auxquelles vous avez attribué l'état *Rejetée* ne seront pas installées sur les appareils. Si une mise à jour rejetée pour une application gérée a été installée précédemment, Kaspersky Security Center Linux essaiera de la désinstaller de tous les appareils.

   L'approbation et le refus de mises à jour est disponible uniquement pour l'Agent d'administration et les applications Kaspersky administrées installées sur les appareils clients Windows et Linux. La mise à jour transparente du Serveur d'administration, de Kaspersky Security Center Web Console et des plug-ins Web d'administration n'est pas prise en charge.

   Instructions pratiques : approbation et refus de mises à jour

   Parfois, après la mise à jour de l'Agent d'administration, vous pouvez être invité à redémarrer les appareils administrés. Si la notification concernant le redémarrage requis s'affiche, cliquez sur le lien **Consulter les appareils** dans la notification, cochez les cases en regard des appareils à redémarrer, puis cliquez sur le bouton **Redémarrage** pour terminer la mise à jour de l'Agent d'administration.

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

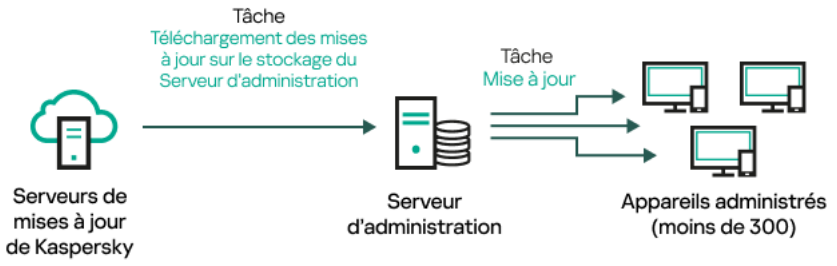
  Kaspersky Security Center Linux permet de mettre à jour automatiquement l'Agent d'administration et les applications Kaspersky installées sur les appareils clients Windows et Linux. La mise à jour transparente du Serveur d'administration, de Kaspersky Security Center Web Console et des plug-ins Web d'administration n'est pas prise en charge. Pour mettre à jour ces modules, vous devez télécharger les dernières versions à partir du site Internet de Kaspersky, puis les installer manuellement.

En fonction de la configuration de votre réseau, vous pouvez utiliser les schémas suivants de téléchargement et de distribution des mises à jour requises sur les appareils administrés :

- En utilisant une seule tâche : *Téléchargement des mises à jour sur le stockage du Serveur d'administration*
- En utilisant deux tâches :
  - *Téléchargement des mises à jour sur le stockage du Serveur d'administration*
  - Tâche de *Téléchargement des mises à jour sur les stockages des points de distribution*
- Manuellement via un dossier 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).



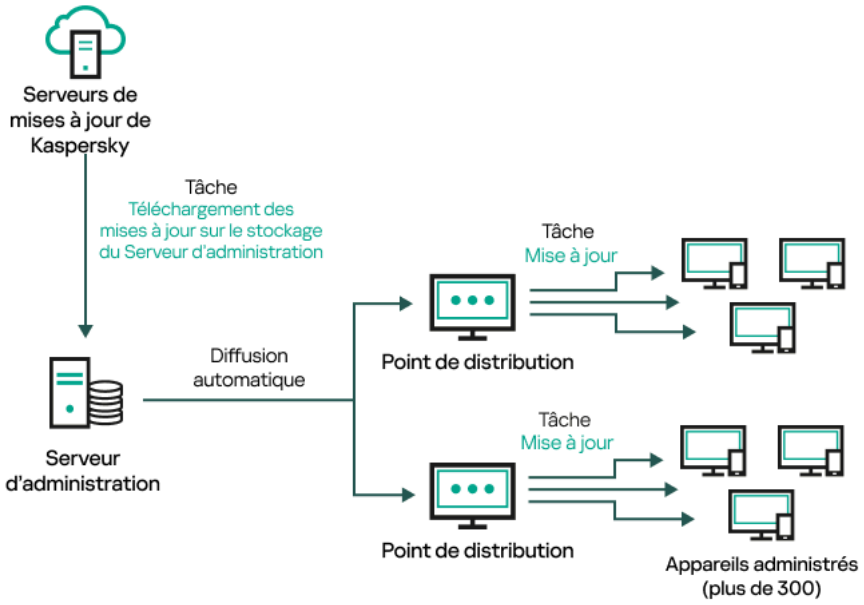
Mise à jour à l'aide de la tâche *Téléchargement des mises à jour sur le stockage du Serveur d'administration* sans points de distribution

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.

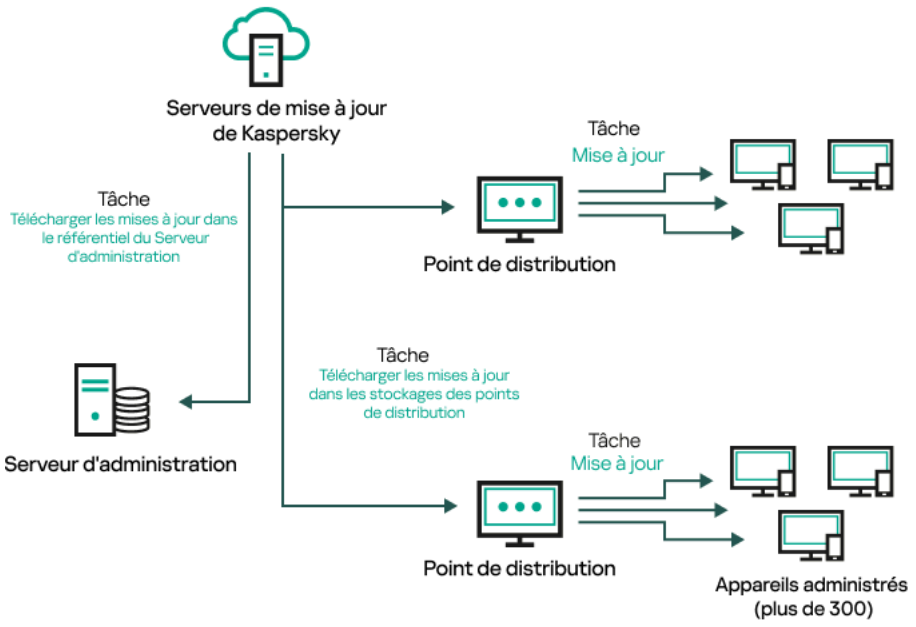
Chaque application de Kaspersky sollicite les mises à jour requises au serveur d'administration. Le Serveur d'administration accumule ces requêtes et télécharge uniquement les mises à jour requises par n'importe quelle application. Cela évite de télécharger les mêmes mises à jour plusieurs fois, voire 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* et de la tâche *Téléchargement des mises à jour sur les stockages des points de distribution*

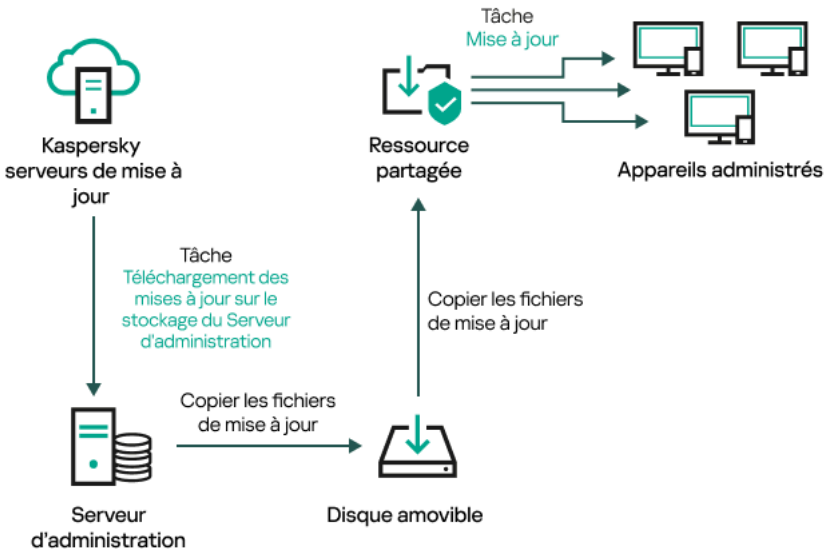
Par défaut, le Serveur d'administration et les points de distribution communiquent avec les serveurs de mise à jour de Kaspersky et télécharge les mises à jour au moyen du protocole HTTPS. Vous pouvez configurer le Serveur d'administration et/ou les points de distribution pour utiliser le protocole HTTP au lieu de HTTPS.

Pour implémenter ce schéma, créez la tâche *Téléchargement des mises à jour sur les stockages des points de distribution* en plus de la tâche *Téléchargement des mises à jour sur le stockage du Serveur d'administration*. Ensuite, les points de distribution téléchargent les mises à jour à partir des serveurs de mise à jour de Kaspersky, et non à partir du stockage du Serveur d'administration.

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 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).



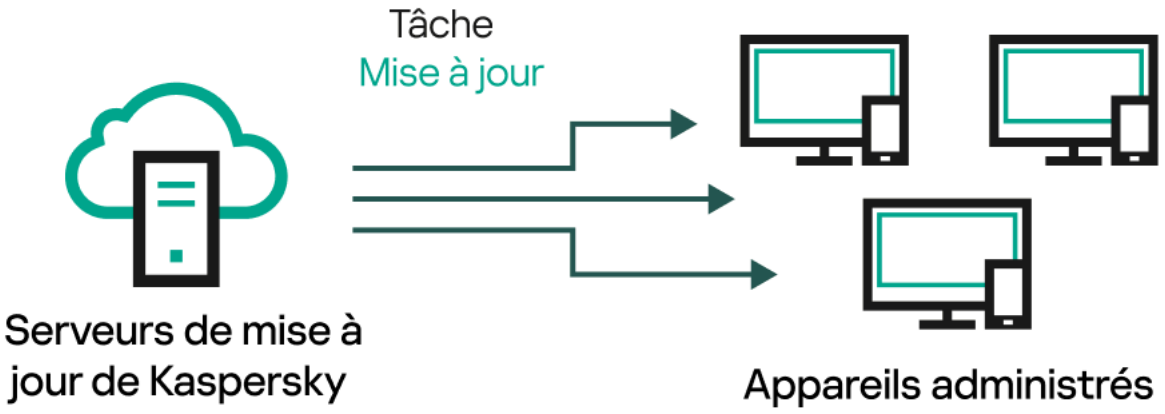
Mise à jour via un dossier local, un dossier partagé ou un serveur FTP

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

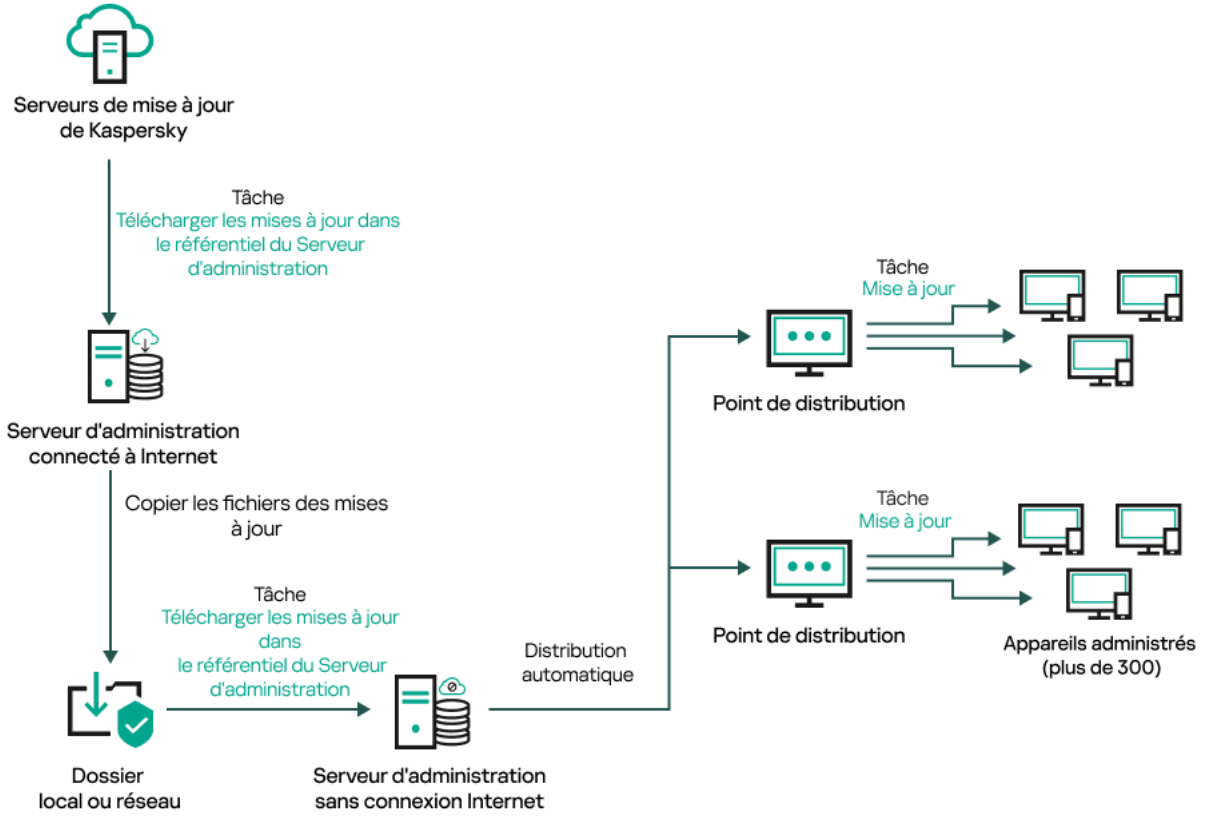
Via un dossier local ou réseau si le Serveur d'administration n'a pas de connexion Internet

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 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*. Si nécessaire, vous pouvez également configurer l'option *Télécharger automatiquement le fichier de demande de mise à jour* afin que Kaspersky Update Utility télécharge uniquement les mises à jour requises.

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 :

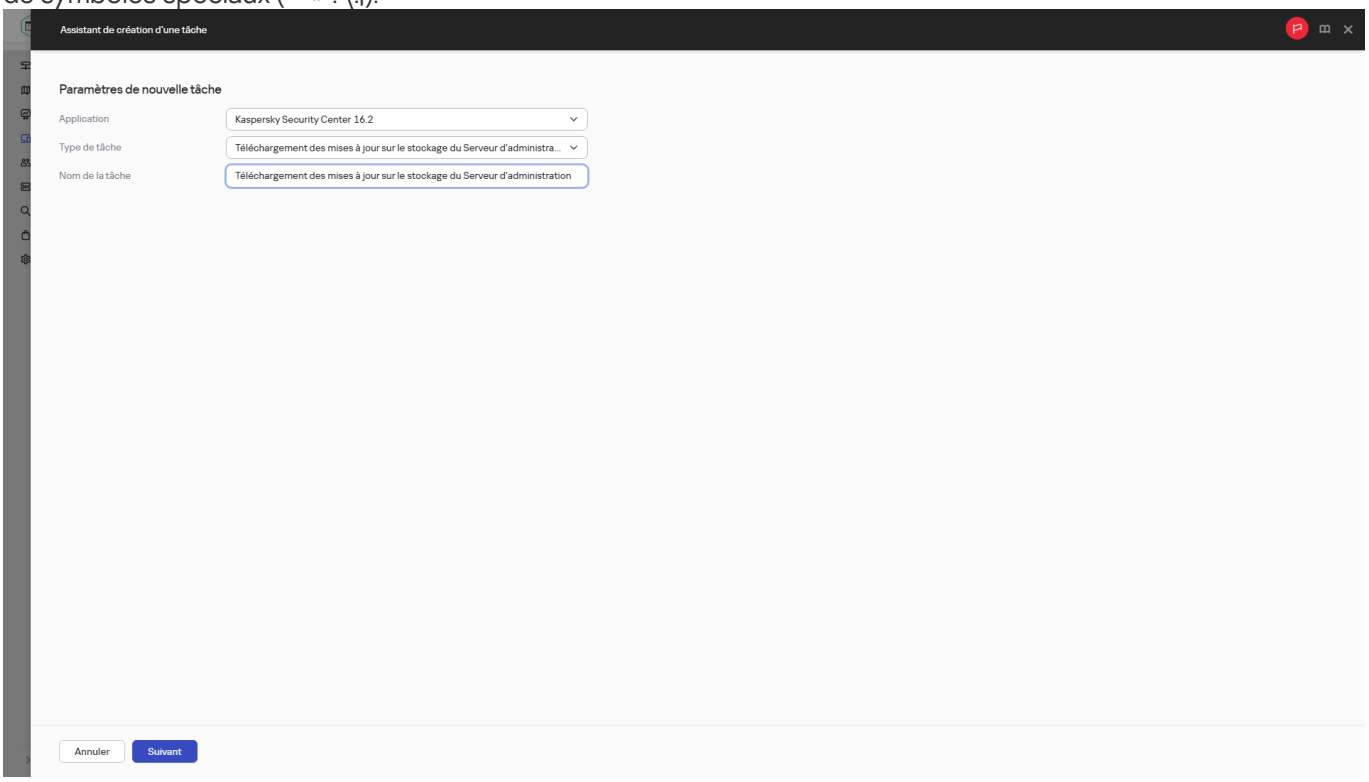
1. Dans le menu principal, accédez à **Gestion des ressources** → **Tâches**.

2. Cliquez sur **Ajouter**.

   Ceci permet de lancer l'assistant de création d'une tâche. Suivez les étapes de l'assistant.

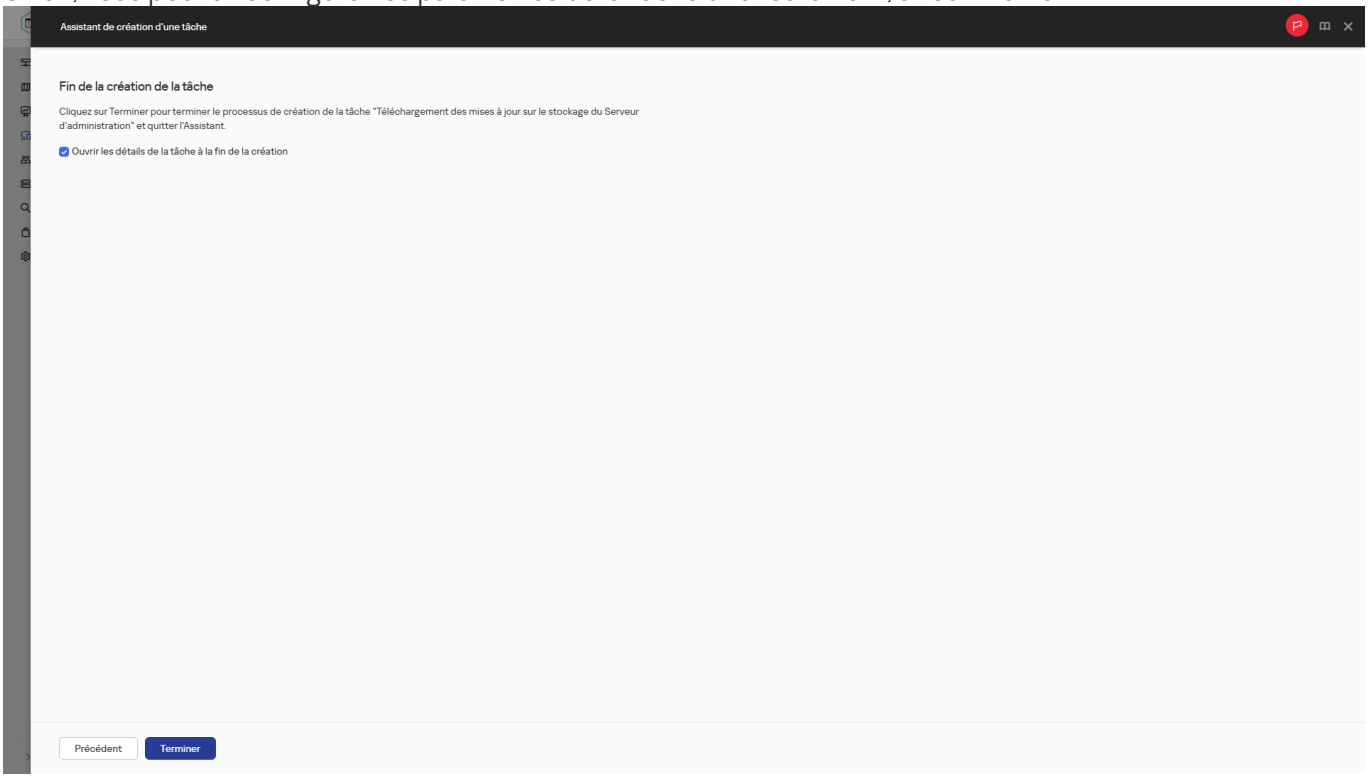
3. Pour l'application Kaspersky Security Center, sélectionnez le type de tâche **Téléchargement des mises à jour sur le stockage du Serveur d'administration**.

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 ("*<>?\:|).



Créez la tâche Téléchargement des mises à jour sur le stockage du Serveur d'administration

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, à tout moment.



Fin de la création de la tâche

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 de l'application**, spécifiez les paramètres suivants :

- **Sources des mises à jour**

  Comme source de mises à jour, voici ce que vous pouvez utiliser :

  - Serveurs de mise à jour de Kaspersky (sélectionnés par défaut)
  - Serveur d'administration principal

    Cette ressource s'applique aux tâches créées pour un Serveur d'administration virtuel ou secondaire.
  - Dossier local ou réseau

    Un dossier local ou de réseau qui contient les mises à jour les plus récentes. Un dossier de réseau peut être un serveur FTP ou HTTP ou un dossier partagé SMB.

    Lors de la sélection du dossier local, il faut indiquer le dossier sur l'appareil avec le Serveur d'administration installé. Le chemin d'accès au dossier dépend du système d'exploitation de l'appareil. Étant donné que le dossier local se trouve sur un Serveur d'administration basé sur Linux, vous devez préciser le chemin d'accès POSIX, par exemple : /path/to/dir.

    Lorsque vous sélectionnez un dossier réseau SMB comme source de mise à jour, montez ce dossier sur l'appareil sur lequel le Serveur d'administration est installé avant de le sélectionner. Indiquez ensuite le chemin d'accès au dossier monté en utilisant son chemin d'accès dans le système de fichiers local. L'accès au dossier s'effectue à l'aide du protocole SMB.

    Un dossier local ou réseau, ou un serveur FTP ou HTTP utilisé comme source de mise à jour, doit contenir une structure de dossiers identique à celle des serveurs de mise à jour de Kaspersky. Vous pouvez obtenir cette structure à l'aide de Kaspersky Update Utility.

  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.

Si vous choisissez de copier les mises à jour téléchargées dans un dossier local, vous devez spécifier un dossier sur l'appareil sur lequel le Serveur d'administration est installé. Le chemin d'accès au dossier dépend du système d'exploitation de l'appareil. Étant donné que le dossier local se trouve sur un Serveur d'administration basé sur Linux, vous devez préciser le chemin d'accès POSIX, par exemple : /path/to/dir.

Lorsque vous sélectionnez un dossier réseau situé sur un Serveur d'administration fonctionnant sous Linux, vous devez vous assurer au préalable que l'accès à ce dossier réseau est possible depuis l'appareil sur lequel le Serveur d'administration est installé, en montant le dossier. L'accès au dossier s'effectue à l'aide du protocole SMB.

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 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 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 sur les stockages** 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.

- **Télécharger automatiquement le fichier de demande de mise à jour**

Si vous souhaitez utiliser Kaspersky Update Utility pour télécharger uniquement les mises à jour requises avec une configuration appropriée, activez cette option et indiquez le chemin où Kaspersky Security Center Linux créera le fichier de demande de mise à jour avec des informations sur les mises à jour à télécharger. Le fichier de demande de mise à jour contient l'horodatage et le hachage MD5 pour le contrôle de version.

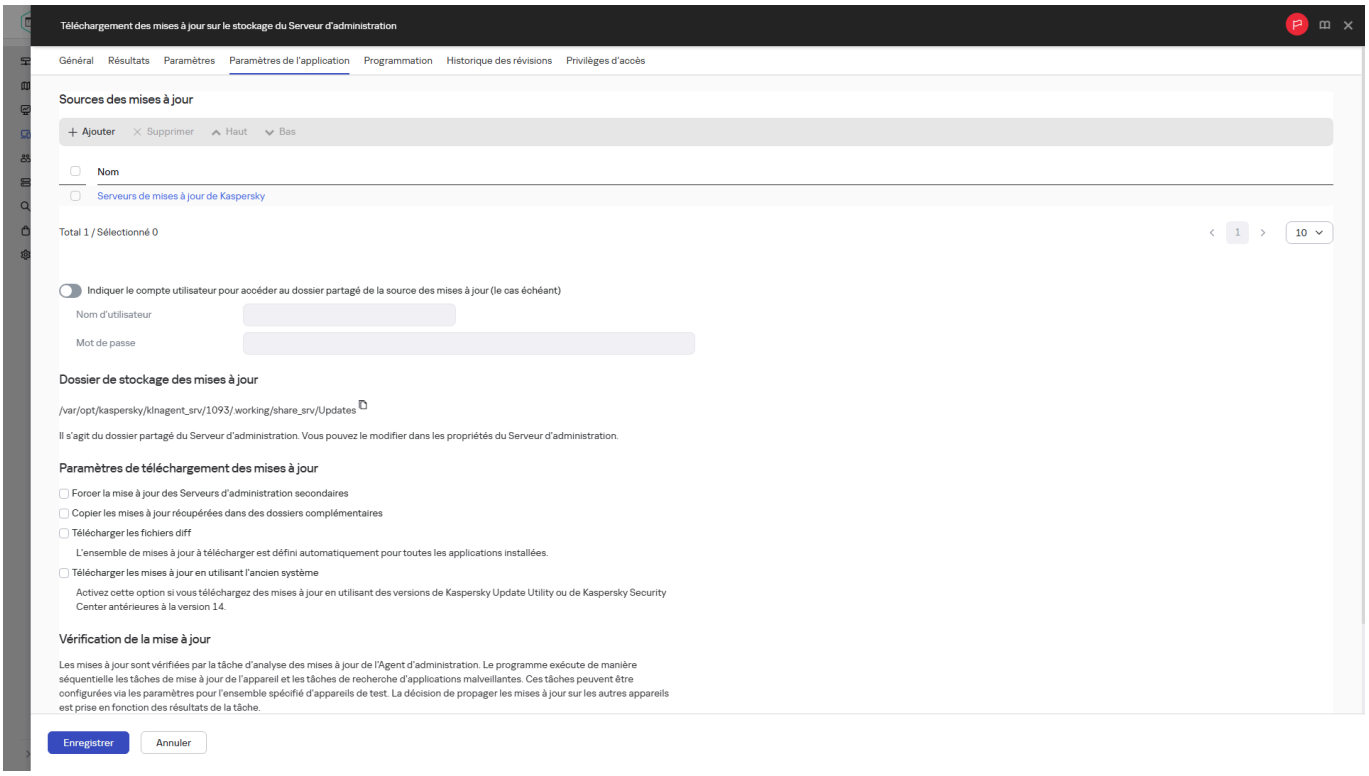
Assurez-vous que l'option **Télécharger les mises à jour en utilisant l'ancien système** est désactivée.

De plus, le téléchargement de la mise à jour dans Kaspersky Update Utility doit être configuré.

Par défaut, le chemin suivant est indiqué : /var/opt/kaspersky/klnagent_srv/1093/.working/share_srv/retranslation_request.xml. Si nécessaire, vous pouvez modifier le nom par défaut (retranslation_request) et le chemin.

> Le fichier de demande peut être placé dans un dossier local ou partagé. Lorsque vous utilisez un dossier partagé, vous devez garantir l'accès à ce dossier depuis 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'exécution de la tâche *Télécharger les mises à jour dans le répertoire du Serveur d'administration*, Kaspersky Security Center Linux crée le fichier de demande de mise à jour au format .xml au niveau du chemin que vous avez indiqué. Kaspersky Update Utility obtient automatiquement les informations du fichier de demande, puis télécharge uniquement les mises à jour requises. Si Kaspersky Update Utility ne parvient pas à obtenir les informations automatiquement (par exemple, Kaspersky Update Utility n'a pas accès au dossier dans lequel Kaspersky Security Center Linux a créé le fichier de demande), vous devez transmettre le fichier à l'aide d'outils tiers.



Spécification des propriétés de la tâche Téléchargement des mises à jour dans le stockage du Serveur d'administration

9. Dans la fenêtre des propriétés de la tâche, onglet **Programmation**, créez une planification pour le démarrage de la tâche. Le cas échéant, configurez les paramètres suivants :

- **Démarrer la tâche** :

  - **Mode 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.

- **Selon les jours de la semaine**

  La tâche s'exécute régulièrement les jours définis de la semaine, à l'heure indiquée.

  Par défaut, la tâche s'exécute chaque vendredi à 18h00.

- **Chaque mois**

  La tâche s'exécute régulièrement le jour du mois défini, à l'heure indiquée.

  Si le jour en question ne figure pas dans le mois, la tâche s'exécute le dernier jour.

  La tâche s'exécute par défaut le premier jour de chaque mois, à l'heure système actuelle.

- **Chaque mois, un jour de semaine donné**

  La tâche s'exécute régulièrement les jours du mois définis, à l'heure indiquée.

  Par défaut, l'heure de début est 18:00 et aucun jour du mois n'est sélectionné.

  Notez que vous ne sélectionnez ni une date précise dans le mois, ni le numéro de la semaine (première, deuxième semaine du mois) mais le numéro d'ordre du jour de la semaine à l'intérieur d'un mois. Par exemple, si vous placez le curseur dans la cellule **Ma** de la ligne **Premier**, cela signifie que la tâche sera exécutée tous les premiers mardis de chaque nouveau mois.

  Vous pouvez sélectionner plusieurs jours de la semaine.

- **À la fin d'une autre tâche**

  La tâche actuelle démarre à la fin d'une autre tâche. Cette option ne fonctionne que si les deux tâches sont affectées aux mêmes appareils. Par exemple, vous pouvez exécuter la tâche *Administration des appareils* avec l'option **&Activer l'appareil** et, une fois celle-ci terminée, exécuter la tâche de *recherche de virus* comme tâche de déclenchement.

  Il faut sélectionner la tâche de déclenchement dans le tableau et l'état avec lequel cette tâche doit se terminer (**Terminée avec succès** ou **Échec**).

  Si nécessaire, vous pouvez rechercher, trier et filtrer les tâches dans le tableau comme suit :

  - Saisissez le nom de la tâche dans le champ de recherche pour rechercher une tâche par son nom.
  - Cliquez sur l'icône de tri pour trier les tâches par nom.

    Par défaut, les tâches sont triées par ordre alphabétique croissant.
  - Cliquez sur l'icône du filtre, et dans la fenêtre qui s'ouvre, filtrez les tâches par groupe, puis cliquez sur le bouton **Appliquer**.

- 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 et automatiquement le lancement de la tâche dans un intervalle de**

    Si cette option est activée, la tâche est lancée sur les appareils clients de manière aléatoire au cours de l'intervalle défini. Un lancement échelonné de tâche permet d'éviter la communication simultanée d'un nombre important d'appareils clients avec le Serveur d'administration lors du lancement de la tâche programmée.

    Si la case n'est pas cochée, le lancement de la tâche sur les appareils clients s'opère selon la planification.

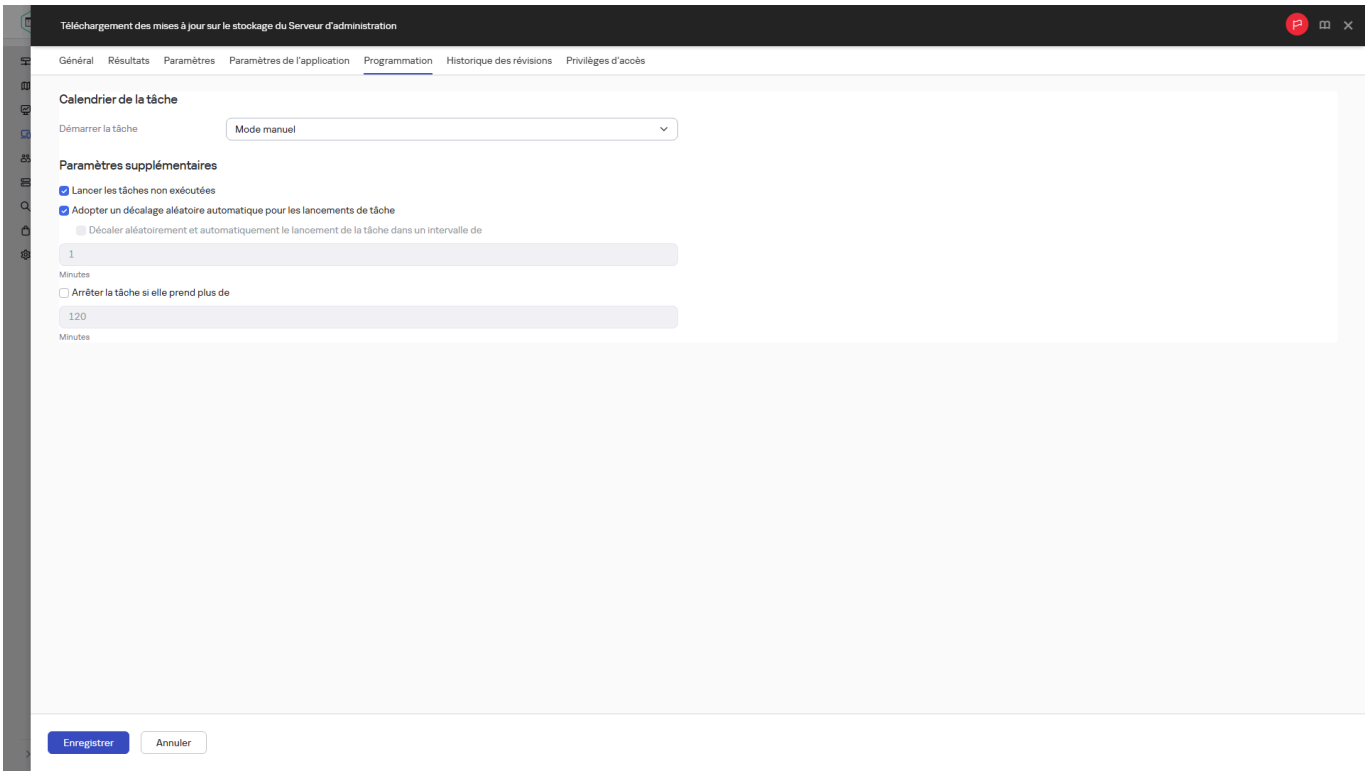
    Cette option est Inactif par défaut. Par défaut, la valeur de cet intervalle est de une minute.

  - **Arrêter la tâche si elle prend plus de**

    A l'issue du délai défini, la tâche s'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.

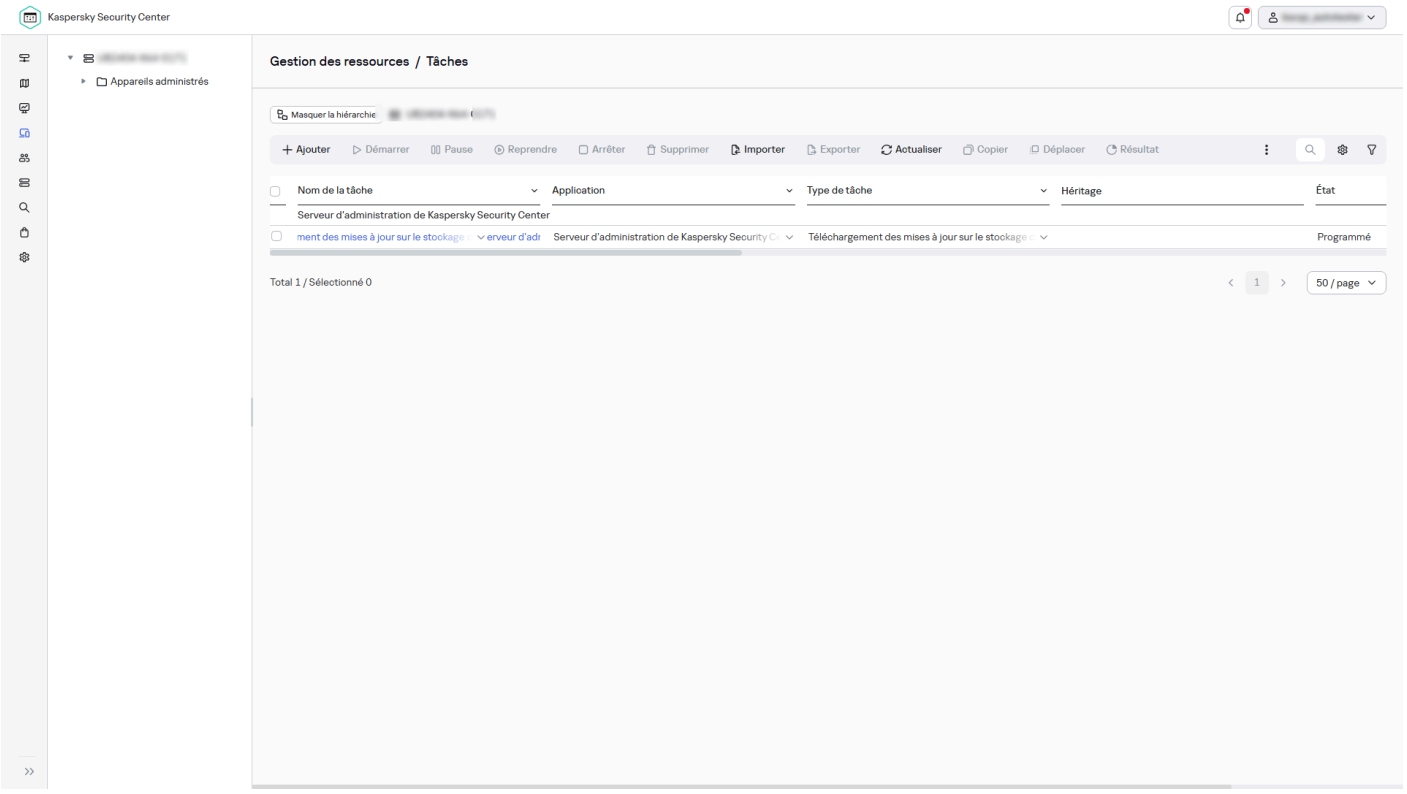
    Cette option est Inactif par défaut. La durée d'exécution de la tâche par défaut est de 120 minutes.



Spécification de la planification de la tâche Téléchargement des mises à jour dans le stockage du Serveur d'administration

10. Cliquez sur le bouton **Enregistrer**.

La tâche est créée et configurée.



La liste des tâches

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 sur les stockages** 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.

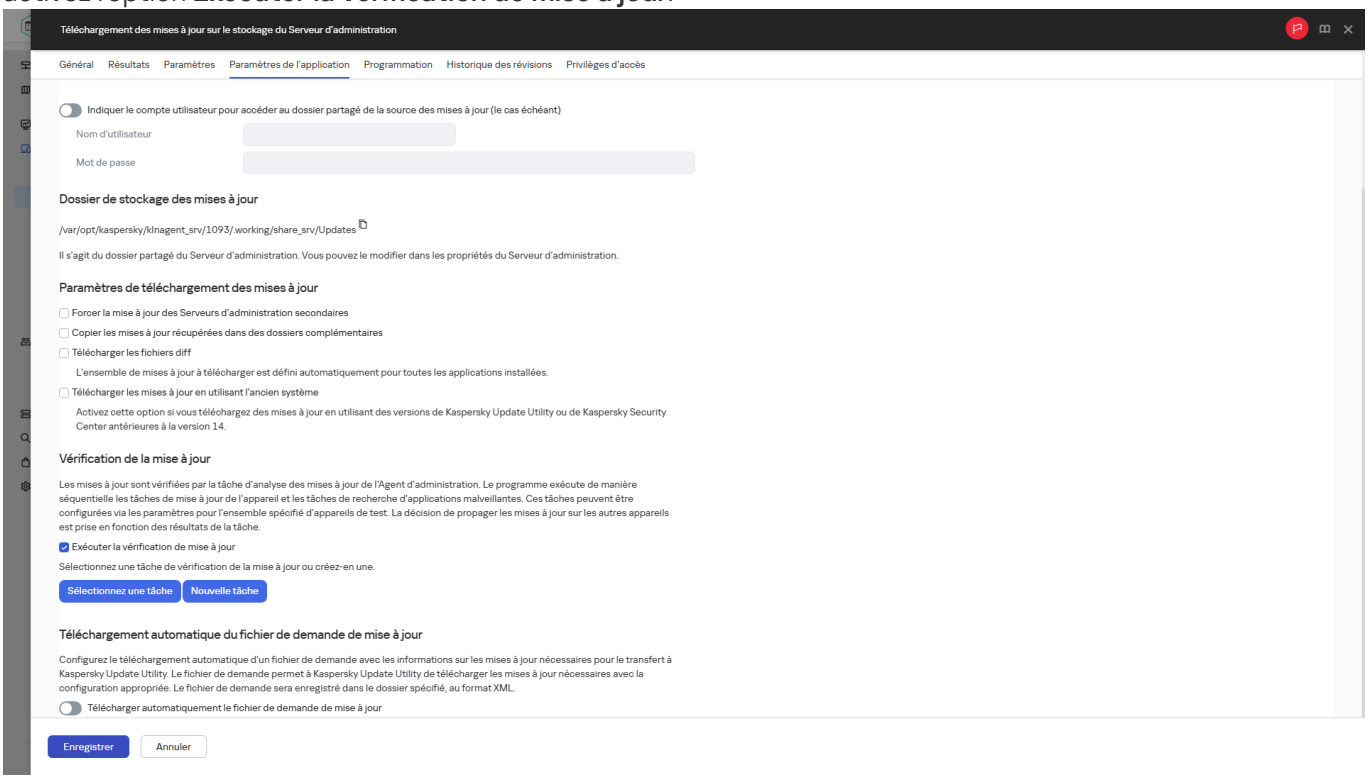
3. Créez la tâche *Téléchargement des mises à jour sur le stockage du Serveur d'administration*.

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 **Gestion des ressources** → **Tâches**.

2. Cliquez sur la tâche **Téléchargement des mises à jour sur le stockage du Serveur d'administration**.

3. Dans la fenêtre des propriétés de la tâche qui s'ouvre, accédez à l'onglet **Paramètres de l'application**, puis activez l'option **Exécuter la vérification de mise à jour**.



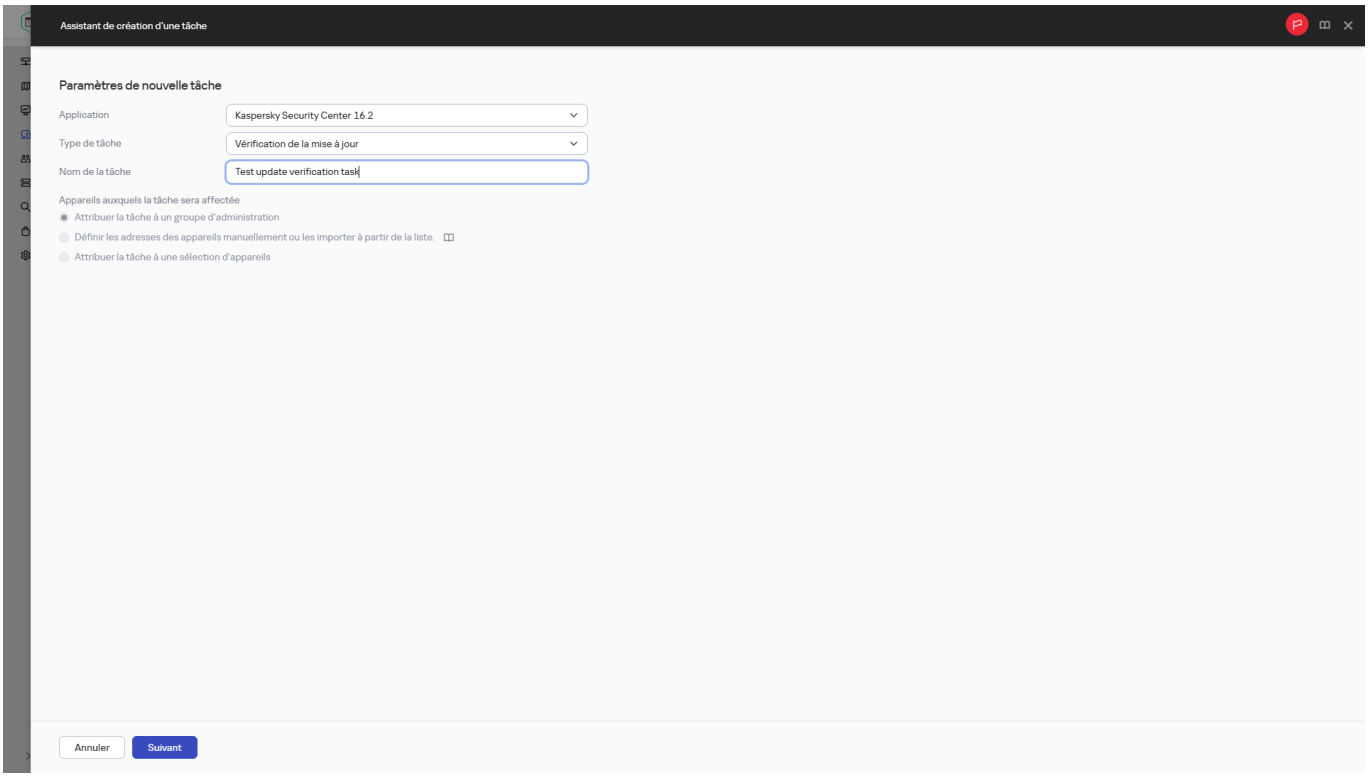
Propriétés de la tâche Téléchargement des mises à jour sur le stockage du Serveur d'administration

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**.

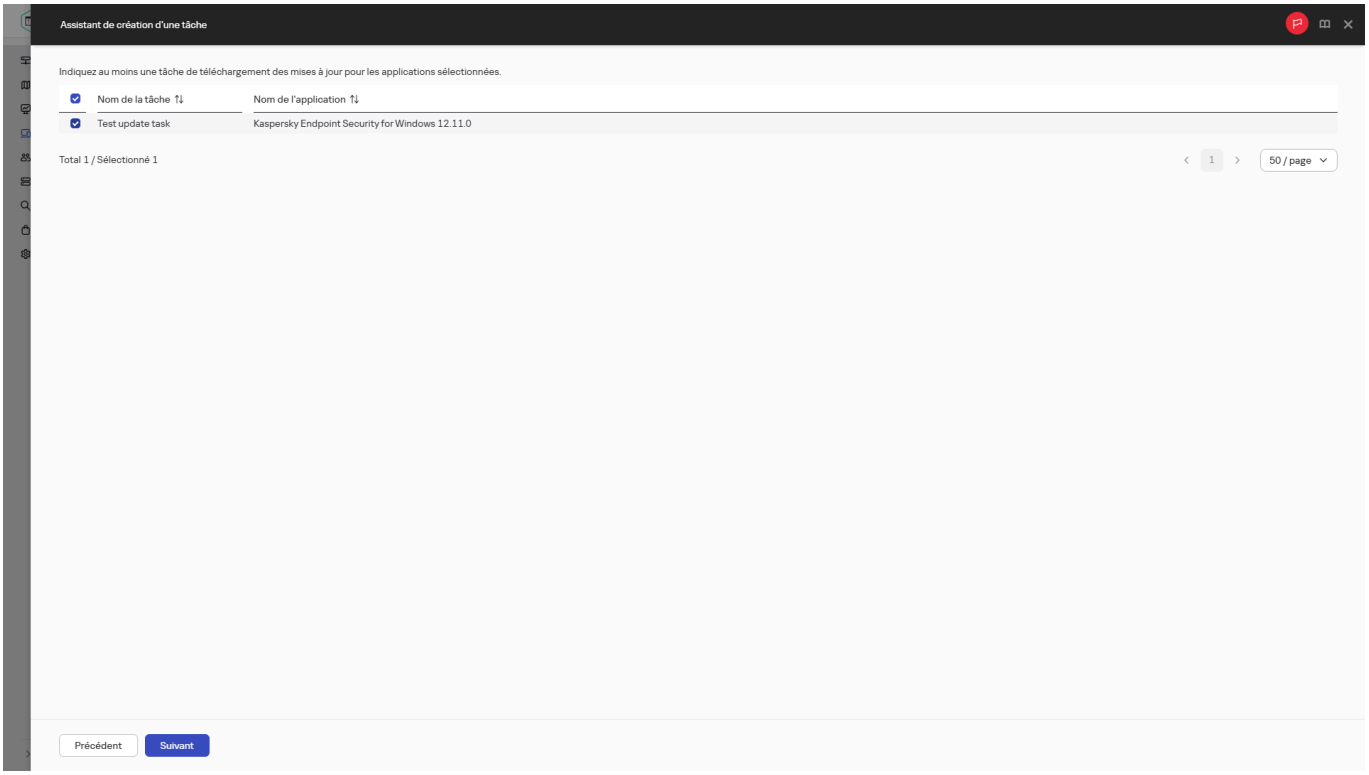
   b. Dans l'Assistant de création d'une tâche qui s'ouvre, indiquez le nom de la tâche si vous souhaitez modifier le nom prédéfini.



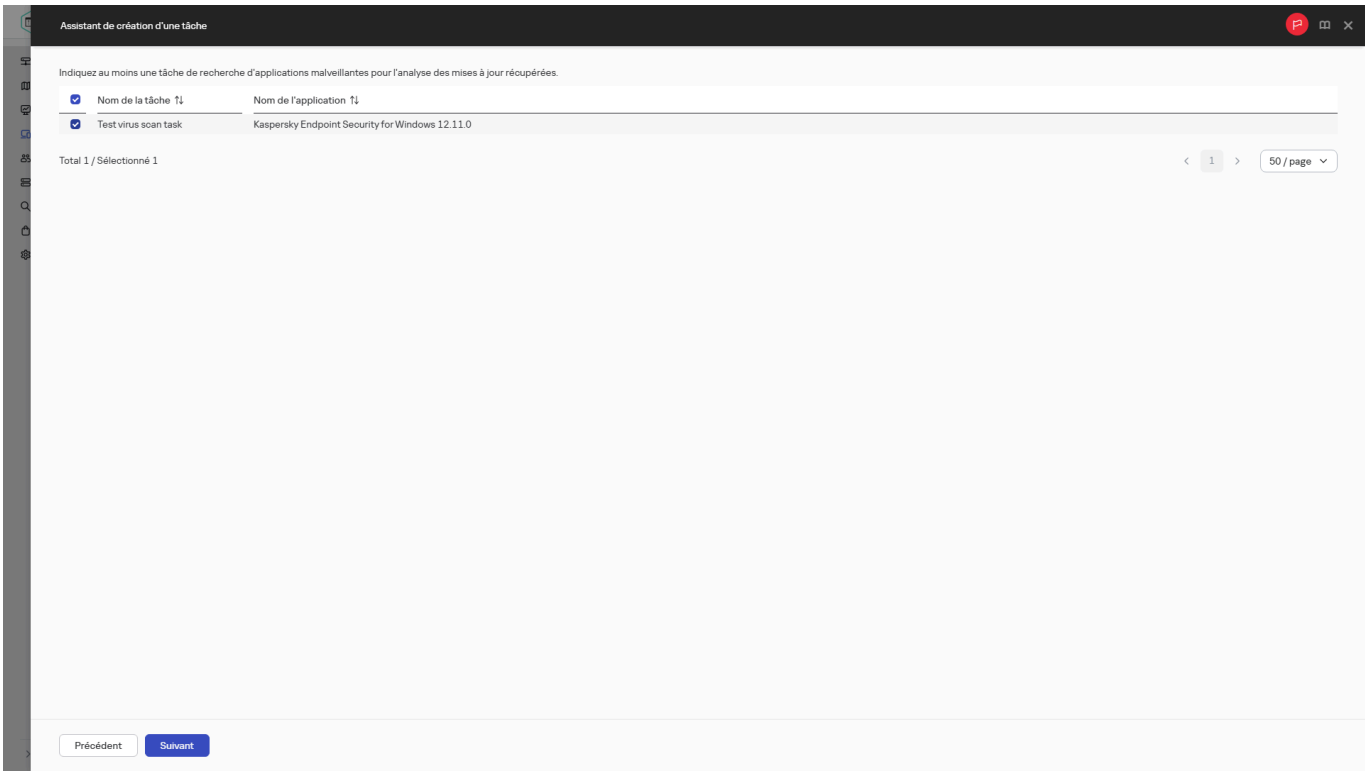
Création d'une tâche d'analyse des mises à jour

   a. Sélectionnez le groupe d'administration avec les appareils de test que vous avez créé précédemment.

   b. Sélectionnez la tâche de mise à jour de l'application requise pris en charge par Kaspersky Security Center Linux.



a. Sélectionnez la tâche d'analyse des logiciels malveillants de l'application requise prise en charge par Kaspersky Security Center Linux.



Sélection de la tâche d'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**

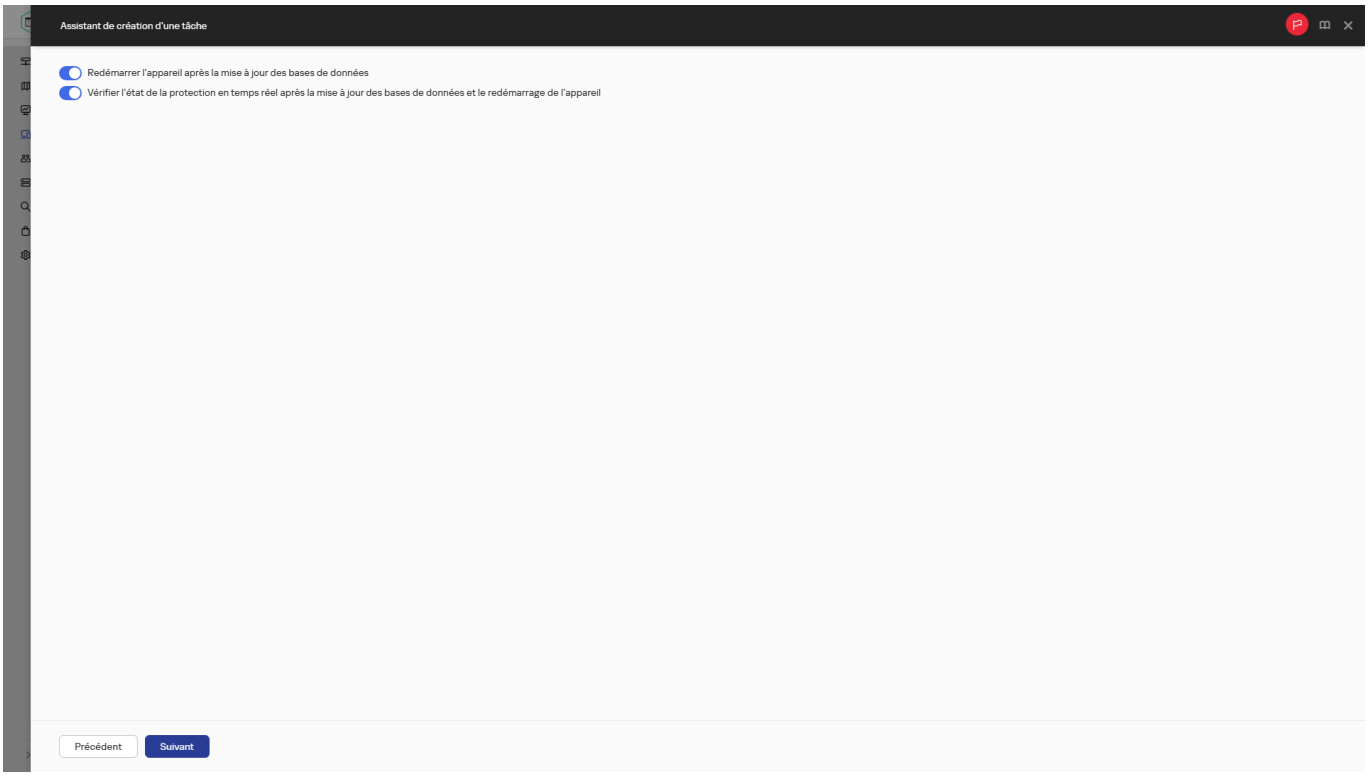
  Une fois que les bases de données antivirus sont mises à jour sur un appareil, nous vous recommandons de redémarrer l'appareil.

  Cette 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.



Spécification des paramètres de la tâche

a. Indiquez un compte à partir duquel la tâche de *vérification des mises à jour* sera exécutée. 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.

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.

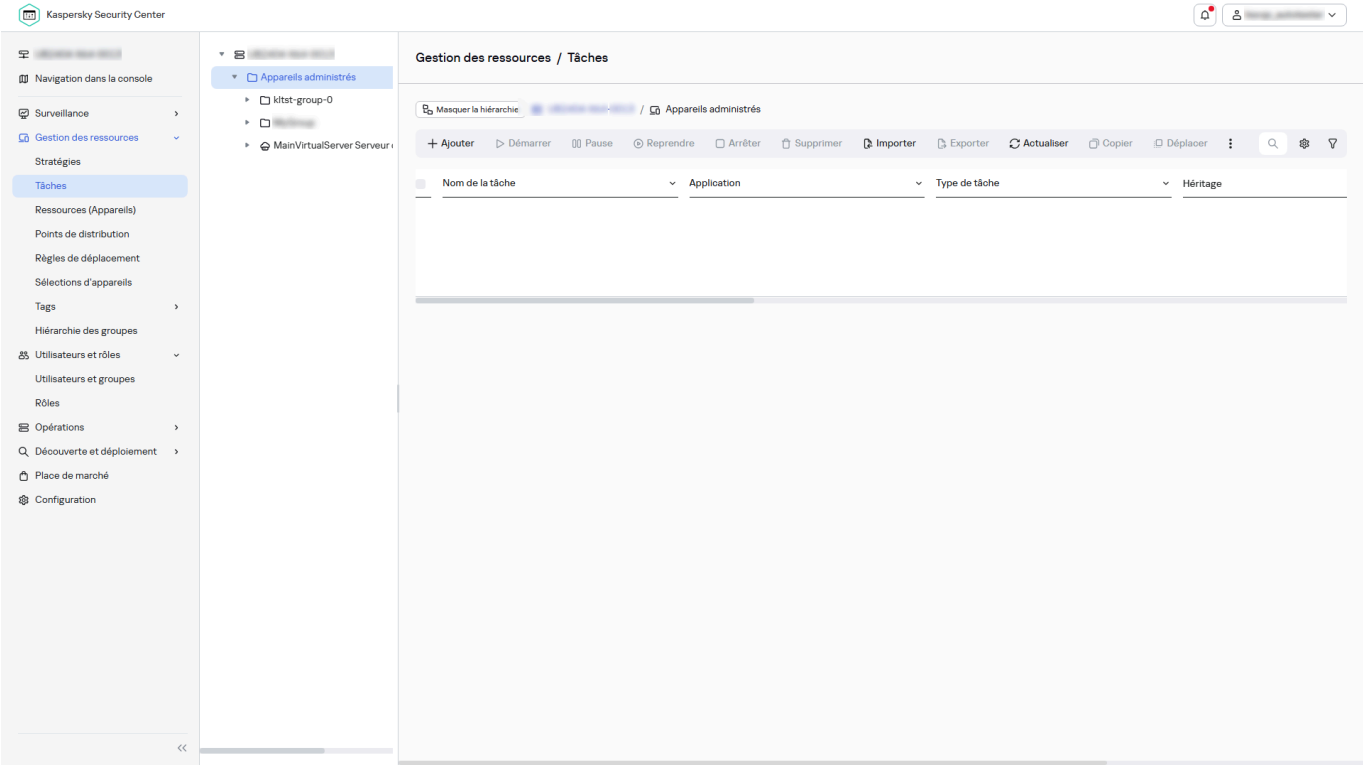
Cette tâche est nécessaire pour télécharger les mises à jour des serveurs de mise à jour de Kaspersky dans les stockages des points de distribution. La liste de mises à jour inclut les éléments suivants :

- 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 **Gestion des ressources** → **Tâches**.



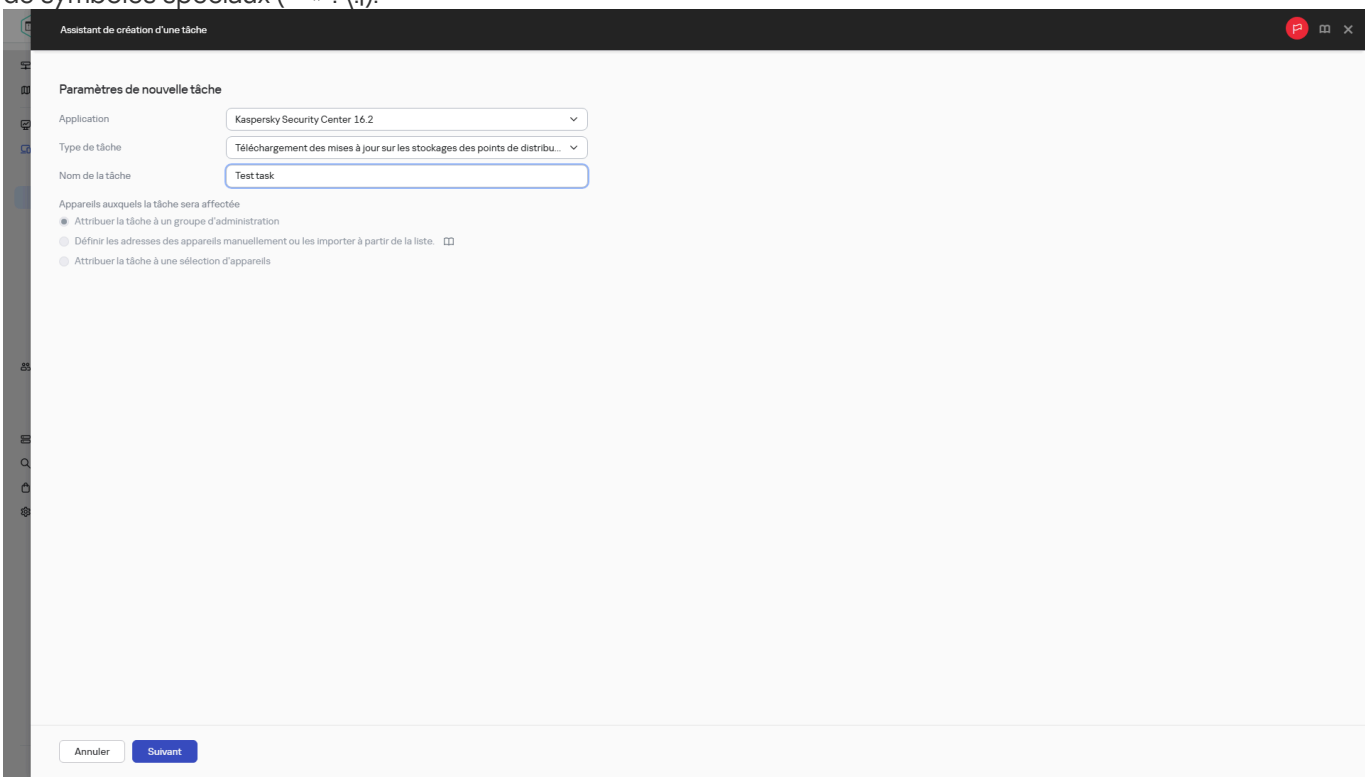
La section Tâches

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, 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 ("*<>?\:|).



Création de la tâche de Téléchargement des mises à jour sur les stockages des points de distribution

5. Sélectionnez un bouton d'option pour spécifier le groupe d'administration, la sélection d'appareils ou les appareils auxquels la tâche s'applique.

6. À l'étape **Fin de la création de la tâche**, si vous souhaitez modifier les paramètres de tâche par défaut, activez l'option **Ouvrir les détails de la tâche à la fin de la création**. Si vous n'activez pas cette tâche, la tâche est créée selon les paramètres par défaut. Vous pourrez modifier ces paramètres par défaut plus tard, à tout moment.

7. Cliquez sur le bouton **Créer**.

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

8. Cliquez sur le nom de la tâche créée pour ouvrir la fenêtre de propriétés de la tâche.

9. Dans l'onglet **Paramètres de l'application** de la fenêtre des propriétés de la tâche, spécifiez les paramètres suivants :

   - **Sources des mises à jour**

     Les ressources suivantes peuvent faire office de source des mises à jour pour le point de distribution :

     - Serveurs de mise à jour de Kaspersky

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

       Par défaut, cette option est sélectionnée.

     - Dossier local ou réseau

       Un dossier local ou de réseau qui contient les mises à jour les plus récentes. 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 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 :

- **Démarrer la tâche** :
  - **Mode 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.

  - **Selon les jours de la semaine**

    La tâche s'exécute régulièrement les jours définis de la semaine, à l'heure indiquée.

    Par défaut, la tâche s'exécute chaque vendredi à 18h00.

  - **Chaque mois**

    La tâche s'exécute régulièrement le jour du mois défini, à l'heure indiquée.

    Si le jour en question ne figure pas dans le mois, la tâche s'exécute le dernier jour.

    La tâche s'exécute par défaut le premier jour de chaque mois, à l'heure système actuelle.

  - **Chaque mois, un jour de semaine donné**

    La tâche s'exécute régulièrement les jours du mois définis, à l'heure indiquée.

Par défaut, l'heure de début est 18:00 et aucun jour du mois n'est sélectionné.

Notez que vous ne sélectionnez ni une date précise dans le mois, ni le numéro de la semaine (première, deuxième semaine du mois) mais le numéro d'ordre du jour de la semaine à l'intérieur d'un mois. Par exemple, si vous placez le curseur dans la cellule **Ma** de la ligne **Premier**, cela signifie que la tâche sera exécutée tous les premiers mardis de chaque nouveau mois.

Vous pouvez sélectionner plusieurs jours de la semaine.

- **Lors de la détection d'une propagation de virus**

  La tâche s'exécute après un événement *Propagation de virus* de virus. Sélectionnez les types d'application qui vont surveiller les propagations de virus. Les types suivants de Application sont présent :

  - Antivirus pour postes de travail et serveurs de fichiers
  - Antivirus de protection du périmètre
  - Antivirus pour systèmes de messagerie

  Tous les types d'application sont cochés par défaut.

  Il se peut que vous souhaitiez exécuter différentes tâches en fonction du type d'application de sécurité qui signale une propagation de virus. Dans ce cas, supprimez la sélection des types d'application dont vous n'avez pas besoin.

- **À la fin d'une autre tâche**

  La tâche actuelle démarre à la fin d'une autre tâche. Cette option ne fonctionne que si les deux tâches sont affectées aux mêmes appareils. Par exemple, vous pouvez exécuter la tâche *Administration des appareils* avec l'option **&Activer l'appareil** et, une fois celle-ci terminée, exécuter la tâche de *recherche de virus* comme tâche de déclenchement.

  Il faut sélectionner la tâche de déclenchement dans le tableau et l'état avec lequel cette tâche doit se terminer (**Terminée avec succès** ou **Échec**).

  Si nécessaire, vous pouvez rechercher, trier et filtrer les tâches dans le tableau comme suit :

  - Saisissez le nom de la tâche dans le champ de recherche pour rechercher une tâche par son nom.
  - Cliquez sur l'icône de tri pour trier les tâches par nom.

    Par défaut, les tâches sont triées par ordre alphabétique croissant.
  - Cliquez sur l'icône du filtre, et dans la fenêtre qui s'ouvre, filtrez les tâches par groupe, puis cliquez sur le bouton **Appliquer**.

- **Lancer les tâches non exécutées**

  Cette option détermine le comportement d'une tâche si un appareil client n'est pas visible sur le réseau quand la tâche est sur le point de démarrer.

Si la case est Activé, lors du lancement suivant de l'application de Kaspersky sur cet appareil client, une tentative de lancement de la tâche sera faite. Si la programmation de la tâche est **Manuel**, **Une fois** ou **Immédiatement**, la tâche est immédiatement lancée dès que l'appareil apparaît sur le réseau ou immédiatement après l'inclusion de l'appareil dans la zone d'action de la tâche.

Si cette option est désactivée, seules les tâches planifiées s'exécutent sur les appareils clients. Pour les planifications **Manuel**, **Une fois** et **Immédiatement**, les tâches s'exécutent uniquement sur les appareils clients qui sont visibles sur le réseau. Par exemple, vous pouvez désactiver cette option pour une tâche qui consomme des ressources que vous voulez exécuter uniquement en dehors des heures de bureau.

Cette option est Inactif par défaut.

- **Adopter un décalage aléatoire automatique pour les lancements de tâche**

  Si cette option est activée, la tâche est lancée sur les appareils clients de manière aléatoire au cours d'un intervalle défini. C'est ce qu'on appelle un *lancement échelonné d'une tâche*. Un lancement échelonné de tâche permet d'éviter la communication simultanée d'un nombre important d'appareils clients avec le Serveur d'administration lors du lancement de la tâche programmée.

  Le temps du lancement aléatoire est automatiquement calculée lors de la création d'une tâche selon le nombre d'appareils clients sur lesquels la tâche est diffusée. Par la suite, la tâche démarre toujours à l'heure de lancement calculée. Toutefois, quand les paramètres de la tâche sont modifiés ou si la tâche est lancée manuellement, la valeur calculée de l'heure de lancement de la tâche est modifiée.

  Si la case n'est pas cochée, le lancement de la tâche sur les appareils clients s'opère selon la planification.

- **Décaler aléatoirement et automatiquement le lancement de la tâche dans un intervalle de**

  Si cette option est activée, la tâche est lancée sur les appareils clients de manière aléatoire au cours de l'intervalle défini. Un lancement échelonné de tâche permet d'éviter la communication simultanée d'un nombre important d'appareils clients avec le Serveur d'administration lors du lancement de la tâche programmée.

  Si la case n'est pas cochée, le lancement de la tâche sur les appareils clients s'opère selon la planification.

  Cette option est Inactif par défaut. Par défaut, la valeur de cet intervalle est de une minute.

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 informations d'identification.

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.

Lors de la sélection du dossier local, il faut indiquer le dossier sur l'appareil avec le Serveur d'administration installé. Le chemin d'accès au dossier dépend du système d'exploitation de l'appareil. Étant donné que le dossier local se trouve sur un Serveur d'administration basé sur Linux, vous devez préciser le chemin d'accès POSIX, par exemple : /path/to/dir.

Seul un partage SMB monté peut être utilisé en tant que dossier réseau. 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.

Pour ajouter les sources de mises à jour :

1. Dans le menu principal, accédez à **Gestion des ressources** → **Tâches**.
2. Cliquez sur **Téléchargement des mises à jour sur le stockage du Serveur d'administration**.
3. Accédez à l'onglet **Paramètres de l'application**.
4. Dans le tableau **Sources des mises à jour**, cliquez sur le bouton **Ajouter**.

5. Dans la fenêtre qui s'ouvre, ajoutez les sources nécessaires, puis cliquez sur le bouton **Enregistrer**.

   Si vous cochez la case **Dossier local ou réseau**, indiquez un chemin d'accès au dossier.

6. 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.

Si vous ajoutez à la fois les serveurs de mise à jour de Kaspersky et le dossier local ou réseau, vous pouvez définir la priorité des mises à jour. Pour cela, dans le tableau **Sources des mises à jour**, cochez la case en regard de la mise à jour dont vous souhaitez modifier la priorité, puis cliquez sur le bouton **Haut** ou **Bas**.

Approbation et refus des mises à jour du logiciel

Les paramètres d'une tâche d'installation de mise à jour peuvent nécessiter l'approbation des mises à jour à installer. Vous pouvez approuver les mises à jour à installer et refuser les mises à jour qui ne doivent pas installer.

Par exemple, vous souhaitez d'abord vérifier l'installation des mises à jour dans un environnement d'essai et vous assurer qu'elles ne perturbent pas le fonctionnement des appareils avant d'autoriser l'installation de ces mises à jour sur les appareils clients.

> L'approbation et le refus de mises à jour est disponible uniquement pour l'Agent d'administration et les applications administrées installées sur les appareils clients Windows. La mise à jour transparente du Serveur d'administration, de Kaspersky Security Center Web Console et des plug-ins Web d'administration n'est pas prise en charge. Pour mettre à jour ces modules, vous devez télécharger les dernières versions à partir du site Internet de Kaspersky, puis les installer manuellement.

Pour approuver ou refuser une ou plusieurs mises à jour :

1. Dans le menu principal, accédez à **Opérations** → **Applications Kaspersky** → **Mises à jour transparentes**.

   Une liste des mises à jour disponibles s'affiche.

   > Les mises à jour des applications administrées peuvent nécessiter l'installation d'une version minimale spécifique de Kaspersky Security Center. Si cette version est postérieure à votre version actuelle, ces mises à jour sont affichées mais ne peuvent pas être approuvées. De plus, aucun paquet d'installation ne peut être créé à partir de ces mises à jour tant que vous n'avez pas mis à niveau Kaspersky Security Center. Vous êtes invité à mettre à niveau votre instance de Kaspersky Security Center vers la version minimale requise.

2. Le cas échéant, acceptez le CLUF en cliquant sur le bouton **Consulter et accepter les Contrats de licence utilisateur final**.

3. Sélectionnez les mises à jour que vous souhaitez approuver ou refuser.

4. Cliquez sur **Approuver** pour approuver les mises à jour sélectionnées ou sur **Refuser** pour les refuser.

   Par défaut, la valeur *Non défini* est cochée.

Les mises à jour auxquelles vous attribuez l'état *Approuvée* sont placées dans une file d'attente d'installation.

Les mises à jour auxquelles vous attribuez l'état *Rejetée* sont supprimées (si possible) de tous les appareils sur lesquels elles avaient été installées. Et elles ne seront installées sur aucun autre appareil à l'avenir.

Il est impossible de désinstaller certaines mises à jour pour les applications de Kaspersky. Si vous leur attribuez l'état *Rejetée*, Kaspersky Security Center Linux ne les supprime pas des appareils sur lesquels elles avaient été installées. Toutefois, ces mises à jour ne seront jamais installées sur d'autres appareils à l'avenir.

Si vous attribuez l'état *Rejetée* aux mises à jour du logiciel tiers, ces mises à jour ne sont pas installées sur les appareils où elles ont été planifiées mais pas encore installées. Les mises à jour seront conservées sur les appareils où elles ont déjà été installées. Si vous devez supprimer les mises à jour, vous pouvez le faire manuellement en local.

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 **Gestion des ressources** → **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 Endpoint Security for Windows, sélectionnez **Mise à jour** comme sous-type de tâche.
4. Spécifiez le nom de la tâche créée. Le nom de la tâche ne peut pas contenir plus de 100 symboles et contenir de symboles spéciaux ("*<>?\:|).
5. Choisissez la zone d'action de la tâche.
6. Spécifiez le groupe d'administration, la sélection d'appareils ou les appareils auxquels la tâche s'applique.
7. À l'étape **Fin de la création de la tâche**, si vous souhaitez modifier les paramètres de tâche par défaut, activez l'option **Ouvrir les détails de la tâche à la fin de la création**. Si vous n'activez pas cette tâche, la tâche est créée selon les paramètres par défaut. Vous pourrez modifier ces paramètres par défaut plus tard, à tout moment.
8. Cliquez sur le bouton **Créer**.

   La tâche est créée et s'affiche dans la liste des tâches.
9. Cliquez sur le nom de la tâche créée pour ouvrir la fenêtre de propriétés de la tâche.

10. Dans l'onglet **Paramètres de l'application** des propriétés de la tâche, définissez les paramètres de la tâche de mise à jour en mode local ou mobile :

    - **Mode local** : la connexion est établie entre l'appareil et le Serveur d'administration.

    - **Mode mobile** : la connexion n'est pas établie entre l'appareil et Kaspersky Security Center 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 le nom du Serveur d'administration.

   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 la source des mises à jour pour le point de distribution :

     - Pour que le point de distribution récupère les mises à jour du Serveur d'administration, sélectionnez **Récupérer depuis le Serveur d'administration**.

     - Pour autoriser le point de distribution à recevoir les mises à jour à l'aide d'une tâche, sélectionnez **Utiliser la tâche d'obtention des mises à jour** de téléchargement des mises à jour, puis spécifiez une tâche *Télécharger les mises à jour dans les référentiels des points de distribution* :

       - Si une telle tâche existe déjà sur l'appareil, sélectionnez-la dans la liste.

       - Si aucune tâche de ce type n'existe encore sur l'appareil, cliquez sur le lien **Créer la tâche** pour créer une tâche. Ceci permet de lancer l'Assistant de création d'une tâche. Suivez les étapes 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 Internet 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 dans la section **Sauvegardes des plug-ins Internet**.

Pour restaurer un plug-in Web à partir d'une sauvegarde :

1. Dans le menu principal, accédez à la section **Paramètres** → **Sauvegardes des plug-ins Internet**.

2. Dans la section **Sauvegardes des plug-ins Internet**, 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 sur les 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.

Déclenchement des règles en mode Apprentissage intelligent

Cette section fournit des informations relatives aux détections réalisées par les règles du contrôle évolutif des anomalies dans Kaspersky Endpoint Security for Windows sur les appareils clients.

Les règles détectent le comportement anormal sur les appareils clients et peuvent le bloquer. Si les règles fonctionnent en mode Apprentissage intelligent, elles détectent tout comportement anormal et envoient des rapports sur chaque cas au Serveur d'administration. Vous pouvez consulter les rapports sur les comportements anormaux détectés dans la section **Opérations → Stockages → Déclenchements de règles dans le mode Apprentissage intelligent**. Vous pouvez confirmer les détections comme étant correctes ou les ajouter en tant qu'exclusions afin que ce type de comportement ne soit plus considéré comme une anomalie.

Les informations relatives aux détections sont stockées dans le journal des événements sur le Serveur d'administration (avec les autres événements) et dans le rapport Contrôle évolutif des anomalies.

Pour en savoir plus sur le Contrôle évolutif des anomalies, les règles, leur mode et les états, consultez l'aide de Kaspersky Endpoint Security for Windows.

Consultation et confirmation des détections réalisées à l'aide des règles du Contrôle évolutif des anomalies

Pour consulter la liste des détections réalisées à l'aide des règles du contrôle évolutif des anomalies, procédez comme suit :

1. Dans le menu principal, accédez à **Opérations → Stockages → Déclenchements de règles dans le mode Apprentissage intelligent**.

   La liste affiche les informations suivantes relatives aux détections réalisées à l'aide des règles du contrôle évolutif des anomalies :

   - **Groupe d'administration**

     Le nom du groupe d'administration dont l'appareil fait partie.

   - **Serveur d'administration virtuel**

     Serveur d'administration virtuel qui gère l'appareil.

- **Nom de l'appareil**

  Le nom de l'appareil client sur lequel la règle a été appliquée.

- **Nom**

  Le nom de la règle qui a été appliquée.

- **État**

  Exclusion en cours : si l'Administrateur a traité cet élément et l'a ajouté en tant qu'exclusion aux règles. Cet état se maintient jusqu'à la synchronisation suivante de l'appareil client avec le Serveur d'administration après la synchronisation, l'appareil disparaît de la liste.

  Confirmation en cours : si l'administrateur a traité cet élément et l'a confirmé. Cet état se maintient jusqu'à la synchronisation suivante de l'appareil client avec le Serveur d'administration après la synchronisation, l'appareil disparaît de la liste.

  Vide : si l'administrateur n'a pas traité cet élément.

- **Nombre de détections**

  Le nombre de détections au sein d'une règle heuristique, un processus et un appareil client. Cette quantité est calculée par Kaspersky Endpoint Security.

- **Nom d'utilisateur**

  Le nom de l'utilisateur de l'appareil client qui exécute le processus qui a généré la détection.

- **Chemin du processus source**

  Chemin d'accès au processus source, à savoir au processus qui réalise l'action (pour en savoir plus, consultez l'aide de Kaspersky Endpoint Security).

- **Hash du processus source**

  Hash SHA256 du fichier du processus source (pour en savoir plus, consultez l'aide de Kaspersky Endpoint Security).

- **Chemin d'accès à l'objet source**

  Chemin d'accès à l'objet qui a lancé le processus (pour en savoir plus, consultez l'aide de Kaspersky Endpoint Security).

- **Hash de l'objet source**

  Hash SHA256 du fichier de base (pour en savoir plus, consultez l'aide de Kaspersky Endpoint Security).

- **Chemin du processus cible**

  Chemin d'accès au processus cible (pour en savoir plus, consultez l'aide de Kaspersky Endpoint Security).

- **Hash du processus cible**

  Hash SHA256 du fichier cible (pour en savoir plus, consultez l'aide de Kaspersky Endpoint Security).

- **Chemin d'accès à l'objet cible**

  Chemin d'accès à l'objet cible (pour en savoir plus, consultez l'aide de Kaspersky Endpoint Security).

- **Hash de l'objet cible**

  Hash SHA256 du fichier cible (pour en savoir plus, consultez l'aide de Kaspersky Endpoint Security).

- **Traité**

  Date de détection de l'anomalie.

Pour consulter les propriétés d'une détection :

1. Dans le menu principal, accédez à **Opérations** → **Stockages** → **Déclenchements de règles dans le mode Apprentissage intelligent**.

2. Exécutez une des actions suivantes :

   - Dans la colonne **Nom**, cliquez sur le lien portant le nom de la détection que vous souhaitez afficher.

   - Dans la liste des détections, cochez les cases en regard des détections que vous souhaitez corriger, puis cliquez sur le bouton **Propriétés**.

   La fenêtre des propriétés de la détection sélectionnée s'ouvre, affichant des informations la concernant.

Vous pouvez confirmer toute détection à partir de la liste des détections des règles du Contrôle évolutif des anomalies ou à partir de la fenêtre des propriétés d'une détection sélectionnée.

Pour confirmer une détection :

- Sélectionnez un (ou plusieurs éléments) dans la liste des détections, puis cliquez sur le bouton **Confirmer**.

- Ouvrez la fenêtre des propriétés d'une détection sélectionnée, puis cliquez sur le bouton **Confirmer**.

  L'état de la ou des détections devient **Confirmation en cours**. La détection disparaît de la liste des détections après la prochaine synchronisation de l'appareil client avec le Serveur d'administration.

  Votre confirmation contribuera aux statistiques utilisées par les règles. Pour en savoir plus, consultez l'aide de Kaspersky Endpoint Security for Windows.

Ajout d'exclusions au départ des règles du contrôle évolutif des anomalies

L'Assistant d'ajout aux exclusions du Contrôle évolutif des anomalies permet d'ajouter des exclusions au départ des règles du contrôle évolutif des anomalies pour Kaspersky Endpoint Security.

Pour ajouter des exclusions à partir des règles du Contrôle évolutif des anomalies à l'aide de l'assistant, procédez comme suit :

1. Lancez l'assistant des fichiers d'une des façons suivantes :

   - Dans le menu principal, accédez à **Opérations** → **Stockages** → **Déclenchements de règles dans le mode Apprentissage intelligent**, sélectionnez une ou plusieurs détections, puis cliquez sur le bouton **Exclure**.

     Vous pouvez ajouter un maximum de 1 000 exclusions en une fois.

     Avant d'ajouter une détection aux exclusions, vous pouvez consulter les propriétés de la détection en cliquant sur le nom de la détection ou sur le bouton **Propriétés**. Dans la fenêtre des propriétés de détection qui s'ouvre, vous pouvez également cliquer sur le bouton **Exclure**.

   - Dans le menu principal, accédez à **Surveillance** → **Sélections d'événements**, cliquez sur le lien avec la sélection d'événements dont vous avez besoin, cochez la case en regard de la détection que vous souhaitez exclure, puis cliquez sur le bouton **Exclure du Contrôle évolutif des anomalies**.

   L'Assistant d'ajout aux exclusions du Contrôle évolutif des anomalies démarre. Naviguez dans les fenêtres de l'Assistant à l'aide du bouton **Suivant**.

2. Sélectionnez les stratégies et les profils que vous souhaitez ajouter aux exclusions.

   Il est impossible de mettre à jour les stratégies héritées. Si vous ne possédez pas les privilèges de modification d'une stratégie, celle-ci ne sera pas mise à jour.

3. Cliquez sur le bouton **Terminé** pour quitter l'Assistant.

   L'état de la ou des détections devient **Exclusion en cours**. La détection disparaît de la liste des détections après la prochaine synchronisation de l'appareil client avec le Serveur d'administration. L'exclusion des règles du Contrôle évolutif des anomalies est configurée et appliquée.

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**, 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**
- **Mises à jour**
- **Statistiques des menaces**
- **Autre**

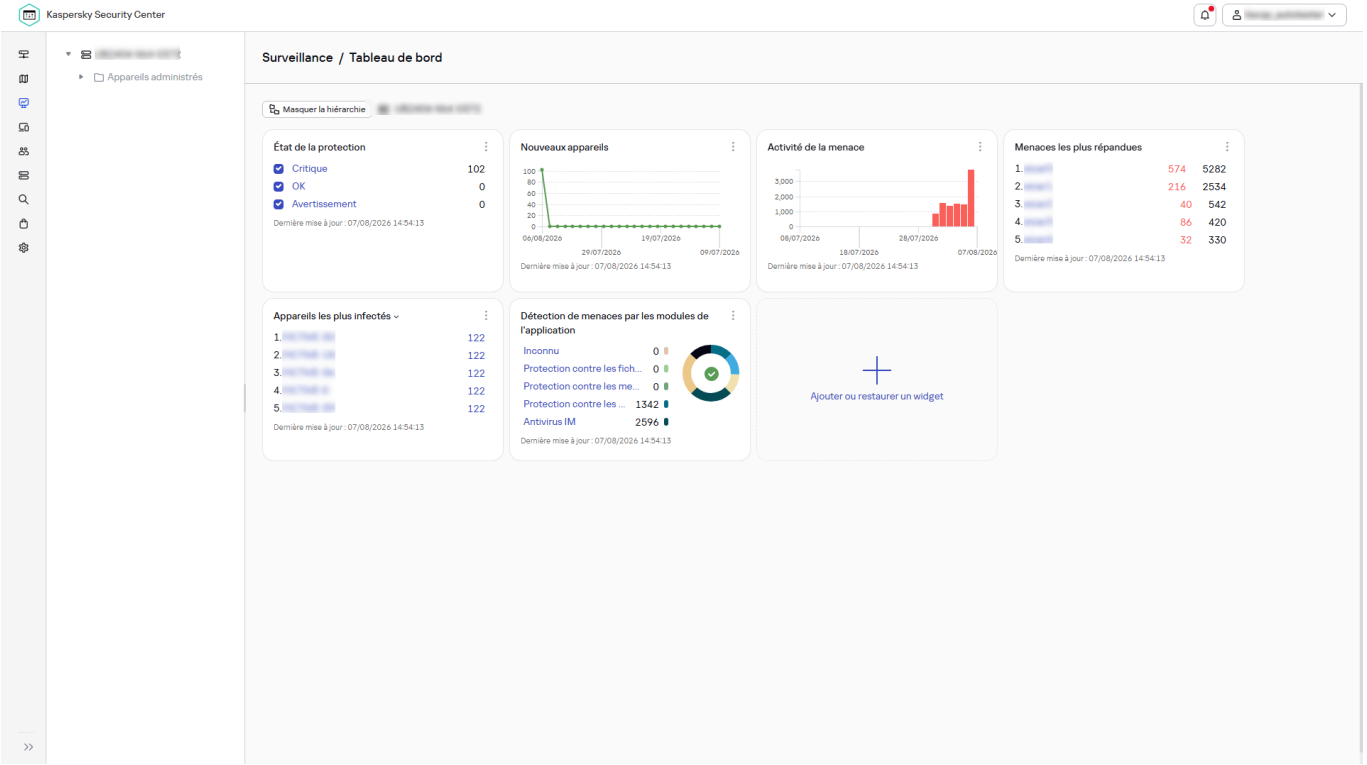
Certains widgets contiennent des informations au format texte avec des liens. Vous pouvez afficher des informations détaillées en cliquant sur le lien.

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

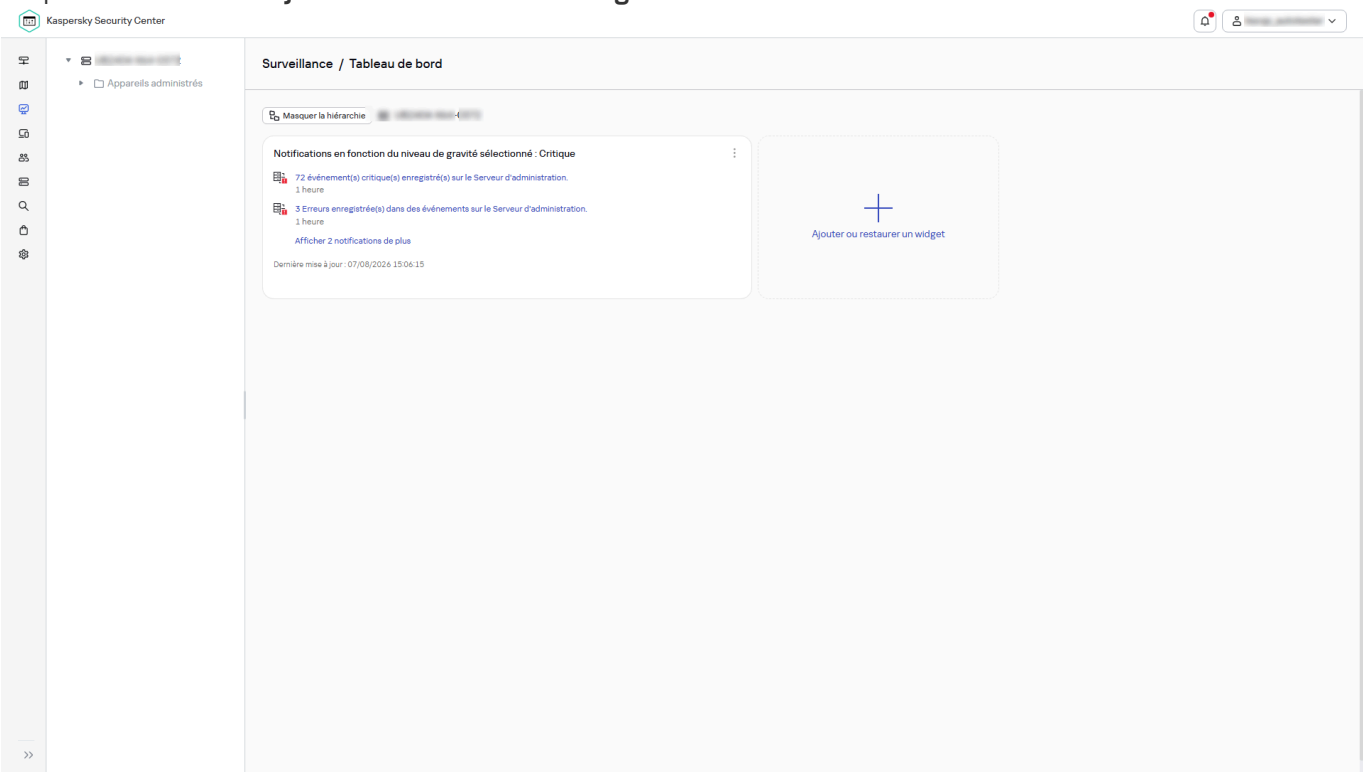
Pour ajouter des widgets au tableau de bord :

1. Dans le menu principal, accédez à **Surveillance** → **Tableau de bord**.



Le tableau de bord avec des widgets

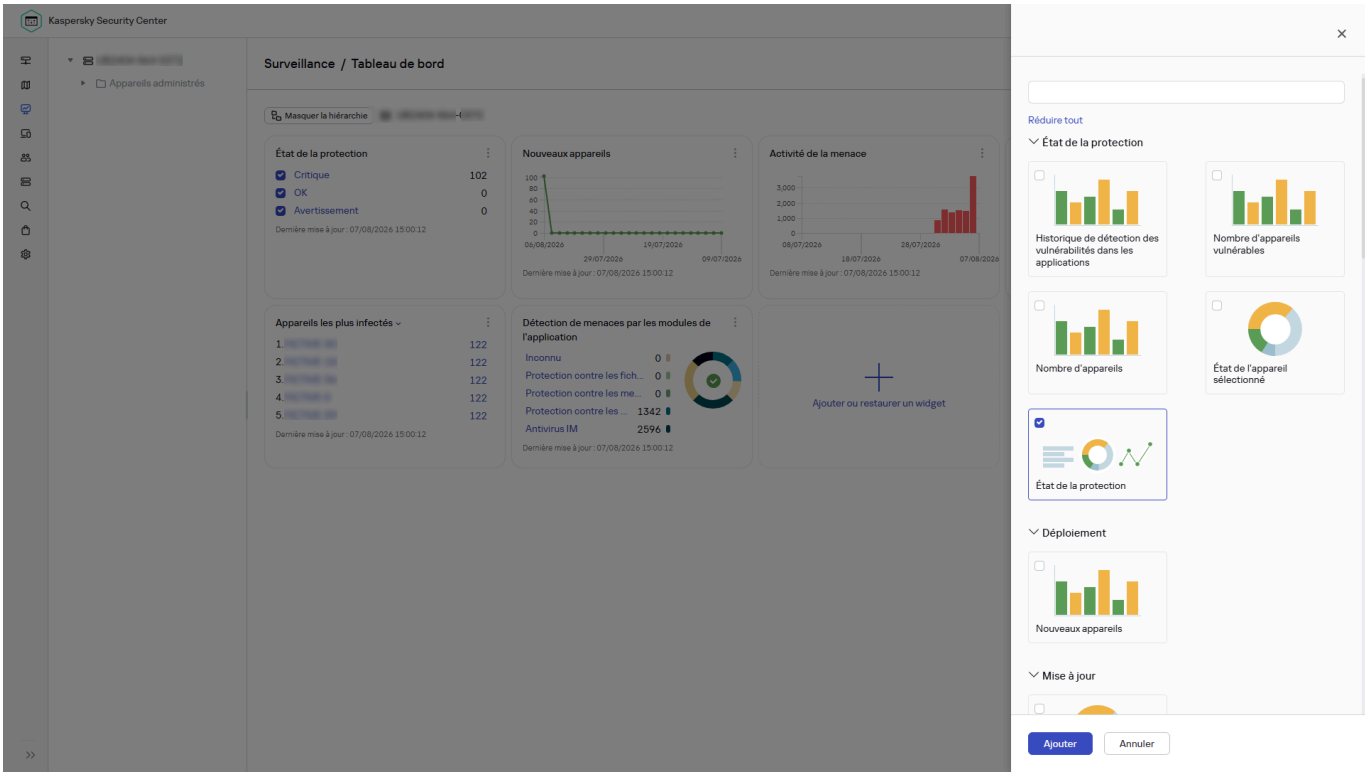
2. Cliquez sur le bouton **Ajouter ou restaurer un widget**.



Ajout d'un widget

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.



Sélection du type de widget

4. Cliquez sur **Ajouter**.

   Les widgets sélectionnés sont ajoutés à la fin du tableau de bord.

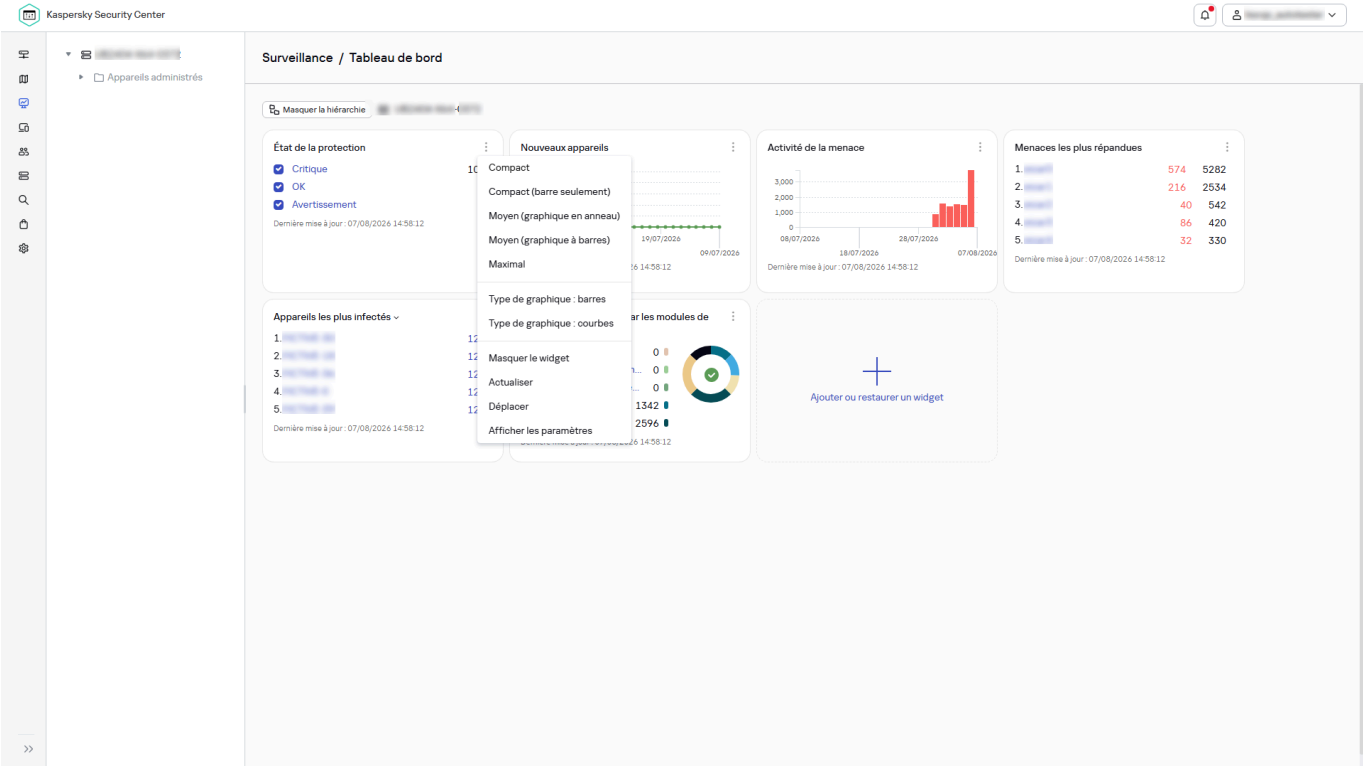
   Vous pouvez alors modifier la représentation et les paramètres des widgets ajoutés.

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** → **Tableau de bord**.

2. Cliquez sur l'icône des paramètres (⚙) en regard du widget que vous souhaitez masquer.



Le menu des widgets

3. Sélectionnez **Masquer le widget**.

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** → **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** → **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** → **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 **Enregistrer** pour enregistrer les modifications.

Les paramètres du widget sélectionnés sont modifiés.

L'ensemble de paramètres dépend de chaque widget. Ci-dessous figurent quelques paramètres habituels :

- **Champ d'application du widget** (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** définit 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.
- Les règles **Définir sur Critique si les paramètres suivants sont indiqués** et **Définir sur Avertissement si les paramètres suivants sont indiqués** déterminent l'attribution des couleurs sur le graphique d'état.

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** → **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** → **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 d'administration et de protection

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**, 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**
- **Mises 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.

Création d'un modèle de rapport

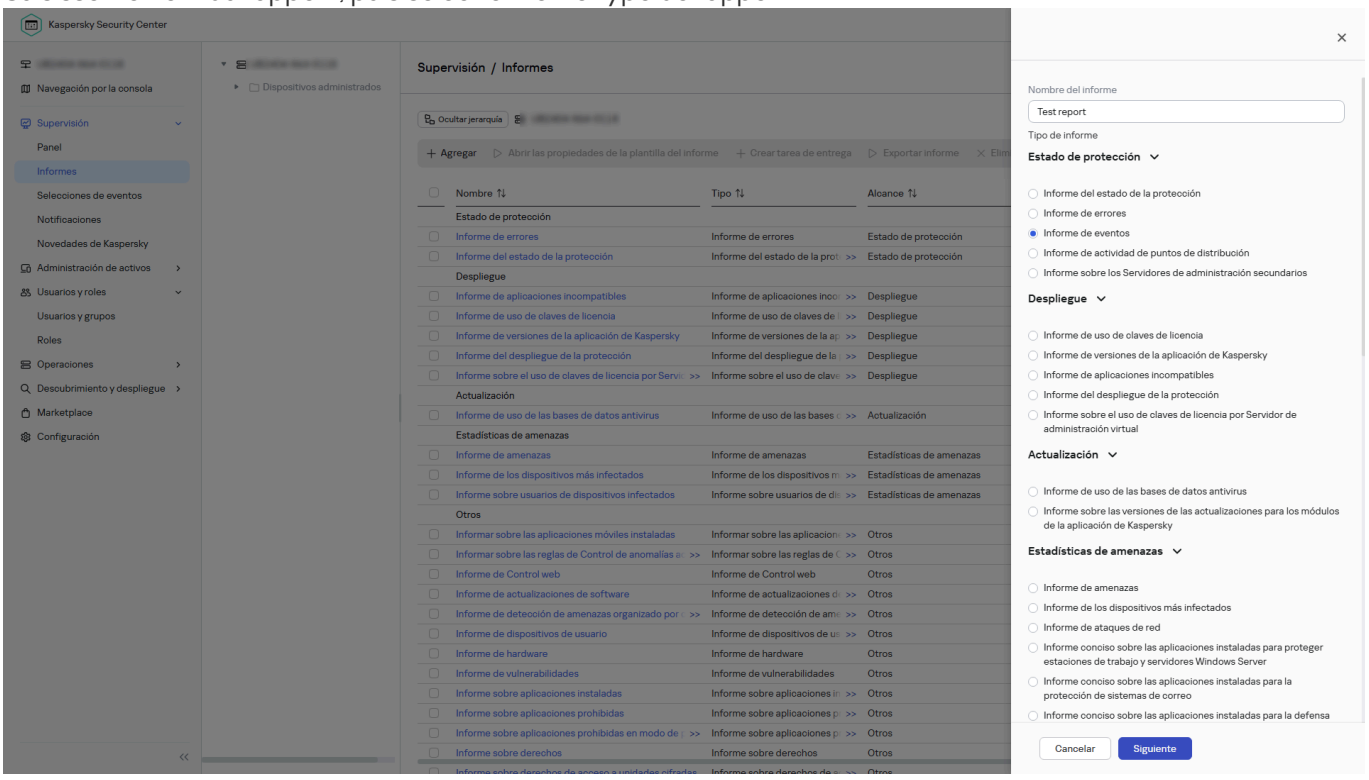
Pour créer un modèle de rapport, procédez comme suit :

1. Dans le menu principal, accédez à **Surveillance** → **Rapports**.

2. Cliquez sur **Ajouter**.

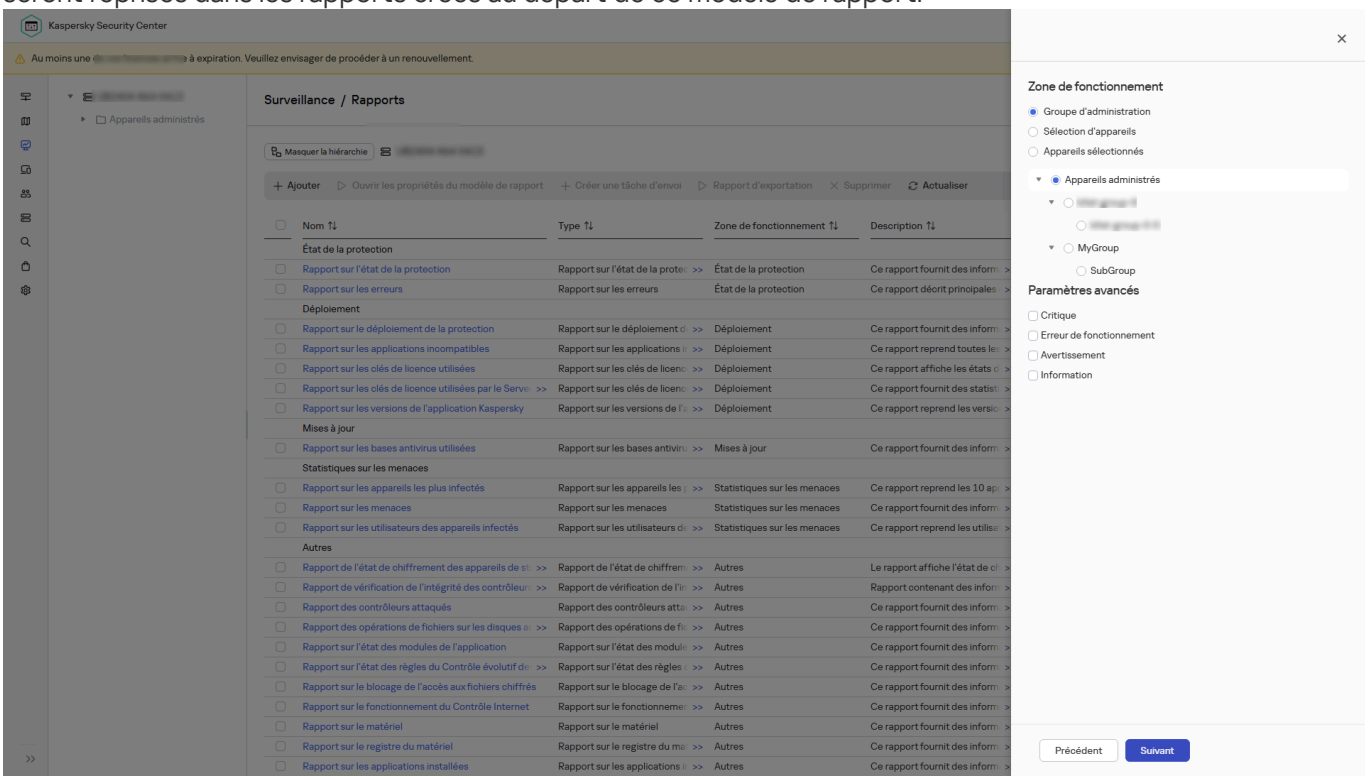
   Finalement, l'assistant de création du modèle du rapport se lancera. Parcourez les étapes de l'assistant à l'aide du bouton **Suivant**.

3. Saisissez le nom du rapport, puis sélectionnez le type de rapport.



Spécification du nom du rapport et sélection du type de rapport

4. À l'étape **Zone de fonctionnement** 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.

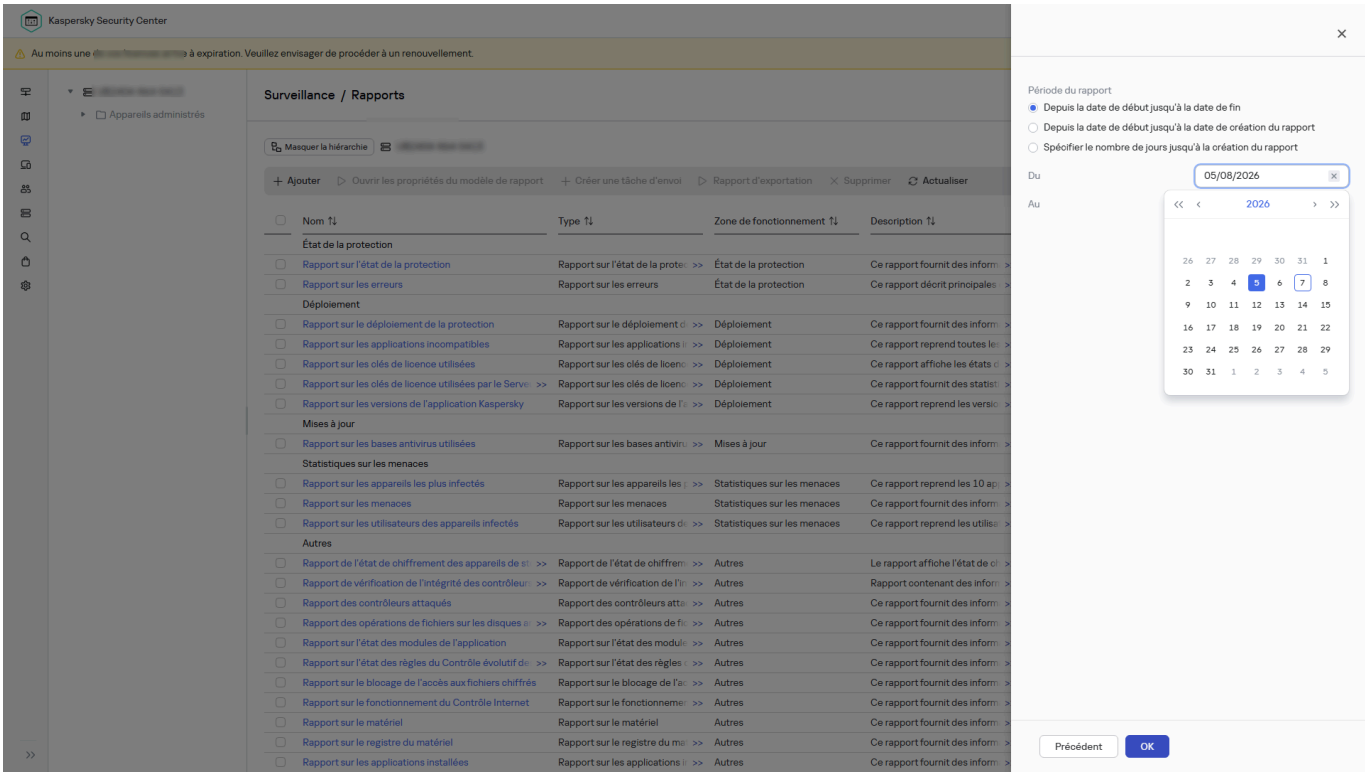


Spécification de la portée du rapport

5. À l'étape **Période du rapport** de l'assistant, définissez la période du rapport. Valeurs possibles :

- 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.



Spécification de la zone de déclaration

6. Cliquez sur le bouton **OK** pour quitter l'assistant.

7. Exécutez une des actions suivantes :

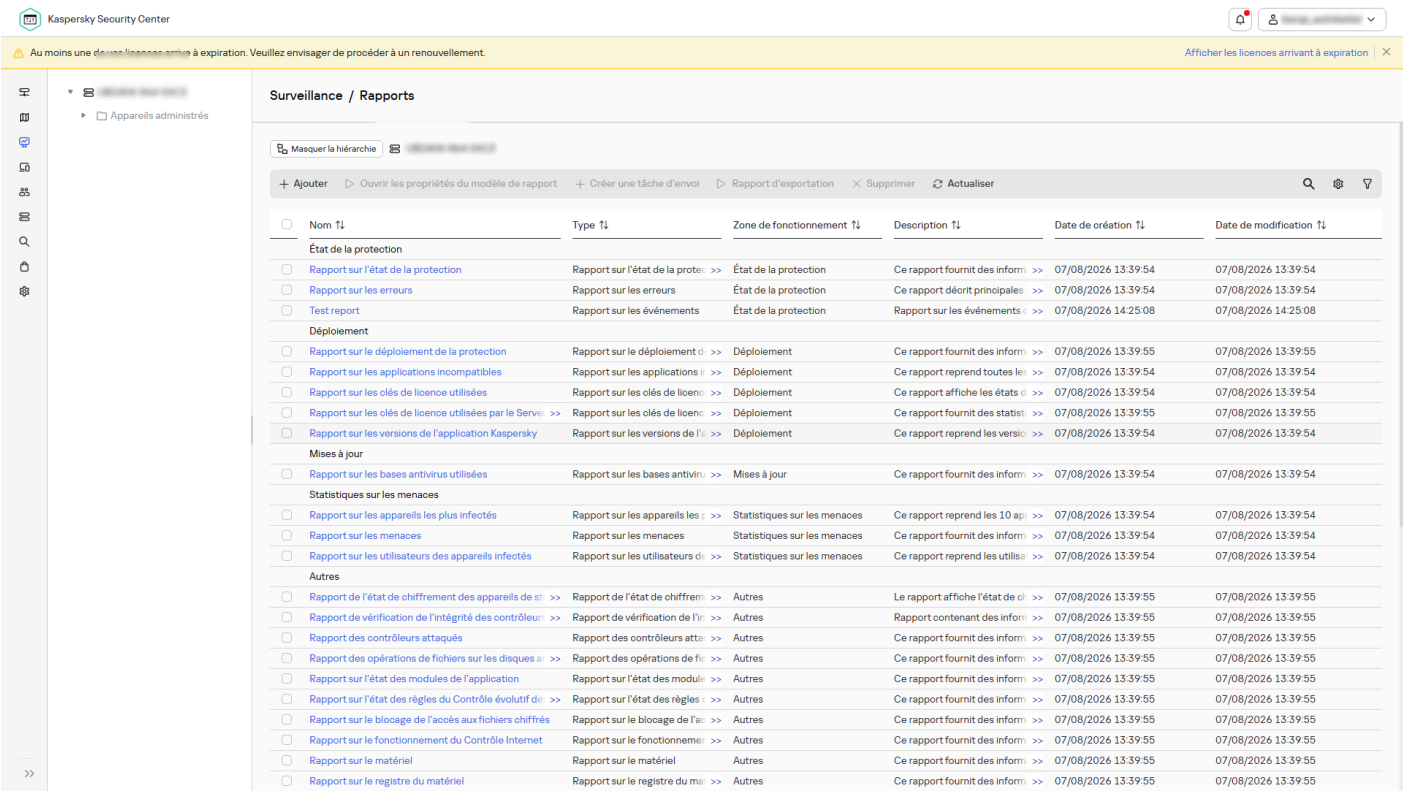
- Cliquez sur le bouton **Enregistrer et exécuter** pour enregistrer le nouveau modèle de rapport et pour exécuter un rapport créé sur la base de ce modèle.

  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.



La liste des rapports

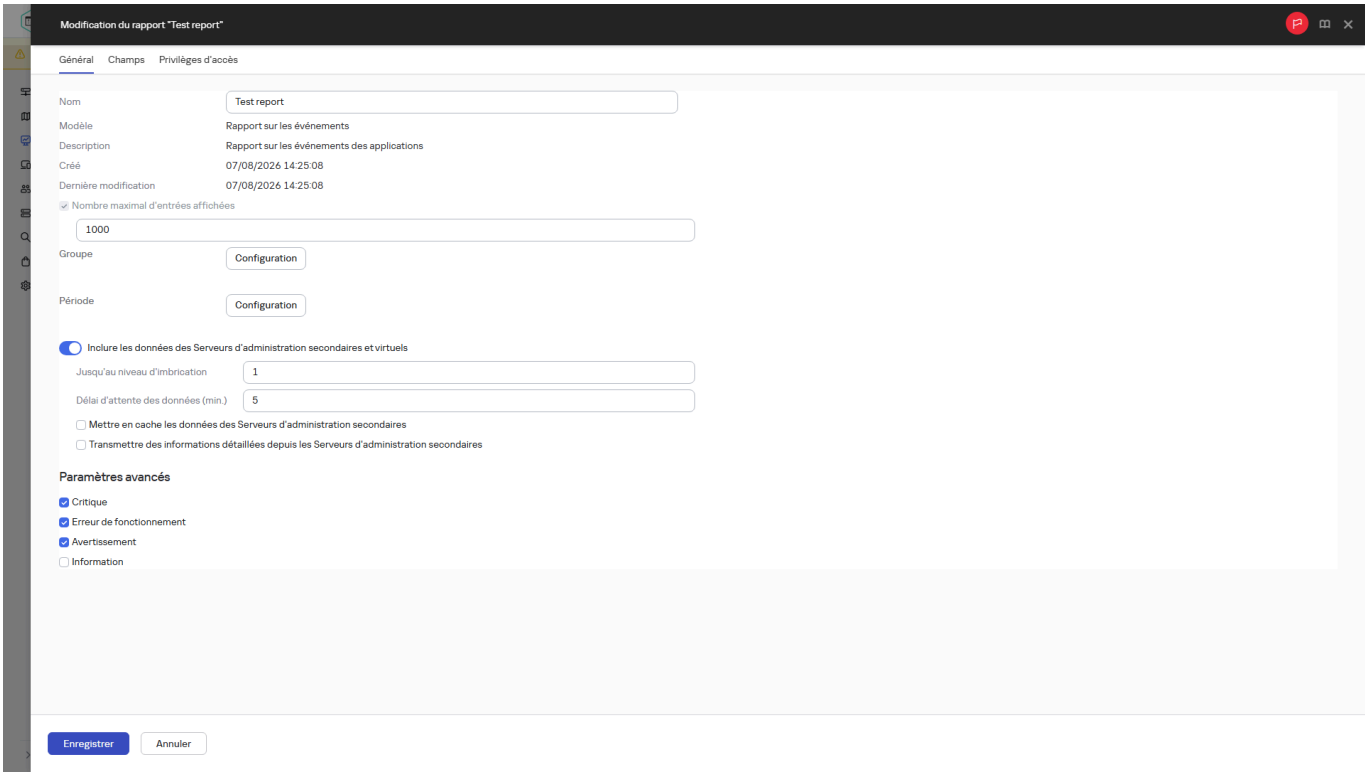
Consultation et modification des propriétés du modèle de rapport

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** → **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**.



Les propriétés du modèle de rapport

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. De plus, l'appareil risque de manquer de mémoire lors de la création d'un tel rapport. Cela peut vous empêcher de consulter le rapport.

    Cette option est activée par défaut. La valeur par défaut est égale à 1000.

- **Groupe**

  Cliquez sur le bouton **Configuration** 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 **Configuration** pour modifier la période du rapport. Pour certains types de rapports, le bouton est parfois indisponible. Valeurs possibles :

  - 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 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.

- **Délai 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.

- **Période mise à jour données en cache (h)**

  Les Serveurs d'administration secondaires transmettent régulièrement 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 depuis les 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 que vous souhaitez afficher dans le rapport. Utilisez les boutons **Haut** et **Bas** pour modifier l'ordre d'affichage 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

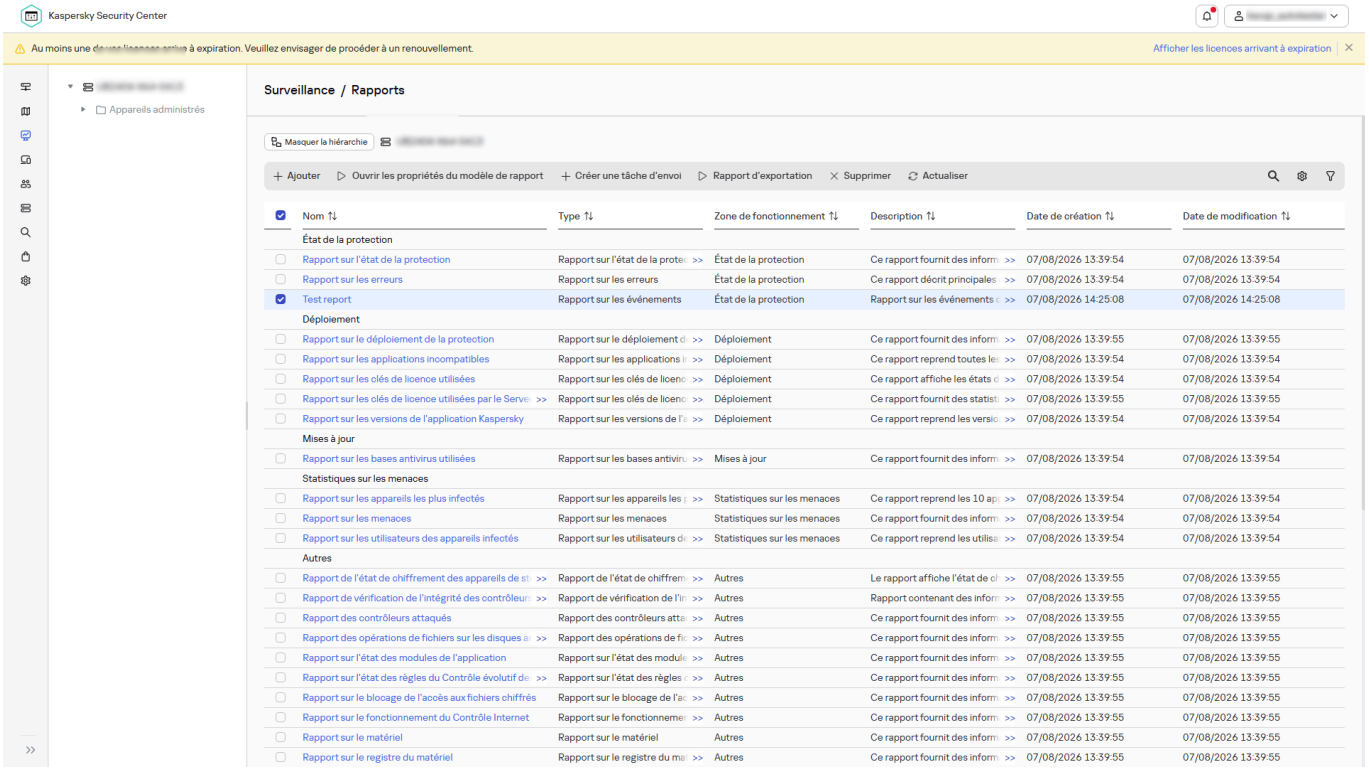
Vous pouvez enregistrer un ou plusieurs rapports au format XML, HTML ou PDF. Kaspersky Security Center Linux vous permet d'exporter simultanément jusqu'à 10 rapports vers des fichiers du format spécifié.

Pour exporter un rapport dans un fichier, procédez comme suit :

1. Dans le menu principal, accédez à **Surveillance** → **Rapports**.

2. Choisissez les rapports que vous souhaitez exporter.

   Si vous choisissez plus de 10 rapports, le bouton **Rapport d'exportation** sera désactivé.



La liste des rapports

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**.

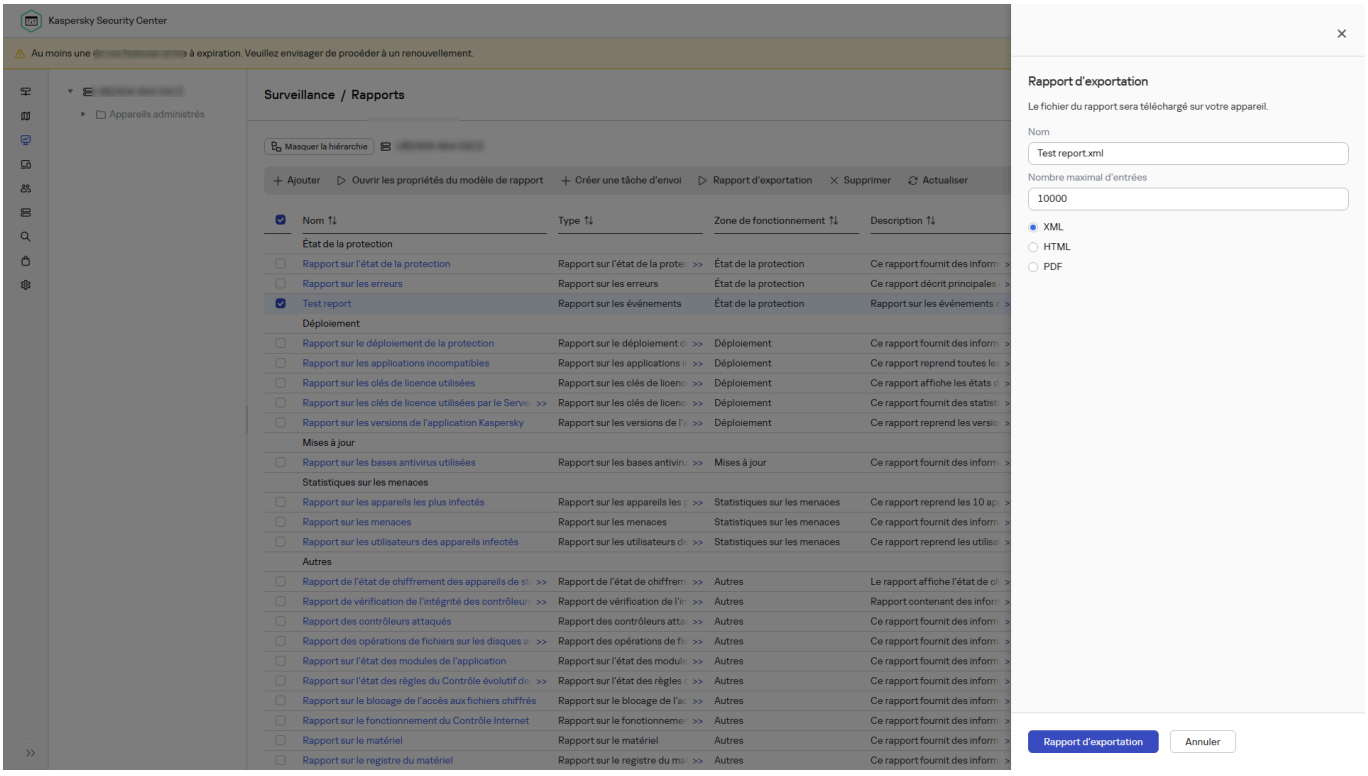
     Indiquez le nombre maximal d'entrées incluses dans le fichier de rapport. La valeur par défaut est de 10 000.

     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.



Spécification des paramètres d'exportation des rapports

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** → **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 **En savoir plus**, un tableau contenant les données de rapport détaillées.

Création d'une tâche d'envoi du rapport

Vous pouvez créer une tâche qui enverra les rapports sélectionnés.

Pour créer une tâche de diffusion des rapports, procédez comme suit :

1. Dans le menu principal, accédez à **Surveillance** → **Rapports**.

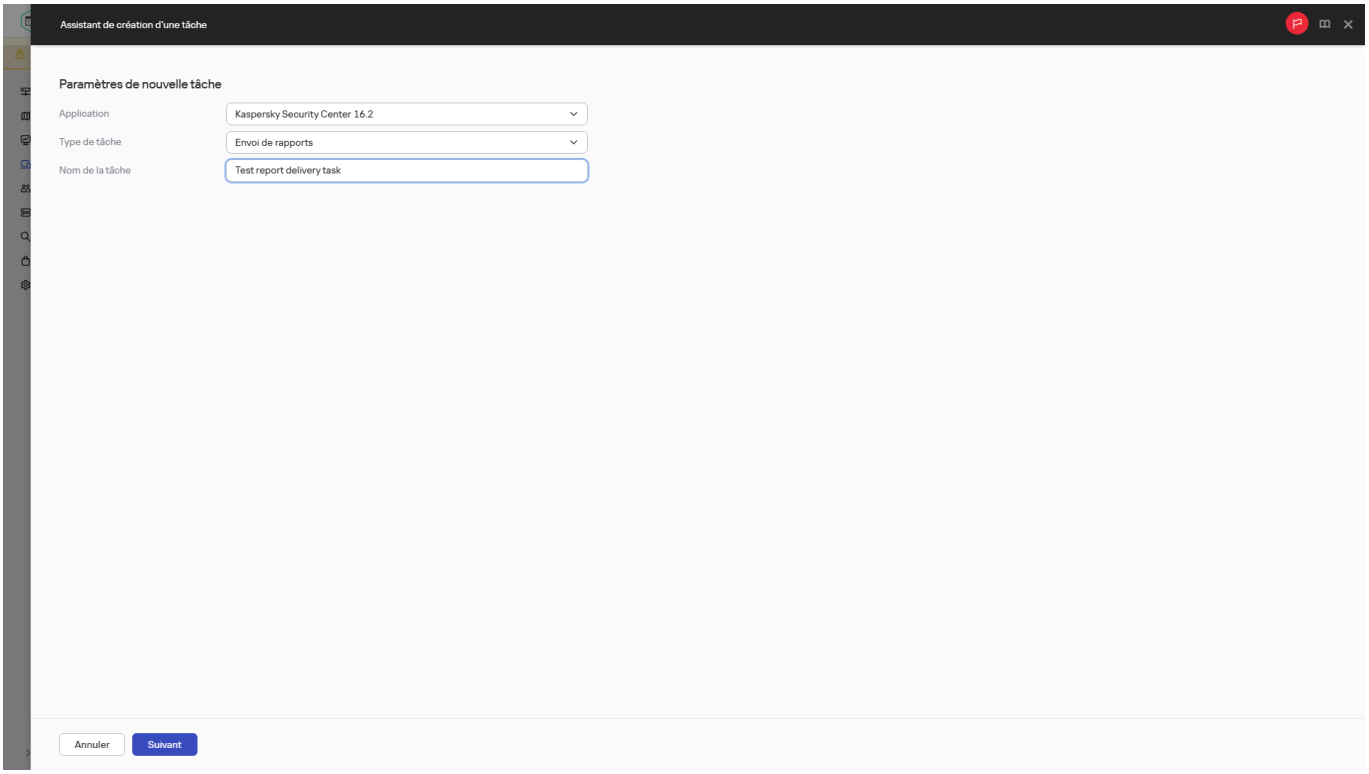
2. Cochez les cases en regard des modèles de rapport pour lequel vous souhaitez créer une tâche de diffusion des rapports.

3. Cliquez sur le bouton **Créer une tâche d'envoi**.

   Ceci permet de lancer l'assistant de création d'une tâche. Parcourez les étapes de l'assistant à l'aide du bouton **Suivant**.

4. À l'étape **Paramètres de nouvelle tâche** de l'Assistant, saisissez le nom de la tâche.

Le nom par défaut est **Envoi de rapports.** Si une tâche portant ce nom existe déjà, un numéro d'ordre (<N>) est ajouté au nom de la tâche.



Création d'une tâche d'envoi du rapport

5. À l'étape de **Configuration du rapport** de l'Assistant, configurez les paramètres suivants :

   a. Modèles de rapports que la tâche doit diffuser.

   b. Le format du rapport est HTML, XLS ou PDF.

   L'outil wkhtmltopdf est requis pour convertir un rapport au format PDF. Lorsque vous sélectionnez l'option PDF, le Serveur d'administration vérifie si l'outil wkhtmltopdf est installé sur l'appareil. Si l'outil n'est pas installé, l'application affiche un message indiquant la nécessité d'installer l'outil sur l'appareil du Serveur d'administration. Installez l'outil manuellement, puis passez à l'étape suivante.

   c. Si les rapports doivent être envoyés par email avec les paramètres d'envoi par email.

   Vous pouvez définir jusqu'à 20 adresses email. Pour séparer les adresses email, appuyez sur la touche **Entrée**. Vous pouvez également coller une liste d'adresses email séparées par une virgule, puis appuyer sur la touche **Entrée**.

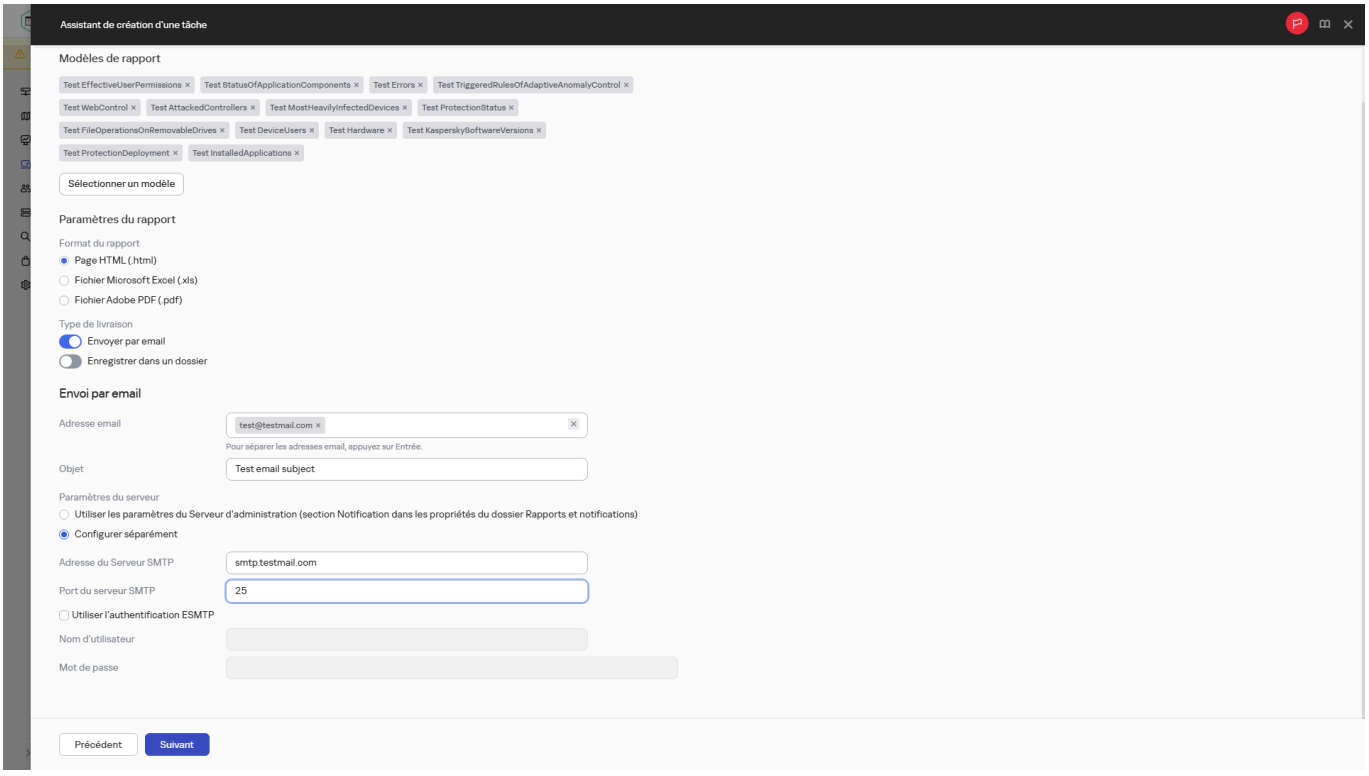
   d. Si les rapports doivent être enregistrés dans un dossier, avec les paramètres correspondants.

   Après avoir activé l'option **Enregistrer 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.



Spécification des paramètres de la tâche

6. À l'étape **Planifier la tâche** de l'Assistant, sélectionnez la planification du lancement de la tâche.

   Voici les options disponibles de planification de la tâche :

   - **Mode manuel**

     La tâche ne s'exécute pas automatiquement. Vous pouvez uniquement la lancer manuellement.

     Cette option est sélectionnée par défaut.

   - **Toutes les N minutes**

     La tâche s'exécute régulièrement, à l'intervalle défini en minutes, à partir de l'heure indiquée le jour de la création de la tâche.

     La tâche s'exécute par défaut toutes les 30 minutes, à partir de l'heure actuelle du système.

   - **Toutes les N heures**

     La tâche s'exécute régulièrement, selon l'intervalle défini en heures, à partir de la date et heure définis.

     La tâche s'exécute par défaut toutes les six heures à partir de la date et de l'heure actuelles du système.

- **Tous les N jours**

  La tâche s'exécute régulièrement, selon l'intervalle défini en jours. En outre, vous pouvez spécifier la date et l'heure de la première exécution de la tâche. Ces options supplémentaires deviennent disponibles si elles sont prises en charge par l'application pour laquelle vous créez la tâche.

  La tâche s'exécute par défaut chaque jour, à partir de la date et de l'heure actuelle du système.

- **Toutes les N semaines**

  La tâche s'exécute régulièrement, selon l'intervalle défini en semaines, le jour indiqué de la semaine et à l'heure indiquée.

  La tâche s'exécute par défaut chaque vendredi à l'heure système actuelle.

- **Chaque mois**

  La tâche s'exécute régulièrement le jour du mois défini, à l'heure indiquée.

  Si le jour en question ne figure pas dans le mois, la tâche s'exécute le dernier jour.

  La tâche s'exécute par défaut le premier jour de chaque mois, à l'heure système actuelle.

- **Aux jours indiqués**

  La tâche s'exécute régulièrement les jours du mois définis, à l'heure indiquée.

  Par défaut, l'heure de début est 18:00 et aucun jour du mois n'est sélectionné.

  Notez que vous ne sélectionnez ni une date précise dans le mois, ni le numéro de la semaine (première, deuxième semaine du mois) mais le numéro d'ordre du jour de la semaine à l'intérieur d'un mois. Par exemple, si vous placez le curseur dans la cellule **Ma** de la ligne **Premier**, cela signifie que la tâche sera exécutée tous les premiers mardis de chaque nouveau mois.

  Vous pouvez sélectionner plusieurs jours de la semaine.

- **Lors de la détection d'une propagation de virus**

  La tâche s'exécute après un événement *Propagation de virus* de virus. Sélectionnez les types d'application qui vont surveiller les propagations de virus. Les types suivants de Application sont présent :

  - Antivirus pour postes de travail et serveurs de fichiers
  - Antivirus de protection du périmètre
  - Antivirus pour systèmes de messagerie

  Tous les types d'application sont cochés par défaut.

  Il se peut que vous souhaitiez exécuter différentes tâches en fonction du type d'application de sécurité qui signale une propagation de virus. Dans ce cas, supprimez la sélection des types d'application dont vous n'avez pas besoin.

- **À la fin d'une autre tâche**

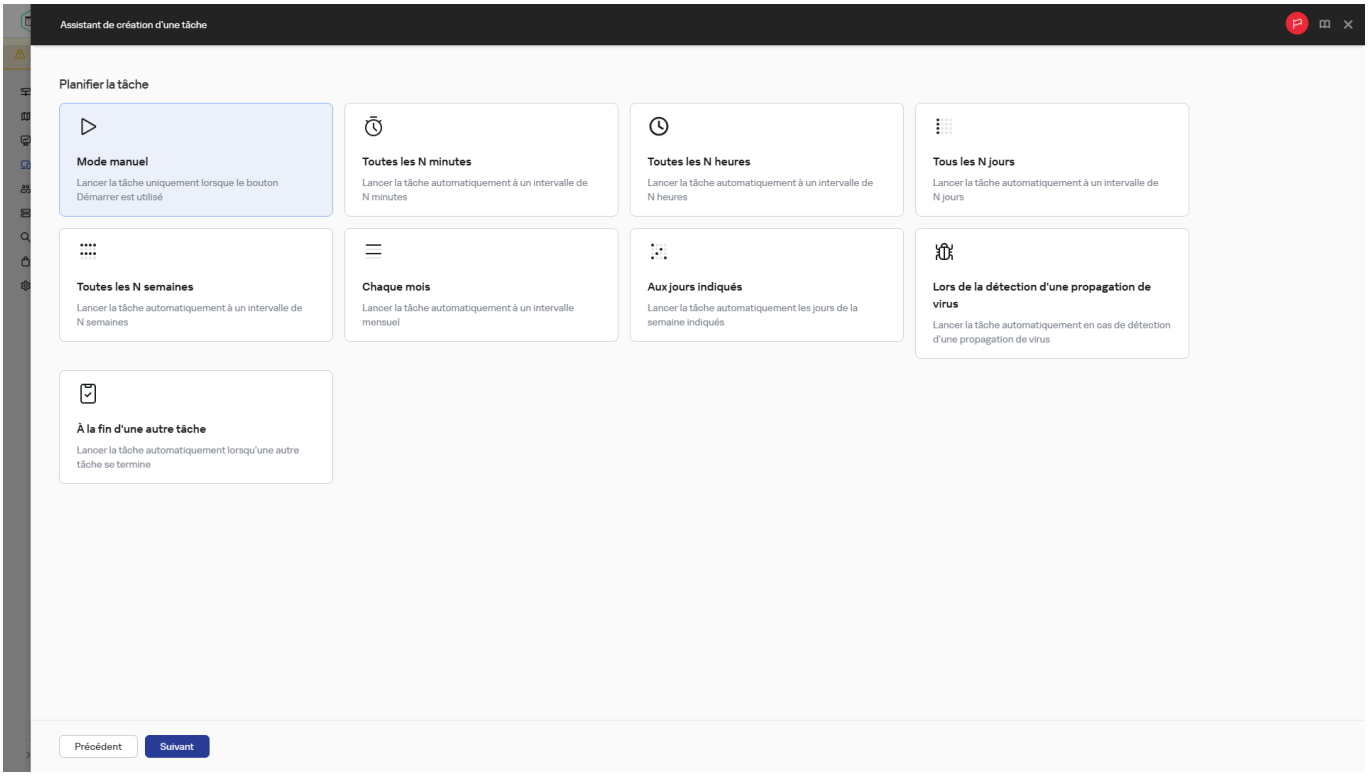
  La tâche actuelle démarre à la fin d'une autre tâche. Cette option ne fonctionne que si les deux tâches sont affectées aux mêmes appareils. Par exemple, vous pouvez exécuter la tâche *Administration des appareils* avec l'option **&Activer l'appareil** et, une fois celle-ci terminée, exécuter la tâche de *recherche de virus* comme tâche de déclenchement.

  Il faut sélectionner la tâche de déclenchement dans le tableau et l'état avec lequel cette tâche doit se terminer (**Terminée avec succès** ou **Échec**).

  Si nécessaire, vous pouvez rechercher, trier et filtrer les tâches dans le tableau comme suit :

  - Saisissez le nom de la tâche dans le champ de recherche pour rechercher une tâche par son nom.
  - Cliquez sur l'icône de tri pour trier les tâches par nom.

    Par défaut, les tâches sont triées par ordre alphabétique croissant.
  - Cliquez sur l'icône du filtre, et dans la fenêtre qui s'ouvre, filtrez les tâches par groupe, puis cliquez sur le bouton **Appliquer**.



Sélection de la planification du lancement de la tâche

7. À cette étape de l'Assistant, configurez d'autres paramètres de planification de tâches :

- Dans la section **Calendrier de la tâche**, vérifiez ou reconfigurez la planification précédemment sélectionnée, puis définissez l'intervalle de temps, les jours du mois ou de la semaine, la condition de propagation de virus ou la fin d'une autre tâche comme déclencheur du lancement de celle-ci. Une heure de début peut également être définie dans cette section si la planification applicable est sélectionnée.

- Dans la section **Paramètres supplémentaires**, définissez les paramètres suivants :

  - **Lancer les tâches non exécutées**

    Cette option détermine le comportement d'une tâche si un appareil client n'est pas visible sur le réseau quand la tâche est sur le point de démarrer.

    Si la case est Activé, lors du lancement suivant de l'application de Kaspersky sur cet appareil client, une tentative de lancement de la tâche sera faite. Si la programmation de la tâche est **Manuel**, **Une fois** ou **Immédiatement**, la tâche est immédiatement lancée dès que l'appareil apparaît sur le réseau ou immédiatement après l'inclusion de l'appareil dans la zone d'action de la tâche.

    Si cette option est désactivée, seules les tâches planifiées s'exécutent sur les appareils clients. Pour les planifications **Manuel**, **Une fois** et **Immédiatement**, les tâches s'exécutent uniquement sur les appareils clients qui sont visibles sur le réseau. Par exemple, vous pouvez désactiver cette option pour une tâche qui consomme des ressources que vous voulez exécuter uniquement en dehors des heures de bureau.

    Cette option est Inactif par défaut.

  - **Adopter un décalage aléatoire automatique pour les lancements de tâche**

    Si cette option est activée, la tâche est lancée sur les appareils clients de manière aléatoire au cours d'un intervalle défini. C'est ce qu'on appelle un *lancement échelonné d'une tâche*. Un lancement échelonné de tâche permet d'éviter la communication simultanée d'un nombre important d'appareils clients avec le Serveur d'administration lors du lancement de la tâche programmée.

    Le temps du lancement aléatoire est automatiquement calculée lors de la création d'une tâche selon le nombre d'appareils clients sur lesquels la tâche est diffusée. Par la suite, la tâche démarre toujours à l'heure de lancement calculée. Toutefois, quand les paramètres de la tâche sont modifiés ou si la tâche est lancée manuellement, la valeur calculée de l'heure de lancement de la tâche est modifiée.

    Si la case n'est pas cochée, le lancement de la tâche sur les appareils clients s'opère selon la planification.

  - **Décaler aléatoirement et automatiquement le lancement de la tâche dans un intervalle de**

    Si cette option est activée, la tâche est lancée sur les appareils clients de manière aléatoire au cours de l'intervalle défini. Un lancement échelonné de tâche permet d'éviter la communication simultanée d'un nombre important d'appareils clients avec le Serveur d'administration lors du lancement de la tâche programmée.

    Si la case n'est pas cochée, le lancement de la tâche sur les appareils clients s'opère selon la planification.

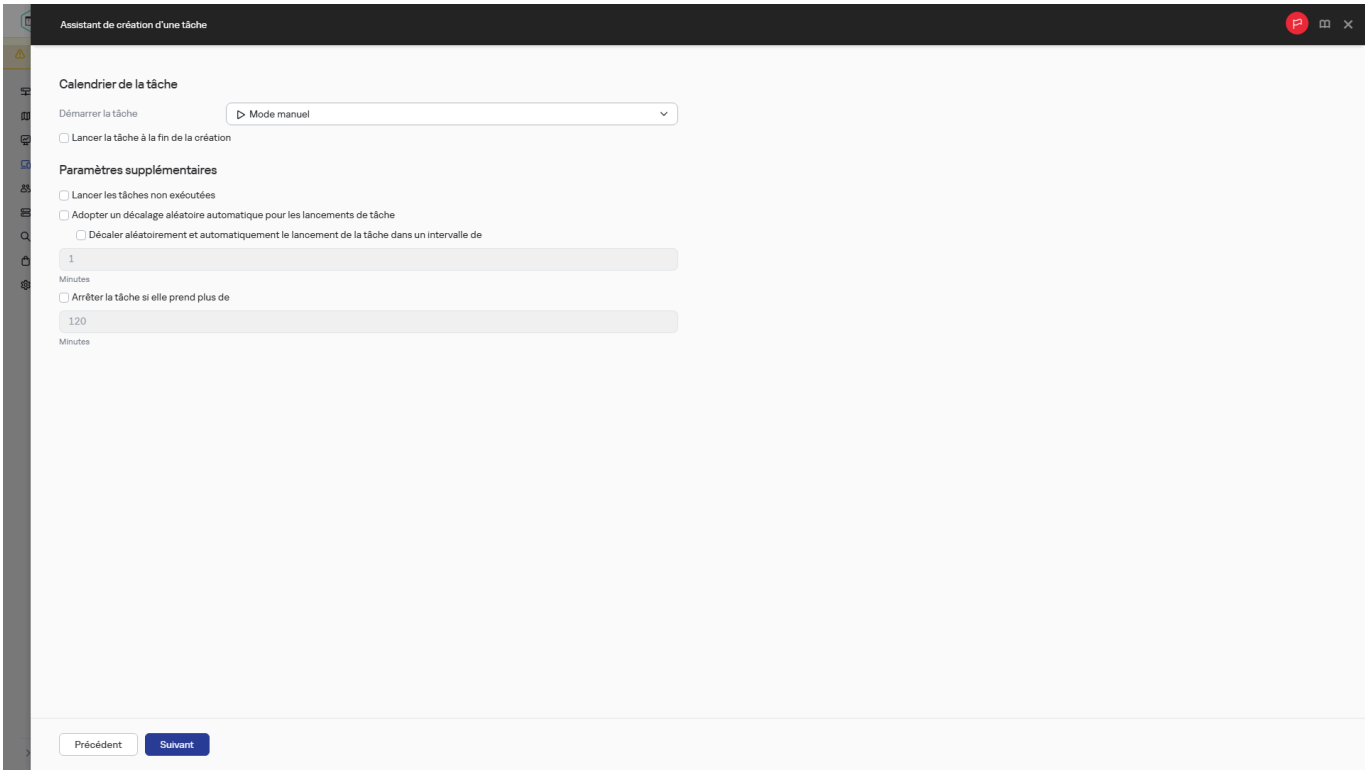
    Cette option est Inactif par défaut. Par défaut, la valeur de cet intervalle est de une minute.

  - **Arrêter la tâche si elle prend plus de**

    A l'issue du délai défini, la tâche s'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.

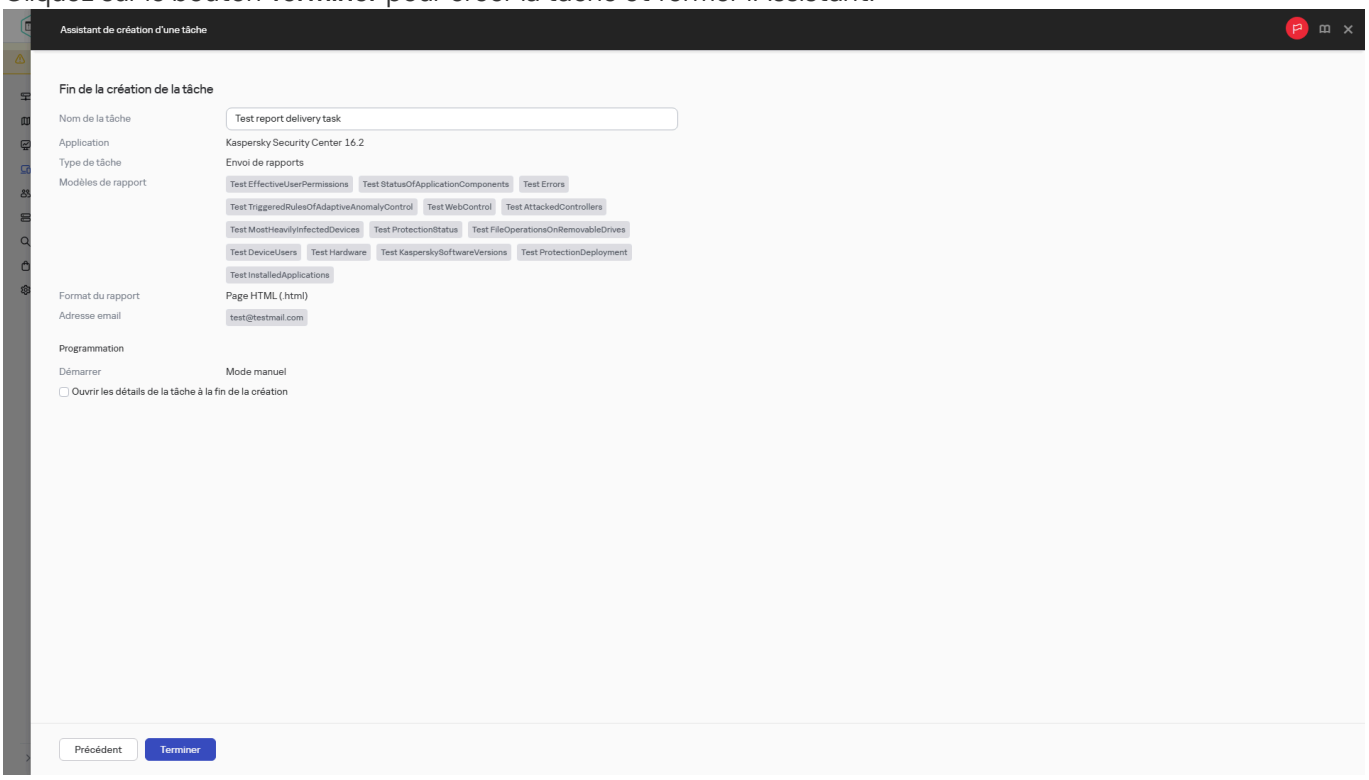


Spécification des paramètres de planification des tâches

8. À l'étape **Sélection du compte utilisateur pour exécuter la tâche** de l'Assistant, indiquez les identifiants du compte utilisateur qui sera utilisé pour exécuter la tâche.

9. Si vous souhaitez modifier d'autres paramètres de la tâche après sa création, à l'étape **Fin de la création de la tâche** de l'Assistant, activez l'option **Ouvrir les détails de la tâche à la fin de la création**. Cette option est activée par défaut.

10. Cliquez sur le bouton **Terminer** pour créer la tâche et fermer l'Assistant.



Fin de la création de la tâche

La tâche de remise de rapports est créée. Si l'option **Ouvrir les détails de la tâche à la fin de la création** est activée, la fenêtre des paramètres de la tâche s'ouvre.

Suppression des modèles de rapport

Pour supprimer un ou plusieurs modèles de rapport, procédez comme suit :

1. Dans le menu principal, accédez à **Surveillance** → **Rapports**.
2. Cochez les cases en regard des modèles de rapport que vous souhaitez supprimer.
3. Ensuite, 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 : Propagation 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 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 ci-dessous présente les événements du Serveur d'administration dont la gravité est **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 du type d'événement	ID de type d'événement	Type d'événement	Description	Durée de stockage par défaut
Le certificat du Serveur d'Administration pour les appareils mobiles a expiré	6129	KLSRV_EV_SRV_CERT_EXPIRED_DN	Des événements de ce type se produisent lorsque les certificats du Serveur d'administration pour les appareils mobiles et les appareils UEFI expirent. Vous devez mettre à jour le certificat expiré.	180 jours
Audit : l'exportation vers le SIEM a échoué	5130	KLAUD_EV_SIEM_EXPORT_ERROR	Les événements de ce type se produisent lorsque l'exportation d'événements vers le système SIEM a échoué en raison d'une erreur de connexion avec le système SIEM.	180 jours
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

Nom affiché du type d'événement	ID de type d'événement	Type d'événement	Description	Durée de stockage par défaut
État de l'appareil 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
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
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 restrictions de la 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

Nom affiché du type d'événement	ID de type d'événement	Type d'événement	Description	Durée de stockage par défaut
Mode limité	4130	KLSRV_EV_LICENSE_SRV_LIMITED_MODE	Ce type d'événements se produit lorsque Kaspersky Security Center Linux commence à fonctionner avec les fonctionnalités de base, sans les fonctionnalités de Gestion des vulnérabilités et des correctifs et d'administration des appareils mobiles. Les causes de l'événement et les réponses appropriées sont indiquées ci-après : • La durée de validité de la licence a expiré. Fournissez une licence pour utiliser le mode de fonctionnalité complète de Kaspersky Security Center Linux (ajoutez un code d'activation valide ou un fichier clé au Serveur d'administration). • Le serveur d'administration gère plus d'appareils que spécifié par la limite de licence. Déplacez les appareils des groupes d'administration d'un serveur d'administration vers les groupes d'un autre serveur d'administration (si permis pas la limite de licence de l'autre serveur d'administration).	180 jours
La durée de validité du certificat MDM a expiré	4132	KLSRV_CERTIFICATE_EXPIRED	Des événements de ce type se produisent lorsque le certificat client sur les appareils mobiles expire.	180 jours
Le 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
Les mises à jour des modules des applications Kaspersky ont été rappelées	4142	KLSRV_SEAMLESS_UPDATE_REVOKED	Des événements de ce type se produisent si les mises à jour ont été révoquées par les Experts Kaspersky, par exemple pour les remplacer par des versions plus récentes. Pour ces mises à jour, l'état est *Révoqué*. L'événement concerne les correctifs de Kaspersky Security Center Linux et non les modules d'applications administrés par Kaspersky. L'événement indique que les mises à jour continues ne sont pas installées.	180 jours
Propagation de virus	• 26 (pour la Protection contre les fichiers malicieux) • 27 (pour la Protection contre les menaces par emails) • 28 (pour le pare-feu)	GNRL_EV_VIRUS_OUTBREAK	Ce type d'événements se produit lorsque le nombre d'objets malveillants détectés sur plusieurs appareils administrés dépasse le seuil sur une courte durée. Vous pouvez répondre à l'événement des manières suivantes : • Vous pouvez configurer le seuil dans les propriétés du Serveur d'administration. • Vous pouvez aussi créer une stratégie plus stricte qui sera activée ou créer une tâche qui sera exécutée quand l'événement se produit.	

Événements liés à des erreurs de fonctionnement du Serveur d'administration

Le tableau ci-dessous présente les événements du Serveur d'administration dont le niveau d'importance est **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
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
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
Pour un des groupes des applications sous licence, la limite des installations a été dépassée	4126	KLSRV_INVLICPROD_EXCEDED	Le serveur d'administration génère ce type d'événements périodiquement (toutes les heures). Ce type d'événements se produit si dans Kaspersky Security Center Linux, vous administrez les clés d'applications tierces et si le nombre d'installations a dépassé la limite définie par la clé de licence de l'application tierce. Vous pouvez répondre à l'événement des manières suivantes : • Parcourez la liste des appareils administrés. Supprimez l'application tierce des appareils où l'application n'est pas utilisée. • Utiliser une licence tierce pour plusieurs appareils. Vous pouvez gérer les clés de licence d'applications tierces à l'aide des fonctionnalités des groupes des applications sous licence. Un groupe des applications sous licence inclut les applications tierces qui répondent aux critères que vous avez définis.	180 jours
Plus d'espace disponible sur le disque	4107	KLSRV_DISK_FULL	Des événements de ce type se produisent lorsque le disque dur de l'appareil sur lequel le Serveur d'administration est installé ne dispose plus d'espace libre. Libérez de l'espace disque sur l'appareil.	180 jours

Nom affiché du type d'événement	ID de type d'événement	Type d'événement	Description	Durée de stockage par défaut
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
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
Le dossier en accès public n'est pas disponible	4108	KLSRV_SHARED_FOLDER_UNAVAILABLE	Ce type d'événements se produit si le dossier partagé du Serveur d'administration n'est pas disponible. Vous pouvez répondre à l'événement des manières suivantes : • Vérifiez si le Serveur d'administration (où se trouve le dossier partagé) est sous tension et disponible. • Vérifiez si un nom d'utilisateur et / ou un mot de passe du dossier a changé. • Vérifiez la connexion réseau.	180 jours
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

Événements d'avertissement du Serveur d'administration

Le tableau suivant reprend les événements de l'Agent d'administration, regroupés par niveau de gravité **Attention**.

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 de l'événement** 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
Le certificat du Serveur d'Administration pour les appareils mobiles expire	6128	KLSRV_EV_SRV_CERT_EXPIRES_SOON	Des événements de ce type se produisent lorsque les certificats du Serveur d'administration pour les appareils mobiles et les appareils UEFI expirent. Vous devez mettre à jour le certificat expiré.	90 jours
La durée de validité du certificat APNs expire bientôt	4136	KLSRV_APN_CERTIFICATE_EXPIRES_SOON	Les événements de ce type se produisent lorsqu'il reste moins de 14 jours avant l'expiration du certificat APNs. Lorsque le certificat APNs expire, vous devez renouveler manuellement le certificat APNs et l'installer sur un serveur MDM iOS. Nous vous recommandons de planifier le renouvellement du certificat APNs avant la date d'expiration.	Non stocké
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
Audit : échec du test de connexion au serveur SIEM	5120	KLAUD_EV_SIEM_TEST_FAILED	Les événements de ce type se produisent lorsqu'un test de connexion automatique au serveur SIEM a échoué.	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

Nom affiché du type d'événement	ID de type d'événement	Type d'événement	Description	Durée de stockage par défaut
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
Noms d'appareil en conflit	4102	KLSRV_EVENT_HOSTS_CONFLICT	Des événements de ce type se produisent lorsque le Serveur d'administration considère deux ou plusieurs appareils administrés comme un seul appareil. La plupart du temps, cela se produit lorsqu'un disque dur cloné a été utilisé pour déployer des logiciels sur des appareils administrés et sans que l'Agent d'administration ne passe en mode de clonage de disque dédié sur un appareil de référence. Pour éviter ce problème, passez l'Agent d'administration en mode de clonage de disque sur un appareil de référence avant de cloner le disque dur de cet appareil.	90 jours
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
La connexion au Serveur d'administration secondaire a été interrompue	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

Nom affiché du type d'événement	ID de type d'événement	Type d'événement	Description	Durée de stockage par défaut
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
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
Échec du téléchargement du fichier sur l'appareil	4165	KLSRV_FILE_DOWNLOAD_FAILED	Des événements de ce type se produisent dans les cas suivants : • Vous essayez de télécharger un fichier dans le conteneur d'entreprise, mais le conteneur d'entreprise n'a pas été créé. • Il n'y a pas assez d'espace sur l'appareil. • Échec du téléchargement des informations sur le fichier depuis le serveur. • Échec du téléchargement du contenu du fichier depuis le serveur. • Impossible de créer le dossier sur l'appareil. • L'autorisation d'accès au fichier est manquante sur l'appareil personnel. • L'autorisation d'accès aux fichiers est manquante dans le conteneur d'entreprise.	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

Nom affiché du type d'événement	ID de type d'événement	Type d'événement	Description	Durée de stockage par défaut
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
Événements fréquents détectés		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
Le disque dur est presque plein	4105	KLSRV_NO_SPACE_ON_VOLUMES	Des événements de ce type se produisent lorsque le disque dur de l'appareil sur lequel le Serveur d'administration est installé ne dispose presque plus d'espace libre. Libérez de l'espace disque sur l'appareil.	90 jours
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 la description de l'événement et répondez en conséquence.	90 jours

Nom affiché du type d'événement	ID de type d'événement	Type d'événement	Description	Durée de stockage par défaut
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 restrictions de la 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
Pour un des groupes des applications sous licence, la limite du nombre d'installations sera bientôt dépassée	4128	KLSRV_INVLICPROD_EXPIRED_SOON	Des événements de ce type se produisent lorsque l'une des clés de licence des applications tierces incluses dans un groupe d'applications sous licence est sur le point d'expirer. En conséquence, la limite d'installation pour l'un des groupes sera réduite. Vous pouvez répondre à l'événement des manières suivantes : • Si l'application tierce n'est pas utilisée sur certains des appareils administrés, supprimez l'application de ces appareils. • Si vous prévoyez que le nombre d'installations pour l'application tierce dépassera le nombre maximum autorisé prochainement, envisagez d'obtenir à l'avance une licence tierce pour un plus grand nombre d'appareils. Vous pouvez gérer les clés de licence d'applications tierces à l'aide des fonctionnalités des groupes d'applications sous licence.	90 jours
Les nouvelles mises à jour des modules de l'application Kaspersky ont été enregistrées	4141	KLSRV_SEAMLESS_UPDATE_REGISTERED	Des événements de ce type se produisent lorsque le Serveur d'administration enregistre de nouvelles mises à jour pour le logiciel Kaspersky installé sur des appareils administrés dont l'installation nécessite une autorisation. Approuvez ou refusez les mises à jour à l'aide de Kaspersky Security Center Web Console.	90 jours

Nom affiché du type d'événement	ID de type d'événement	Type d'événement	Description	Durée de stockage par défaut
Espace insuffisant 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. • 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 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.

Nom affiché du type d'événement	ID de type d'événement	Type d'événement	Description	Durée de stockage par défaut
Le certificat du Serveur d'administration pour les appareils mobiles est renouvelé	6127	KLSRV_EV_SRV_CERT_RENEWED	Cet événement se produit lorsque le certificat du Serveur d'administration a été renouvelé.	30 jours
Audit : la connexion au Serveur d'administration a été interrompue	4151	KLAUD_EV_SERVERDISCONNECT		30 jours
Audit : une connexion au Serveur d'administration a été établie	4147	KLAUD_EV_SERVERCONNECT	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.	30 jours
Audit : clés de chiffrement importées/exportées	5100	KLAUD_EV_DPEKEYSEXPORT	Par exemple, cet événement se produit pendant la migration.	30 jours
Audit : les paramètres de groupe ont été modifiés	4149	KLAUD_EV_ADMGROUP_CHANGED	Des événements de ce type se produisent lorsqu'un groupe de sécurité a été modifié.	30 jours
Audit : un objet a été modifié	4148	KLAUD_EV_OBJECTMODIFY	Cet événement permet de suivre les modifications apportées aux objets suivants : • Groupe d'administration • Groupe de sécurité • Utilisateur • Paquet • Tâche • Stratégie • Serveur • Serveur virtuel	30 jours
Audit : les propriétés de l'objet ont été modifiées	4152	KLAUD_EV_OBJECTPROPMODIFIED	Cet événement suit les modifications apportées aux propriétés suivantes : • Utilisateur • Licence • Serveur • Serveur virtuel	30 jours
Audit : l'état de l'objet a été modifié	4150	KLAUD_EV_TASK_STATE_CHANGED	Par exemple, cet événement se produit lorsqu'une tâche a échoué avec une erreur.	30 jours
Audit : la commande a été envoyée à l'appareil	4170	KLAUD_EV_COMMAND_SENT	Ce genre d'événements se produit lorsque l'utilisateur envoie une commande à l'appareil mobile.	30 jours
Audit : le test de connexion au serveur SIEM a réussi	5110	KLAUD_EV_SIEM_TEST_SUCCESS	Les événements de ce type se produisent lorsqu'un test de connexion au serveur SIEM a réussi.	30 jours

Nom affiché du type d'événement	ID de type d'événement	Type d'événement	Description	Durée de stockage par défaut
Audit : les autorisations de l'utilisateur ont été modifiées	4153	KLAUD_EV_OBJECTACLMODIFIED	Cet événement se produit lorsque les autorisations de l'utilisateur ont été modifiées	30 jours
La connexion au Serveur d'administration principal a été établie	4117	KLSRV_EV_MASTER_SRV_CONNECTED		30 jours
La connexion au Serveur d'administration secondaire a été établie	4115	KLSRV_EV_SLAVE_SRV_CONNECTED	Pour en savoir plus, consultez l'article suivant : Création d'une hiérarchie des Serveurs d'administration : ajout d'un Serveur d'administration secondaire.	30 jours
Les bases de données ont été mises à jour	4144	KLSRV_UPD_BASES_UPDATED	Ce type d'événements se produit lorsque la tâche **Téléchargement des mises à jour sur le stockage du Serveur d'administration** termine la mise à jour des bases de données.	30 jours
L'appareil a été ajouté automatiquement au groupe	4101	KLSRV_EVENT_HOSTS_NEW_REDIRECTED	Ce type d'événements se produit lorsque les appareils ont été attribués à un groupe conformément aux règles de déplacement des appareils.	30 jours
L'appareil a été déplacé automatiquement selon la règle	1074	KLSRV_HOST_MOVED_WITH_RULE_EX	Les événements de ce type se produisent lorsque des appareils ont été déplacés vers des groupes d'administration à l'aide de règles de déplacement des appareils.	30 jours
L'appareil a été supprimé du groupe : longue absence d'activité sur le réseau	4104	KLSRV_INVISIBLE_HOSTS_REMOVED	Ce type d'événements se produit lorsque les appareils ont été automatiquement supprimés d'un groupe pour inactivité.	30 jours
L'ID d'instance FCM de l'appareil mobile a modifié	4137	KLSRV_GCM_DEVICE_REGID_CHANGED	Des événements de ce type se produisent lorsque le jeton Firebase Cloud Messaging a été modifié sur l'appareil. Pour en savoir plus sur la rotation des jetons FCM, veuillez consulter la documentation du service Firebase.	30 jours
Des fichiers à envoyer à Kaspersky pour analyse ont été détectés	4131	KLSRV_APS_FILE_APPEARED		30 jours
Fichier chargé sur le Serveur d'administration	4162	KLSRV_FILE_UPLOADED	Les événements de ce type se produisent lorsque l'Administrateur a chargé un fichier dans la liste **Gestion des ressources** → **Mobile** → **Apps & files** → **Files**.	30 jours
Fichier supprimé du Serveur d'administration	4163	KLSRV_FILE_REMOVED	Les événements de ce type se produisent lorsque l'Administrateur a supprimé un fichier de la liste **Gestion des ressources** → **Mobile** → **Apps & files** → **Files**.	30 jours

Nom affiché du type d'événement	ID de type d'événement	Type d'événement	Description	Durée de stockage par défaut
Fichier téléchargé sur l'appareil	4164	KLSRV_FILE_DOWNLOADED	Des événements de ce type se produisent dans les cas suivants : • L'Administrateur a téléchargé un fichier sur le poste de travail de l'administrateur depuis la liste de Web Console : **Gestion des ressources** → **Mobile** → **Apps & files** → **Files**. • Le fichier de la Web Console : **Gestion des ressources** → **Mobile** → **Apps & files** → **Files** a été téléchargé sur l'appareil sur lequel Kaspersky Endpoint Security for Android est installé.	
Impossible de télécharger le fichier sur l'appareil	4165	KLSRV_FILE_DOWNLOAD_FAILED	Des événements de ce type se produisent dans les cas suivants : • Une erreur s'est produite lorsque l'administrateur a tenté de télécharger un fichier depuis la liste de la Web Console (**Gestion des ressources** → **Mobile** → **Apps & files** → **Files**) sur le poste de travail de l'administrateur. • Une erreur s'est produite lors du téléchargement d'un fichier depuis la liste de la Web Console (**Gestion des ressources** → **Mobile** → **Apps & files** → **Files**) sur un appareil sur lequel Kaspersky Endpoint Security for Android est installé.	30 jours
Pour un des groupes des applications sous licence, le nombre d'installations autorisées est épuisé à plus de 90 %	4127	KLSRV_INVLICPROD_FILLED	Des événements de ce type se produisent lorsque le nombre d'installations pour des applications tierces incluses dans un groupe d'applications sous licence atteint 90 % de la valeur maximale autorisée indiquée dans les propriétés de la clé de licence. Vous pouvez répondre à l'événement des manières suivantes : • Si l'application tierce n'est pas utilisée sur certains des appareils administrés, supprimez l'application de ces appareils. • Si vous prévoyez que le nombre d'installations pour l'application tierce dépassera le nombre maximum autorisé prochainement, envisagez d'obtenir à l'avance une licence tierce pour un plus grand nombre d'appareils. Vous pouvez gérer les clés de licence d'applications tierces à l'aide des fonctionnalités des groupes d'applications sous licence.	30 jours
Un nouvel appareil a été détecté	4100	KLSRV_EVENT_HOSTS_NEW_DETECTED	Des événements de ce type se produisent lorsque de nouveaux appareils en réseau ont été découverts.	30 jours

Nom affiché du type d'événement	ID de type d'événement	Type d'événement	Description	Durée de stockage par défaut
Clé de licence utilisée à plus de 90 %	4097	KLSRV_EV_LICENSE_CHECK_90	Ce type d'événements se produit si le serveur d'administration détecte que certaines restrictions de la 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 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.	30 jours
Le certificat du Serveur d'administration pour les appareils mobiles est créé	6126	KLSRV_EV_SRV_CERT_RESERVE_CREATED	Cet événement se produit lorsqu'un certificat de Serveur d'administration a été créé.	30 jours
Les mises à jour ont bien été copiées dans le dossier indiqué	4122	KLSRV_UPD_REPL_OK	Ce type d'événements se produit lorsque la tâche **Téléchargement des mises à jour sur le stockage du Serveur d'administration** termine la copie des fichiers dans le dossier indiqué.	30 jours

Les événements **Certificat de réserve créé** et **Renouvellement du certificat** sont publiés automatiquement par le Serveur d'administration et affichés dans la Console d'administration uniquement quand sont exécutées les opérations correspondant aux événements pour les certificats de Serveur d'administration des appareils mobiles et les appareils UEFI.

Événements de l'Agent d'administration

Cette section contient des informations sur les événements liés à l'agent d'administration.

Événements liés aux erreurs de fonctionnement de l'Agent d'administration

Le tableau suivant reprend les événements de l'Agent d'administration de Kaspersky Security Center Linux, regroupés par niveau de gravité **Erreur de fonctionnement**.

Pour chaque événement pouvant être généré par une application, vous pouvez spécifier les paramètres de notification et les paramètres de stockage sous l'onglet **Configuration des événements** dans la stratégie de l'application. Si vous souhaitez configurer les paramètres de notification pour tous les événements à la fois, configurez les paramètres de notification généraux dans les propriétés du Serveur d'administration.

Nom affiché du type d'événement	ID de type d'événement	Type d'événement	Description	Durée de stockage par défaut
Il est impossible d'installer les certificats racine	7728	KLNAG_EV_ROOT_CERT_INSTALL_ERR	L'événement contient la description de l'erreur d'installation des certificats.	30 jours
Échec de l'installation de la mise à jour du logiciel tiers	7697	KLNAG_EV_3P_PATCH_INSTALL_ERROR	Des événements de ce type se produisent si les fonctionnalités de la gestion des vulnérabilités et des correctifs sont en cours d'utilisation, et si la mise à jour des logiciels tiers n'a pas réussi. Vérifiez si le lien vers le logiciel tiers est valide. Lisez la description de l'événement.	30 jours
Échec de l'installation des mises à jour Windows Update	7717	KLNAG_EV_WUA_INSTALL_ERROR	Ce type d'événements se produit si les mises à jour Windows échouent. Lisez la description de l'événement. Recherchez l'erreur dans la base de connaissance Microsoft. Contactez le Support Technique de Microsoft si vous ne parvenez pas à résoudre le problème vous-même.	30 jours
Impossible de supprimer les certificats racine	7730	KLNAG_EV_ROOT_CERT_REMOVE_ERR	L'événement contient la description de l'erreur de suppression des certificats.	30 jours
Impossible de restaurer le fichier sudoers à la valeur de référence	7726	KLNAG_EV_SUDOER_RESTORED_ERR	L'événement contient la description de l'erreur de remplacement du fichier sudoers.	30 jours
Erreur d'installation de la mise à jour	7702	KLNAG_EV_PATCH_INSTALL_ERROR	Des événements de ce type se produisent si l'Installation automatique des mises à jour et des correctifs pour les modules de Kaspersky Security Center Linux ne réussit pas. L'événement ne concerne pas les mises à jour des applications Kaspersky administrées. Lisez la description de l'événement. Cet événement peut être dû à un problème Windows sur le serveur d'administration. Si la description mentionne un problème de configuration Windows, résolvez le problème.	30 jours
Gestion des utilisateurs : erreurs	7723	KLNAG_EV_USR_MNG_ERR	Événement d'avertissement général.	30 jours

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
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
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 fichier sudoers ne correspond pas à la valeur de référence	7724	KLNAG_EV_SUDOER_DIFFERENT	Des événements de ce type se produisent lorsqu'il existe une discordance entre le fichier sudoers et le fichier de référence.	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
Gestion des utilisateurs : avertissements	7722	KLNAG_EV_USR_MNG_WRN	Événement d'avertissement général.	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
Certificat reçu pour le port HTTPS du serveur Internet	—	WEB_SERVER_CERTIFICATE_RENEWED	30 jours
L'appareil a été autorisé	7711	KLNAG_EV_NAC_HOST_AUTHORIZED	30 jours
Un nouvel appareil a été détecté	7710	KLNAG_EV_NAC_DEVICE_DISCOVERED	30 jours
L'appareil a été supprimé	7709	KLNAG_EV_DEVICE_REMOVE	30 jours
L'installation de la mise à jour du module logiciel est lancée	7700	KLNAG_EV_PATCH_INSTALL_STARTING	30 jours
Le proxy KSN a démarré. La vérification de la disponibilité de KSN a réussi	7719	KSNPROXY_STARTED_CON_CHK_OK	30 jours

Nom affiché du type d'événement	ID de type d'événement	Type d'événement	Durée de stockage par défaut
Le serveur proxy KSN a été arrêté	7720	KSNPROXY_STOPPED	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
Certificats racine installés	7727	KLNAG_EV_ROOT_CERT_INSTALLED	30 jours
Certificats racine supprimés	7729	KLNAG_EV_ROOT_CERT_REMOVED	30 jours
Le fichier sudoers a été restauré avec succès à sa valeur de référence	7725	KLNAG_EV_SUDOER_RESTORED	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
La mise à jour des modules de l'application a bien été appliquée	7699	KLNAG_EV_PATCH_INSTALLED_SUCCESSFULLY	30 jours
Gestion des utilisateurs : informations	7721	KLNAG_EV_USR_MNG_INF	30 jours
Serveur Internet lancé sur l'hôte	—	WEB_SERVER_STARTED	30 jours
Le Serveur Internet s'est arrêté sur l'hôte	—	WEB_SERVER_STOPPED	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

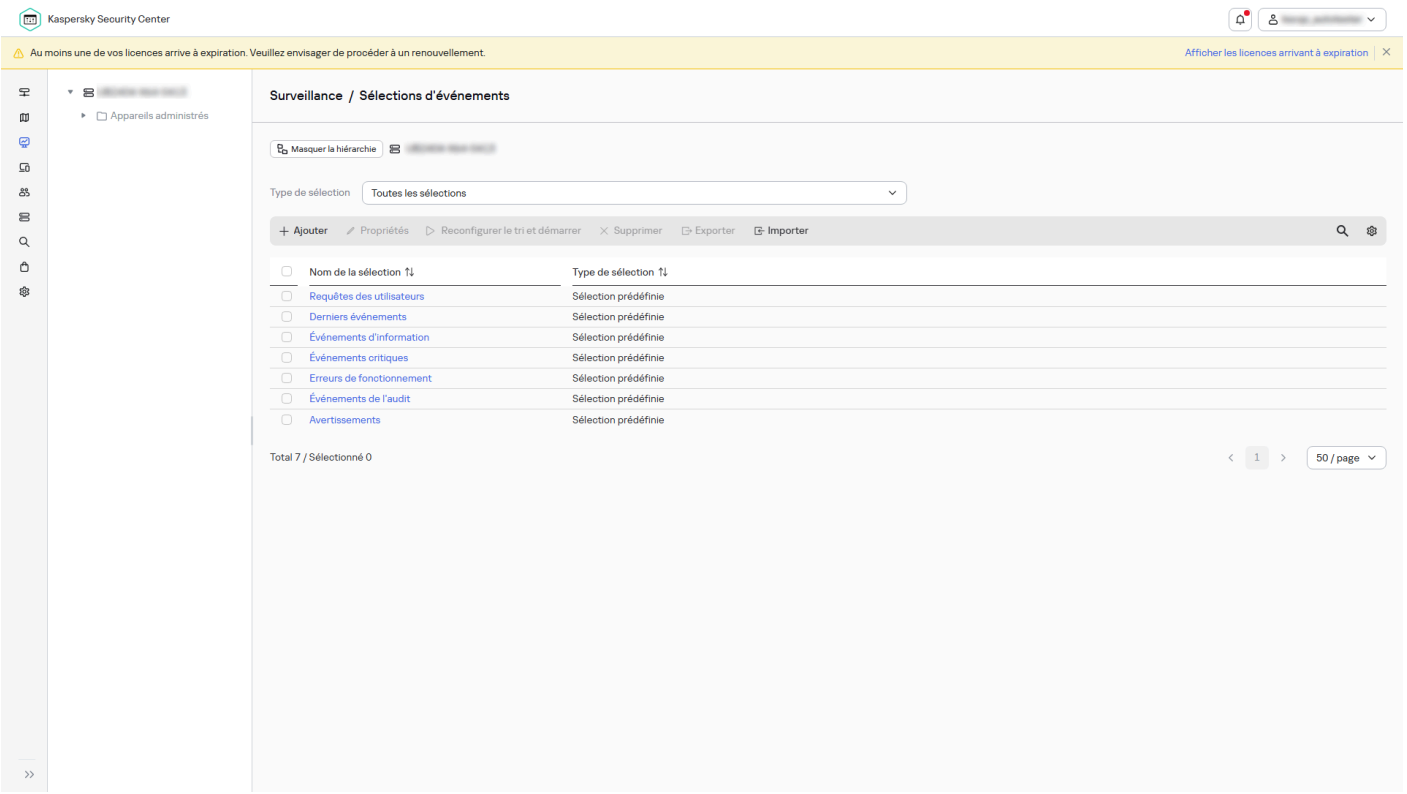
Utilisation des sélections d'événements

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**, en cliquant sur **Sélections d'événements**.



La liste des 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.

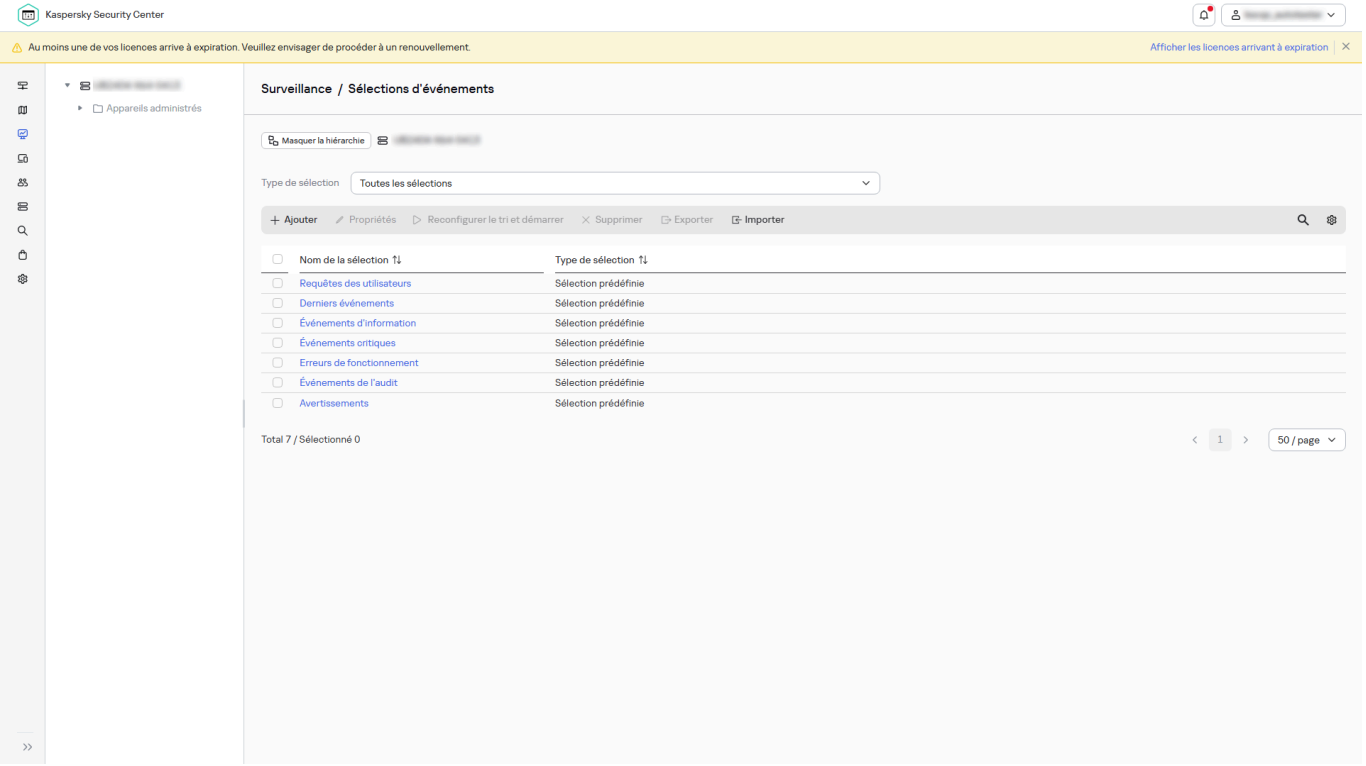
Vous pouvez réaliser les opérations suivantes :

- 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 :

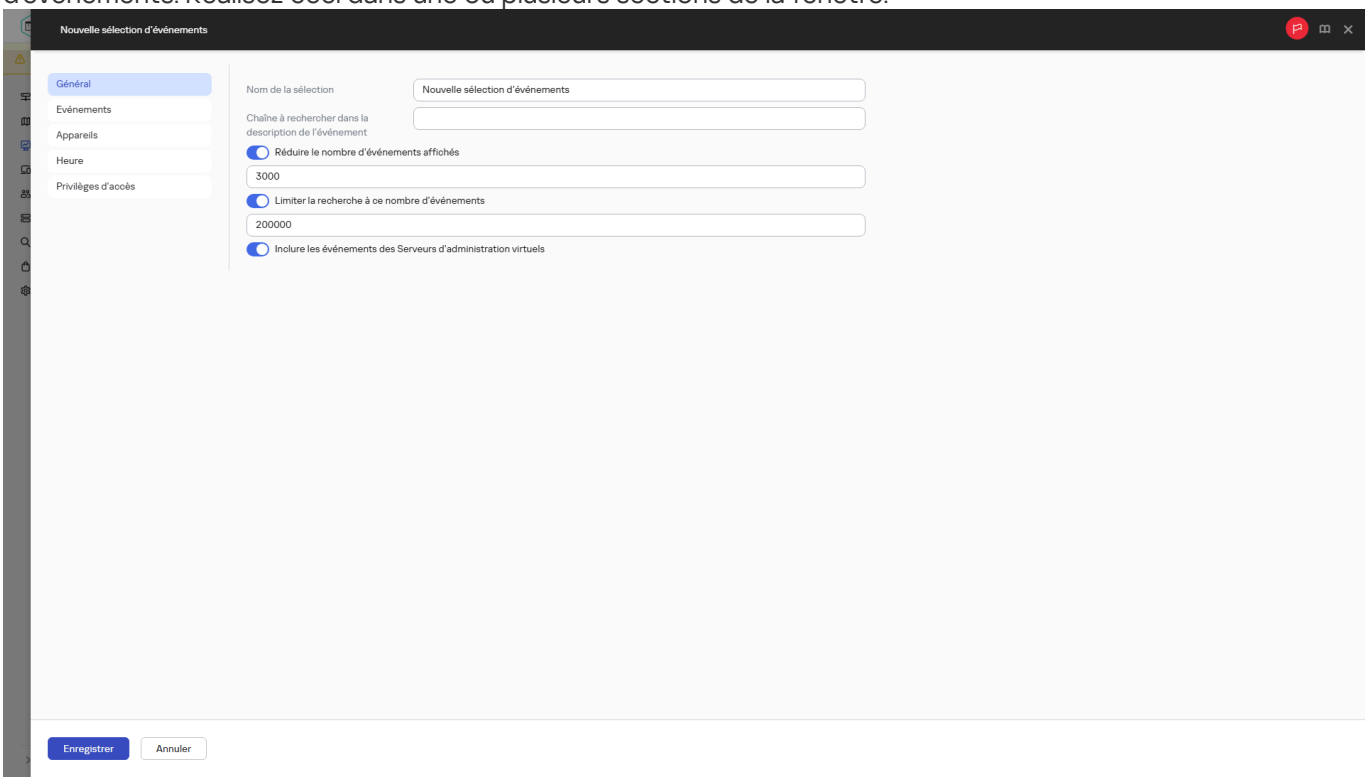
1. Dans le menu principal, accédez à **Surveillance** → **Sélections d'événements**.



La liste des 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.



Création d'une sélection d'événements

4. Cliquez sur **Enregistrer** pour enregistrer les modifications.

   Une 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.

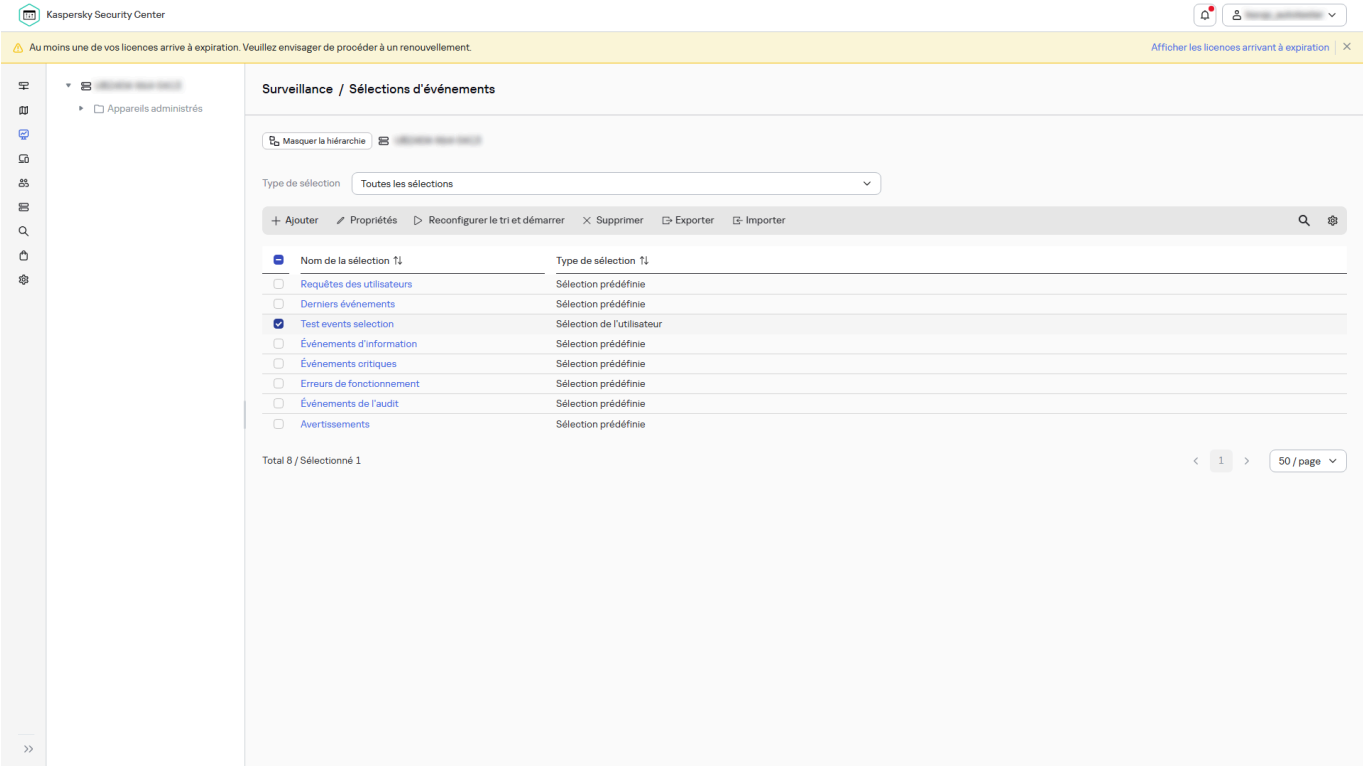
Si vous n'avez pas décoché la case **Accéder au résultat de la sélection**, les résultats de la sélection d'événements sont affichés. Dans le cas contraire, la nouvelle sélection d'événements apparaît dans a liste des sélection d'événements.

Édition d'une sélection d'événements

Pour modifier une sélection d'événements, procédez comme suit :

1. Dans le menu principal, accédez à **Surveillance** → **Sélections d'événements**.

2. Cochez la case en regard de la sélection d'événements que vous souhaitez modifier.



La liste des sélections d'événements

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 **Enregistrer** pour enregistrer les modifications.

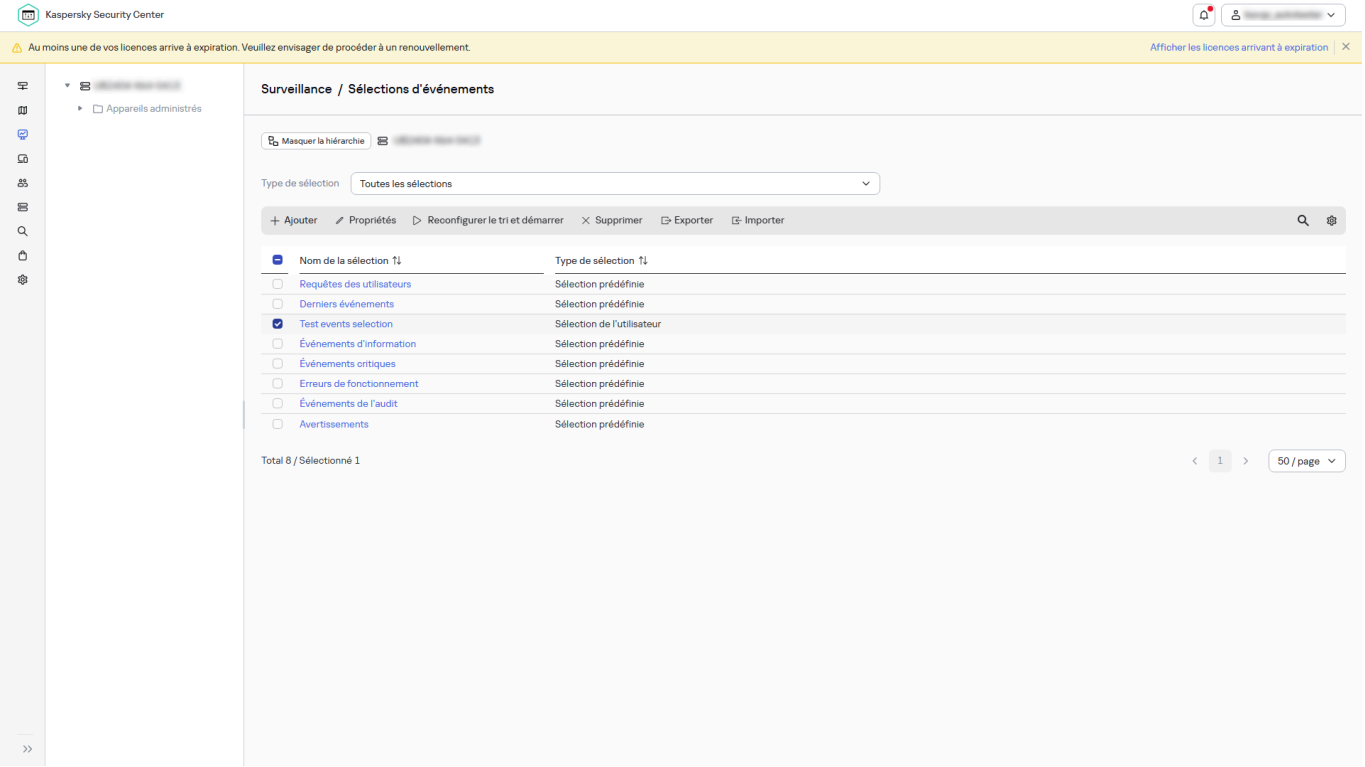
La sélection d'événements modifiée apparaît dans la liste.

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** → **Sélections d'événements**.

2. Cochez la case en regard de la sélection d'événements que vous souhaitez lancer.



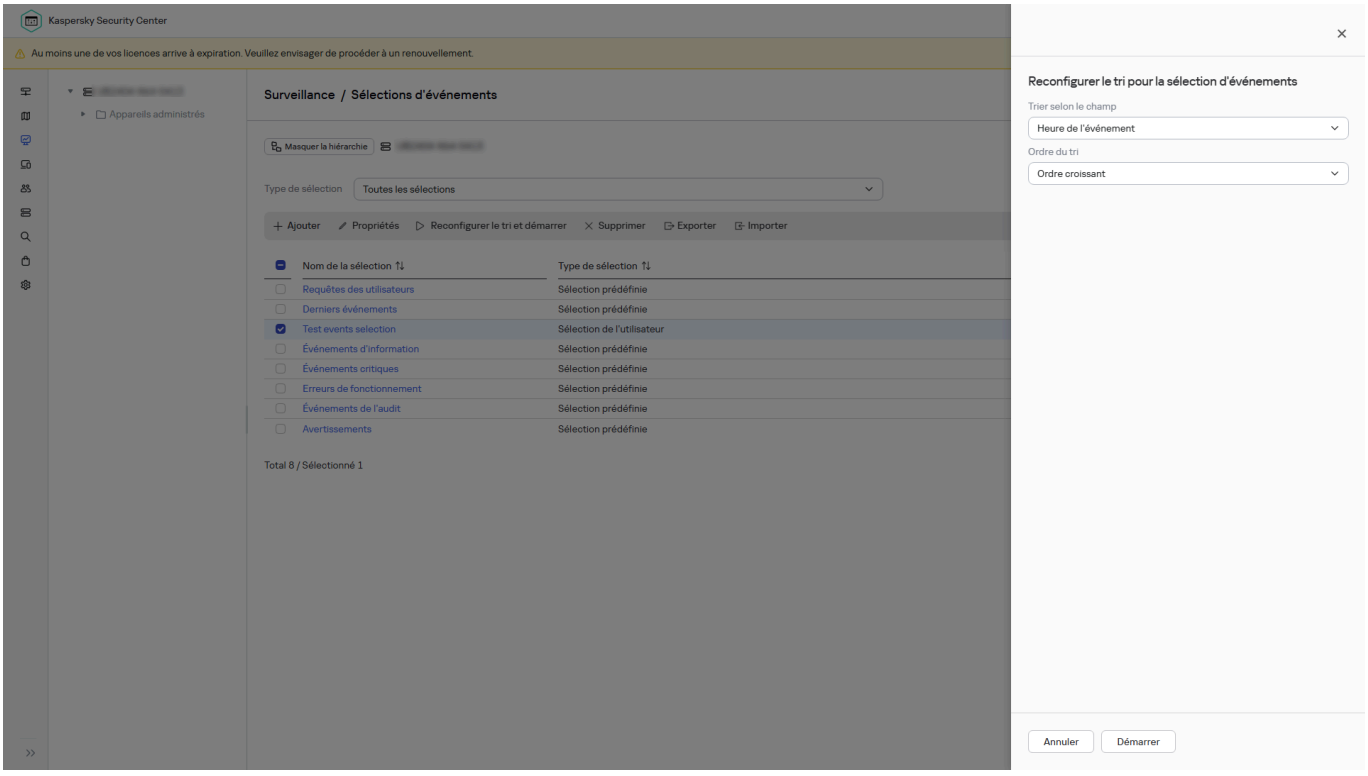
La liste des sélections d'événements

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.

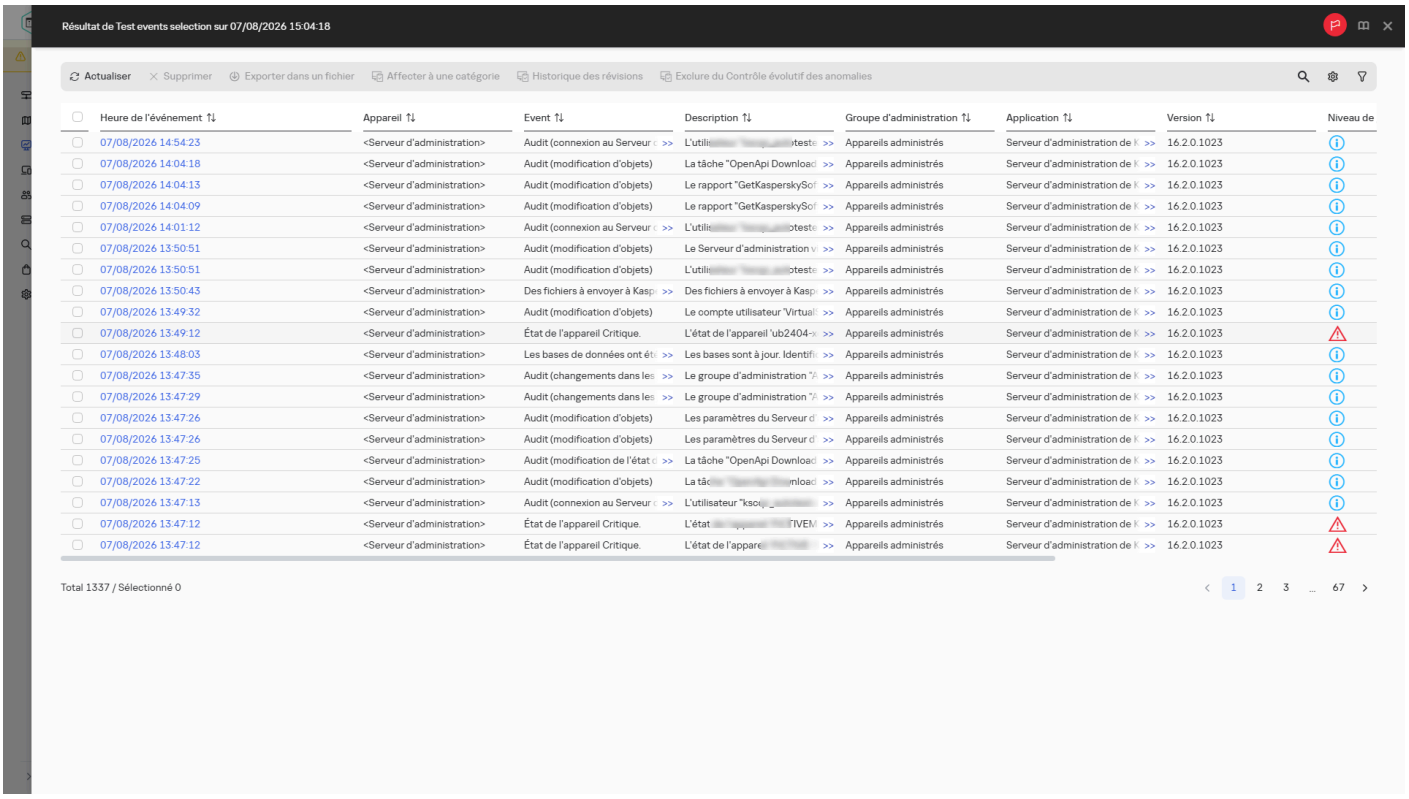


Spécification des paramètres de tri de la sélection d'événements

  a. 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.



Le résultat de la sélection d'événements

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** → **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** → **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.

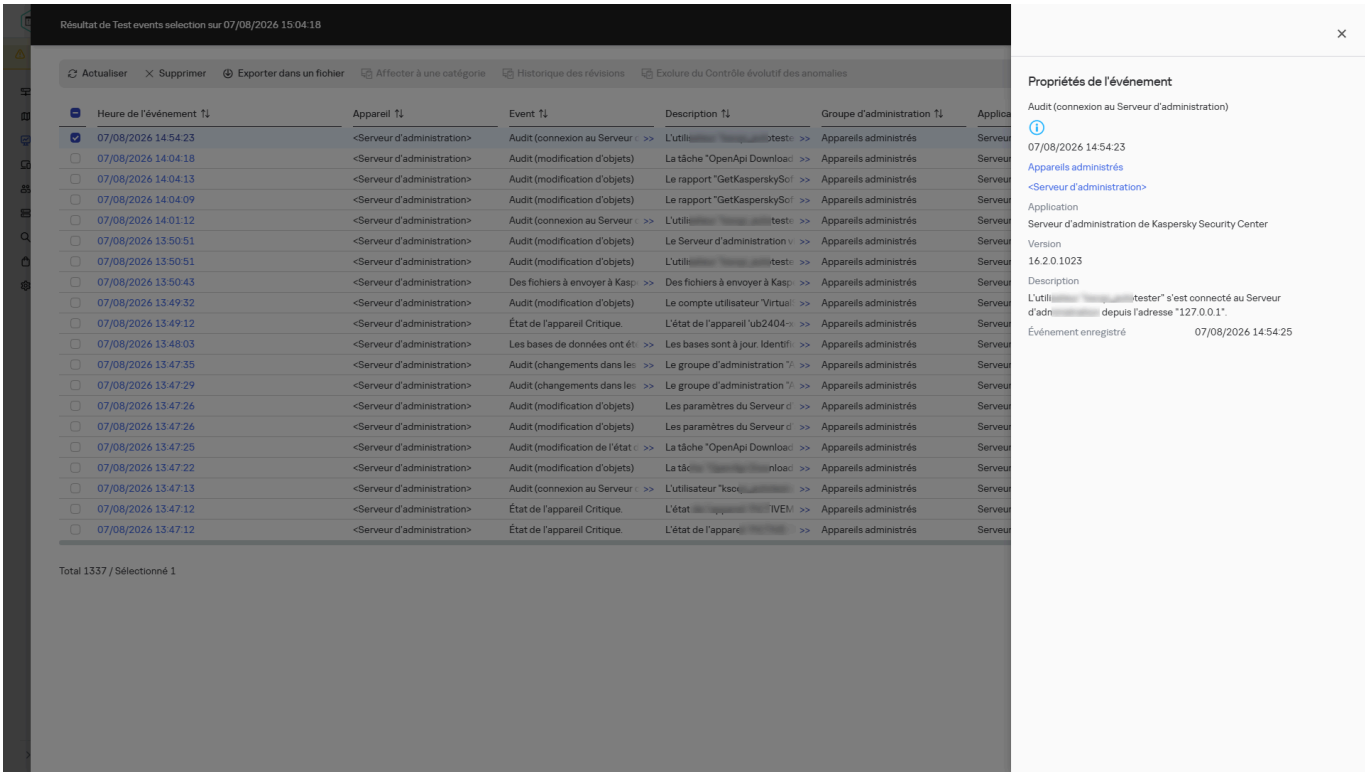
Si la sélection d'événements nouvellement importée a un nom identique à celui d'une sélection d'événements existante, le nom de la sélection importée est suivi de l'index **(<numéro de séquence suivant>)**, par exemple : **(1)**, **(2)**.

Affichage des zones de détails des événements

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.



La fenêtre de propriétés des événements

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'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

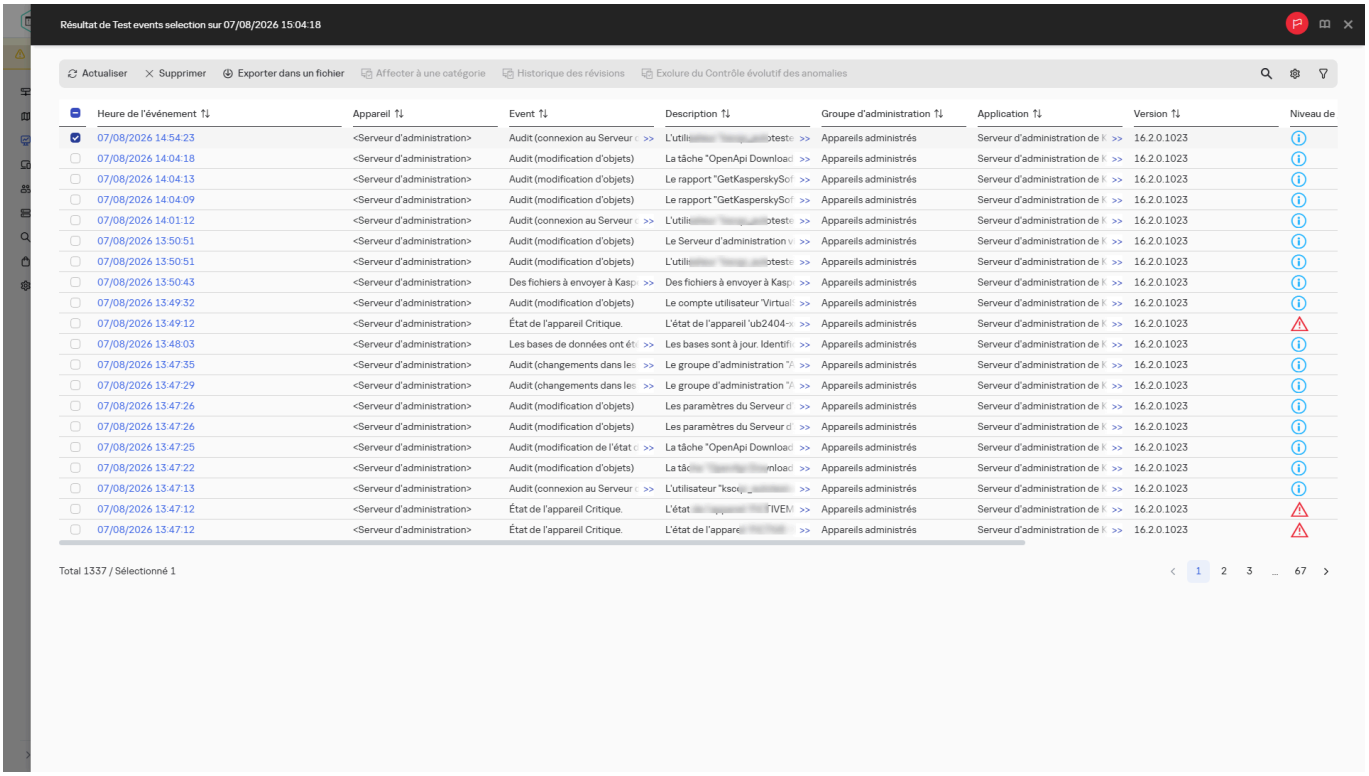
Exportation des événements dans un fichier

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.



Le résultat de 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 des événements d'une sélection d'événements, procédez comme suit :

1. Démarrage d'une sélection d'événements.
2. Sélectionnez les événements :
   - Si vous souhaitez supprimer un ou plusieurs événements, cochez les cases situées à côté de ceux-ci.
   - Si vous souhaitez supprimer tous les événements de la page actuelle, cochez la case située au-dessus de la liste des événements, puis cliquez sur l'option **Tout sélectionner sur la page actuelle**.
   - Si vous souhaitez supprimer tous les événements d'une sélection, cochez la case située au-dessus de la liste des événements, puis cliquez sur l'option **Tout sélectionner**.
3. Cliquez sur le bouton **Supprimer**.
4. Dans la fenêtre qui s'ouvre, cliquez sur **Supprimer**.

Pour supprimer des événements de la liste des événements d'un appareil, procédez comme suit :

1. Ouvrez la liste des appareils.
   - Pour les appareils administrés : **Gestion des ressources** → **Ressources (Appareils)**.
   - Pour les appareils non définis : **Découverte et déploiement** → **Appareils non définis**.
2. Dans la liste des appareils, cliquez sur le lien portant le nom de l'appareil requis, puis passez à l'onglet **Événements**.
3. Sélectionnez les événements :
   - Si vous souhaitez supprimer un ou plusieurs événements, cochez les cases situées à côté de ceux-ci.
   - Si vous souhaitez supprimer tous les événements de la page actuelle, cochez la case située au-dessus de la liste des événements, puis cliquez sur l'option **Tout sélectionner sur la page actuelle**.
   - Si vous souhaitez supprimer tous les événements d'une sélection, cochez la case située au-dessus de la liste des événements, puis cliquez sur l'option **Tout sélectionner**.
4. Cliquez sur **Supprimer**, puis confirmez l'action.
5. Dans la fenêtre qui s'ouvre, cliquez sur **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** → **Sélections d'événements**.
2. Cochez les cases en regard des sélections d'événements que vous souhaitez supprimer.
3. Cliquez sur le bouton **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 **Gestion des ressources** → **Stratégies**.
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 conservation des événements en cliquant sur le nom du Serveur d'administration.
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 d'administration 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 d'administration 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, 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 le nom du Serveur d'administration.

   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 le nom du Serveur d'administration.

   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.

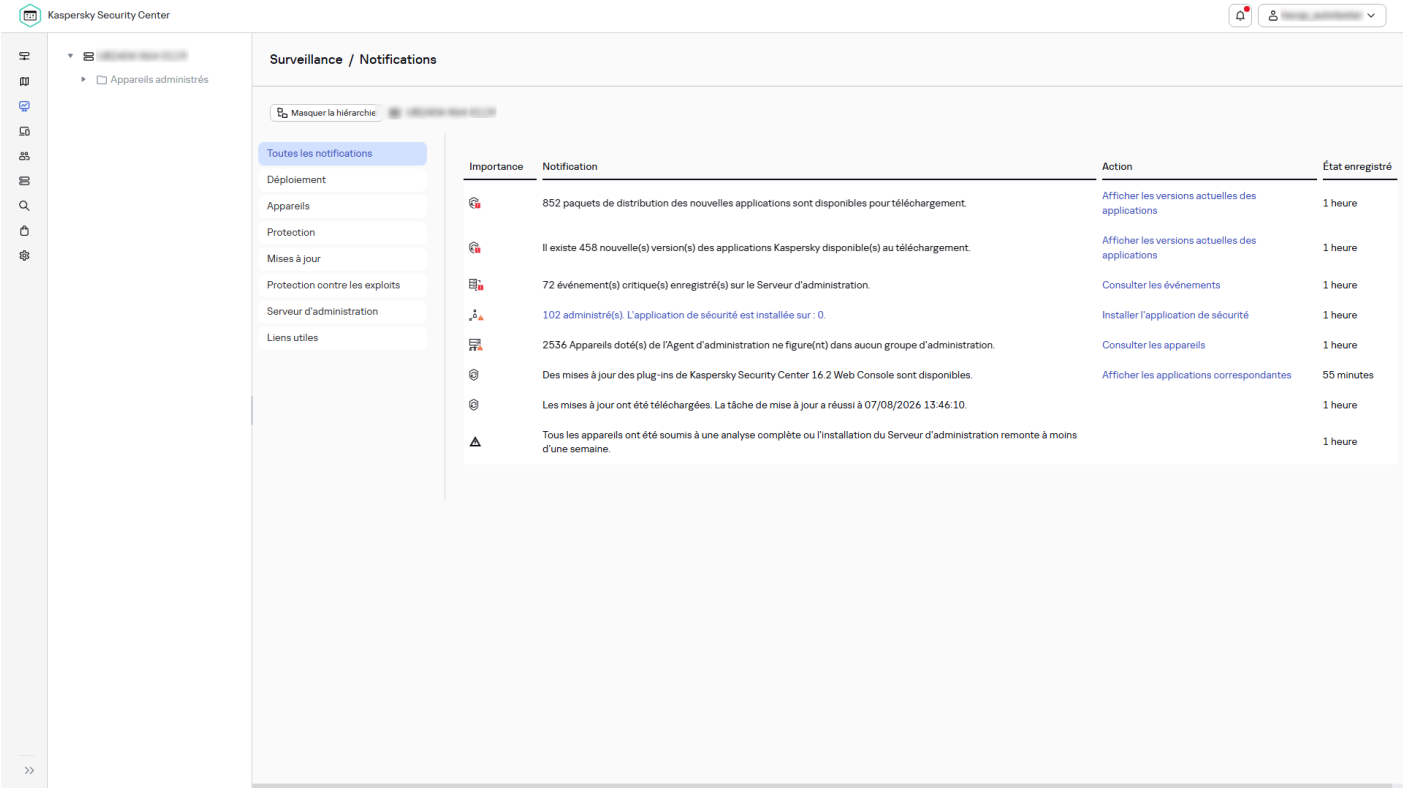
Quand le Serveur d'administration supprime les anciens événements, il ne peut pas enregistrer les nouveaux événements dans la base de données. Durant cette période, les informations sur les événements rejetés sont écrites dans le journal du système d'exploitation. Les nouveaux événements sont placés 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.



La liste des notifications

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 :

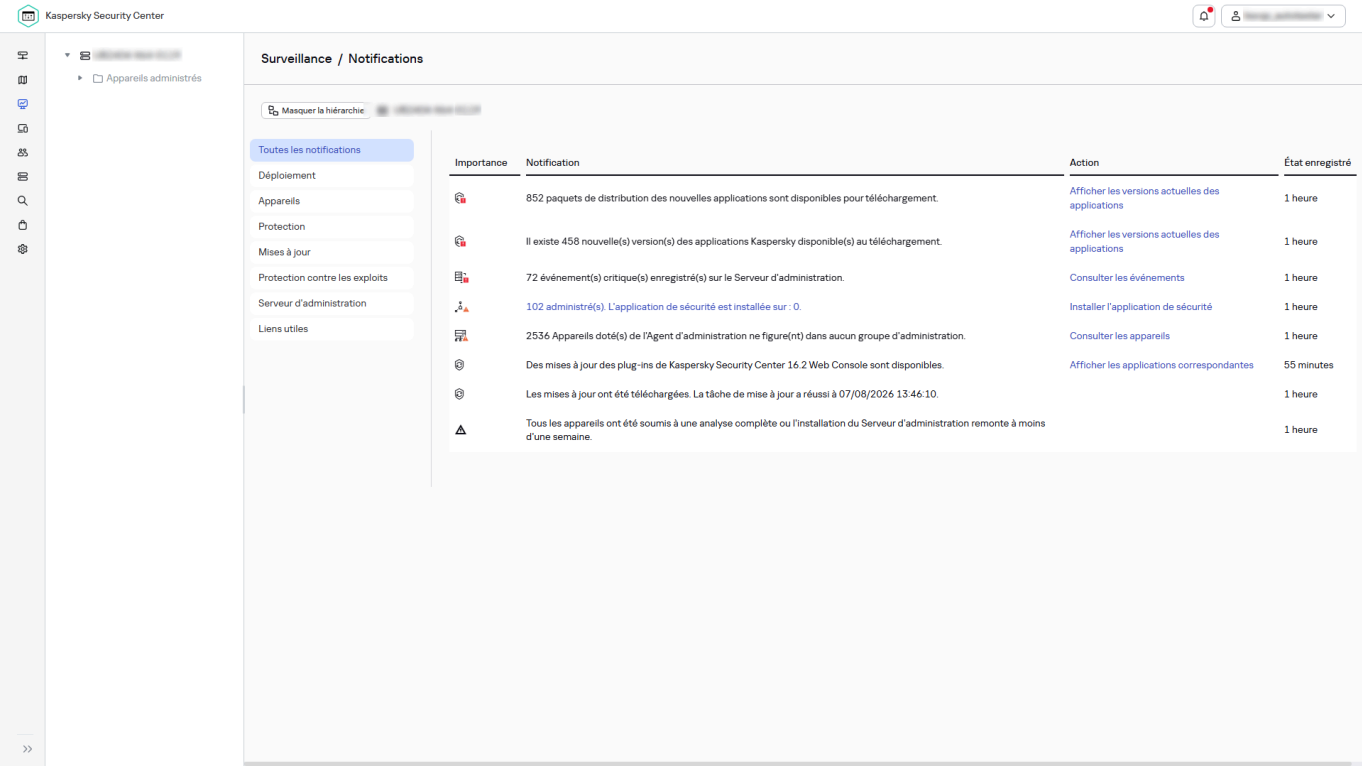
- Dans la section **Surveillance** → **Notifications**. Ici, vous pouvez afficher des notifications concernant les catégories prédéfinies.
- Dans une fenêtre séparée qui peut être ouverte, quelle que soit la section en cours d'utilisation. Dans ce cas, vous pouvez marquer les notifications comme révisées.
- Dans le widget **Notifications en fonction du niveau de gravité sélectionné**, dans la section **Surveillance** → **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** → **Notifications**.

   La catégorie **Toutes les notifications** est sélectionnée dans le volet gauche et toutes les notifications s'affichent dans le volet droit.



La liste des notifications

2. Dans le volet gauche, sélectionnez une des catégories :

   - **Déploiement**
   - **Appareils**
   - **Protection**
   - **Mises à jour**

     Cette notification inclut les notifications sur les applications Kaspersky disponibles au téléchargement, les notifications sur les mises à jour de la base de données antivirus qui ont été téléchargées, ainsi que les notifications sur les appareils (le cas échéant) qui doivent être redémarrés après une mise à jour de l'Agent d'administration.
   - **Protection contre les exploits**
   - **Serveur d'administration**.

     Cela inclut les événements concernant uniquement le Serveur d'administration.

- **Liens utiles**.

  Cela inclut des liens vers des ressources Kaspersky, par exemple le Support technique de Kaspersky, le Forum Kaspersky, la page de renouvellement de la licence ou l'Encyclopédie IT de Kaspersky.

Une liste des notifications de la catégorie sélectionnée s'affiche. La liste contient les éléments suivants :

- Icône liée au sujet de la notification : déploiement (), protection (), mises à jour (), administration d'appareils (), Protection contre les Exploits (), Serveur d'administration ().
- Niveau d'importance des notifications. Les notifications des niveaux d'importance suivants sont affichées : **Notifications critiques** (), **Notifications d'avertissement** (), **Notifications d'information**. Les notifications dans la liste sont regroupées par niveau d'importance.
- **Notification**. Contient une description de la notification.
- **Action**. Contient un lien vers une action rapide que nous vous recommandons. Par exemple, en cliquant sur ce lien, vous pouvez accéder au stockage et installer les applications de sécurité sur les appareils ou afficher une liste des appareils ou des événements. Après que vous avez effectué l'action recommandée pour la notification, cette notification passe à l'état *révisé*.
- **État enregistré**. Contient le nombre de jours ou écoulé(e)s depuis que la notification a été enregistrée sur le Serveur d'administration.

Pour consulter les notifications à l'écran dans une fenêtre séparée par niveau d'importance :

1. Dans le coin supérieur droit de Kaspersky Security Center Web Console, cliquez sur l'icône drapeau ().

   Si l'icône drapeau a un point rouge, cela signifie que certaines notifications n'ont pas été révisées.

   Une fenêtre s'ouvre avec la liste des notifications. Par défaut, l'onglet **Toutes les notifications** est sélectionné et les notifications sont regroupées par niveau d'importance : *Critique*, *Attention* et *Information*.

2. Sélectionnez l'onglet **Système**.

   La liste des notifications de niveau d'importance *Critique* () et *Attention* () s'affiche. La liste des notification inclut les éléments suivants :

   - Marqueur de couleur. Les notifications critiques sont marquées en rouge. Les notifications d'avertissement sont marquées en jaune.
   - Icône indiquant le sujet de la notification : déploiement (), protection (), mises à jour (), administration d'appareils (), Protection contre les Exploits (), Serveur d'administration ().
   - Description de la notification.
   - L'icône en forme de coche. 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**.

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**.

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). 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*. 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. • 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.

Condition	Description de la condition	Valeurs possibles
Durée requise depuis le redémarrage	L'appareil est visible sur le réseau, mais une application a demandé son redémarrage depuis plus longtemps que la durée indiquée.	Plus de 0 minute.
Raison du redémarrage	L'appareil est visible sur le réseau, mais une application nécessite son redémarrage pour l'une des raisons sélectionnées.	• Raison de redémarrage inconnue • L'application ne peut s'exécuter avant le redémarrage • Le redémarrage est requis pour terminer la mise à jour. L'application est exécutée • Le redémarrage est requis pour le lancement de la mise à jour • Le redémarrage est requis pour la fin de l'analyse ou la désinfection • Le redémarrage est requis pour terminer l'installation/la désinstallation à distance • Fin de chiffrement des données sur le disque
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.
Des vulnérabilités dans les applications ont été détectées	L'appareil est visible sur le réseau, et l'Agent d'administration est installé sur l'appareil, mais la tâche *Recherche de vulnérabilités et de mises à jour requises* a détecté des vulnérabilités avec le niveau de gravité indiqué dans les applications installées sur l'appareil.	• Critique • Élevé. • Normal. • Ignorer s'il est impossible de fermer la vulnérabilité. • Ignorer si la mise à jour a été désignée à l'installation.
La licence a expiré	L'appareil est visible sur le réseau, mais la licence a expiré.	• Le bouton radio est éteint. • Le bouton radio est allumé.
La licence expire bientôt	L'appareil est visible sur le réseau, mais la licence expirera sur l'appareil dans moins de jours que le nombre indiqué.	Plus de 0 jour.

Condition	Description de la condition	Valeurs possibles
La vérification de mises à jour Windows Update n'a pas eu lieu depuis longtemps	L'appareil est visible sur le réseau, mais la tâche *Recherche de vulnérabilités et des mises à jour requises* n'a plus été exécutée dans la période indiquée.	Plus de 1 jour.
État de chiffrement non valide	L'Agent d'administration est installé sur l'appareil mais le résultat du chiffrement de l'appareil est égal à la valeur indiquée.	• Ne correspond pas à la stratégie à cause du refus de l'utilisateur (uniquement pour les appareils externes). • Ne correspond pas à la stratégie à cause de l'erreur. • Stratégie en cours d'application – le redémarrage est requis. • La stratégie de chiffrement n'est pas définie. • Non pris en charge. • Stratégie en cours d'application.
Les paramètres de l'appareil mobile ne correspondent pas à la stratégie	Les paramètres de l'appareil mobile se distinguent des paramètres définis dans la stratégie Kaspersky Endpoint Security for Android lors de l'analyse des règles de concordance.	• Le bouton radio est éteint. • Le bouton radio est allumé.
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. Les appareils administrés peuvent voir leur état défini par les applications administrées, indépendamment des paramètres de Kaspersky Security Center Linux. Une fois que cet état renvoie l'un des états définis par Kaspersky Security Center Linux, le Serveur d'administration attribue à un appareil administré l'état le plus critique parmi ceux renvoyés par l'application administrée et attribués par le Serveur d'administration. Les états définis par les applications gérées sont accompagnés de descriptions transférées par les applications gérées. Vous pouvez consulter les descriptions dans la liste des appareils administrés, dans la colonne **Description de l'état**.	• 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.

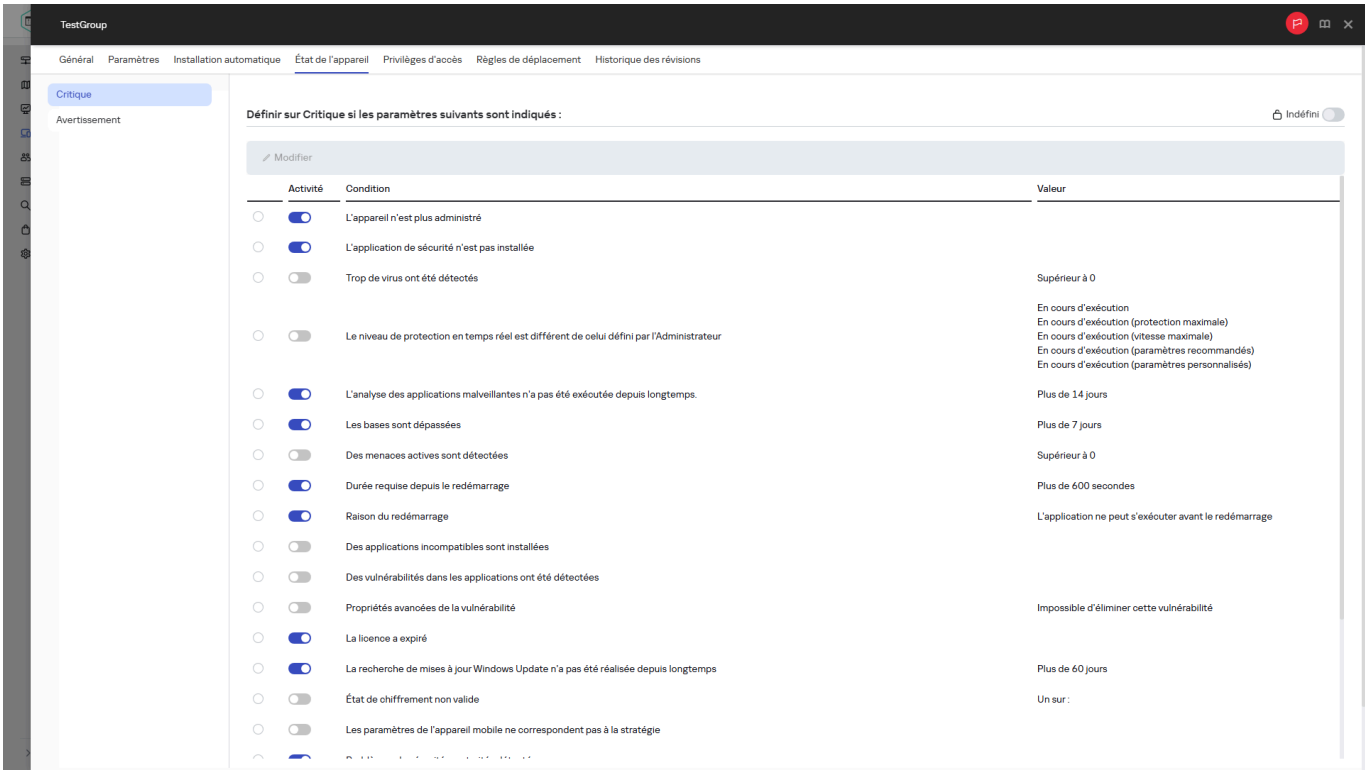
Configuration de la permutation des états des appareils

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 **Gestion des ressources** → **Hiérarchie des groupes**.
2. Accédez aux propriétés du groupe d'administration pour lequel vous souhaitez modifier l'état des appareils de l'une des manières suivantes :
   - Cliquez sur le nom du groupe d'administration.
   - Cliquez sur le bouton **Afficher la hiérarchie** en haut de la page. Dans le panneau de navigation qui s'ouvre, placez le curseur de la souris sur le nom du groupe requis, puis cliquez sur l'icône des paramètres (⚙).

   La fenêtre des propriétés du groupe d'administration s'ouvre.
3. Dans la fenêtre des propriétés, sélectionnez l'onglet **État de l'appareil**.
4. Dans le volet de gauche, sélectionnez **Critique**.
5. Dans le volet droit, dans la section **Définir sur Critique si les paramètres suivants sont indiqués**, 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**.
10. Cliquez sur **Enregistrer** pour enregistrer les modifications.

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 **Gestion des ressources** → **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 sur Avertissement si les paramètres suivants sont indiqués,** 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**.
10. Cliquez sur **Enregistrer** pour enregistrer les modifications.

Lorsque certaines conditions spécifiées sont remplies, l'appareil administré se voit affecter l'état *Avertissement*.

Configuration des paramètres d'envoi des notifications

Vous pouvez configurer une notification à propos des événements qui se produisent dans Kaspersky Security Center 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 le nom du Serveur d'administration.

   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 sont indépendants l'un de l'autre. L'ordre de chargement des fichiers n'a pas d'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**, saisissez l'objet de l'email à l'aide des paramètres de substitution, par exemple : `[KSC-SAMARA-1] [%SEVERITY%] %EVENT%`. Exemple d'objet d'email en cas de détection d'une menace : `[KSC-SAMARA-1] [Critical] Threat detected`. 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.

Exemple de valeur de champ

```
Sender - KSC-SAMARA-1

Host: %COMPUTER%

Product: %KL_PRODUCT%

Version: %KL_VERSION%

Occurred at: %RISE_TIME%

Event: %EVENT%

Details:

%DESCR%
```

La chaîne `Sender` est facultative. Par exemple, si vous disposez de plusieurs Serveurs d'administration, vous pouvez indiquer le nom du Serveur d'administration dont provient la notification : `Sender - KSC-SAMARA-1`.

Exemple de texte de notification :

```
Sender - KSC-SAMARA-1

Host: nb-123456.example.net

Product: Kaspersky Endpoint Security 12.5 for Linux

Version: 12.5.0.1569

Occurred at: 2026-08-17T13:15:36

Event: Threat detected

Details:
```

```
Initiator: Product; Task type: ODS; ID of running task: 107; User receiving
access: root; Object type: File; File owner: user; Detection certainty: Sure;
File: /home/user/eicar_com.zip//eicar.com; Detected object name: EICAR-Test-
File; Detected object type: Virware; MD5 hash: <hash>; Unique ID: <ID>
```

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 de réseau Windows (nom NetBIOS) de l'appareil
- Nom complet du serveur SMTP

Dans le champ **Port du serveur SMTP**, spécifiez le numéro d'un port de communication du serveur SMTP. Le numéro de port par défaut est 25.

Si vous activez l'option **Utiliser l'authentification &ESMTP**, vous pouvez spécifier les paramètres d'authentification ESMTP dans les champs **Nom d'utilisateur** et **Mot de passe**. Par défaut, cette option est décochée et les paramètres d'authentification ESMTP ne sont pas disponibles.

Vous pouvez indiquer les paramètres TLS de connexion au serveur SMTP :

- **Ne pas utiliser le protocole TLS**

Vous pouvez choisir cette option si vous désactivez le chiffrement des emails.

- **Utiliser le protocole TLS si le serveur SMTP le permet**

Vous pouvez choisir cette option si vous voulez utiliser une connexion TLS pour un serveur SMTP. Si le serveur SMTP n'est pas compatible avec TLS, le Serveur d'administration connecte le serveur SMTP sans utiliser TLS.

- **Utiliser toujours le protocole TLS, vérifier la validité du certificat du serveur**

Vous pouvez choisir cette option si vous voulez utiliser les paramètres d'authentification TLS. Si le serveur SMTP n'est pas compatible avec TLS, le Serveur d'administration ne peut pas connecter le serveur SMTP.

Nous vous recommandons d'utiliser cette option pour améliorer la protection de la connexion avec un serveur SMTP. Si vous choisissez cette option, vous pouvez définir les paramètres d'authentification pour une connexion TLS.

Si vous sélectionnez la valeur **Utiliser toujours le protocole TLS, vérifier la validité du certificat du serveur**, vous pouvez définir un certificat pour l'authentification du serveur SMTP et choisir si vous souhaitez activer la communication via n'importe quelle version de TLS ou uniquement via TLS 1.2 ou les versions ultérieures. Vous pouvez également spécifier un certificat pour l'authentification du client sur le serveur SMTP.

Vous pouvez préciser le fichier de certificat du serveur SMTP en cliquant sur le lien **Indiquer les certificats** :

Vous pouvez recevoir un fichier avec la liste des certificats de l'autorité de certification de confiance et charger le fichier sur le Serveur d'administration. Kaspersky Security Center 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 le lien **Configurer la limite du nombre de notifications** pour indiquer le nombre maximum de notifications que l'application peut envoyer pendant l'intervalle de temps spécifié.

Cliquez sur **Envoyer un message d'essai** pour vérifier si vous avez correctement configuré les notifications : l'application envoie une notification de test au destinataire que vous avez indiqué.

- **Fichier exécutable à exécuter**

Le fichier exécutable doit contenir les variables d'environnement de l'événement que vous souhaitez transmettre à l'Administrateur.

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.

Exemple de valeur du champ :

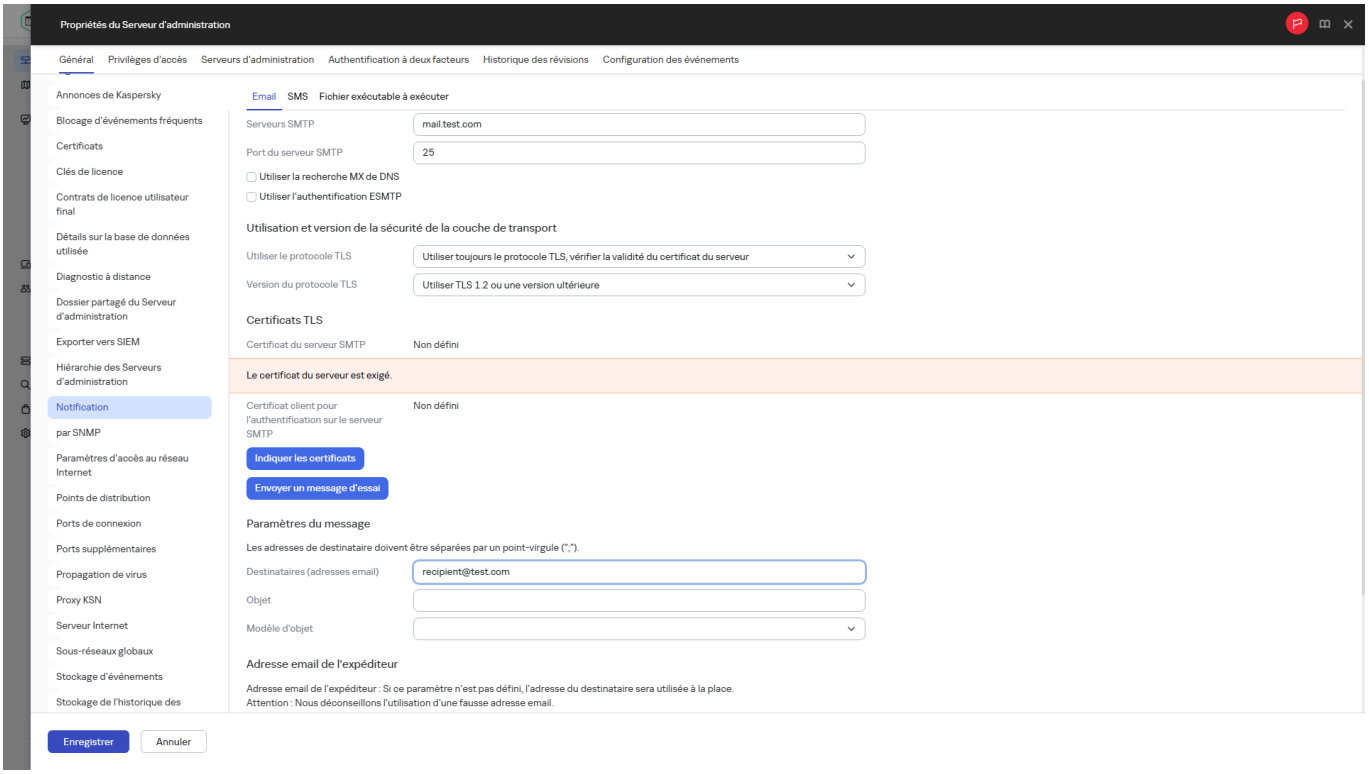
```
/opt/scripts/notifications.sh
```

Le fichier doit être préparé à l'avance en spécifiant les paramètres de remplacement correspondant aux informations sur l'événement qui seront envoyées dans le message. Le dossier et le fichier doivent se trouver sur le Serveur d'administration.

Exemple de script de test ou de débogage :

```
#!/usr/bin/env bash
touch /tmp/ksc_notification.txt
echo "$RISE_TIME $COMPUTER $EVENT" >> /tmp/ksc_notification.txt
```

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.



Sélection du mode de notification

3. Dans l'onglet, définissez les paramètres des notifications.

4. Cliquez sur **Enregistrer** pour enregistrer les modifications et 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** → **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.

Paramètres et variables d'environnement pour décrire un événement

Lors de la configuration des notifications relatives aux événements de Kaspersky Security Center Linux, vous pouvez utiliser des paramètres et des variables d'environnement pour décrire les événements (voir le tableau ci-dessous).

Si vous avez choisi d'exécuter un fichier exécutable comme méthode de notification, utilisez des variables lors de l'écriture du fichier.

Si vous souhaitez envoyer des notifications concernant les événements par email ou SMS, vous pouvez également, lors de la configuration des notifications dans l'onglet correspondant, indiquer des variables dans les champs **Objet** et **Message de notification**.

Paramètres et variables d'environnement pour décrire un événement

Paramètre de substitution (à utiliser dans les notifications)	Variable d'environnement (à utiliser dans les scripts)	Description de la variable d'environnement
%SEVERITY%	$SEVERITY	Importance de l'événement. Valeurs possibles : • **Information** • **Avertissement** • **Erreur** • **Critique**
%COMPUTER%	$COMPUTER	Nom de l'appareil où l'événement s'est produit. La longueur maximale du nom de l'appareil est de 256 caractères.
%DOMAIN%	$DOMAIN	Nom de domaine de l'appareil où l'événement s'est produit.

Paramètre de substitution (à utiliser dans les notifications)	Variable d'environnement (à utiliser dans les scripts)	Description de la variable d'environnement
%EVENT%	$EVENT	Nom du type d'événement. La longueur maximale du nom du type d'événement est de 50 caractères.
%DESCR%	$DESCR	Description de l'événement. La longueur maximale de la description est de 1 000 caractères.
%RISE_TIME%	$RISE_TIME	Heure de création de l'événement.
%KLCSAK_EVENT_TASK_DISPLAY_NAME%	$KLCSAK_EVENT_TASK_DISPLAY_NAME	Nom de la tâche. La longueur maximale du nom de la tâche est de 100 caractères.
%KL_PRODUCT%	$KL_PRODUCT	Nom de l'application.
%KL_VERSION%	$KL_VERSION	Numéro de version de l'application.
%$KLCSAK_EVENT_SEVERITY_NUM%	$KLCSAK_EVENT_SEVERITY_NUM	Numéro d'importance de l'événement. Valeurs possibles : • 1—**Information** • 2—**Avertissement** • 3—**Erreur** • 4—**Critique**
%HOST_IP%	$HOST_IP	Adresse IP de l'appareil où l'événement s'est produit.
%HOST_CONN_IP%	$HOST_CONN_IP	Adresse IP de connexion de l'appareil où 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 Annonces de Kaspersky (**Surveillance** → **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.

- 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. Avertissement
3. 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.

Si vous ne souhaitez pas recevoir les annonces, vous pouvez désactiver cette fonctionnalité.

Désactivation des annonces de Kaspersky

La section Annonces de Kaspersky (**Surveillance** → **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.

Pour désactiver les annonces relatives à la sécurité, procédez comme suit :

1. Dans le menu principal, cliquez sur le nom du Serveur d'administration.

   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.

La désactivation de KSN peut affecter les applications Kaspersky administrées qui utilisent les services KSN. Ces applications peuvent ne plus être en mesure de communiquer avec Kaspersky pour envoyer ou recevoir des données de réputation, des données de télémétrie ou des statistiques.

Affichage d'informations sur les détections de menaces

Vous pouvez activer ou désactiver l'affichage des informations sur les alertes.

Après avoir activé le Serveur d'administration avec une licence Kaspersky Extended Detection and Response Optimum ou Kaspersky Next XDR Optimum, Kaspersky Security Center Web Console affiche automatiquement la sous-section **Alerte** dans la section **Surveillance** du menu principal.

*Pour activer ou désactiver l'affichage de la section **Alerte** dans le menu principal :*

1. Dans le menu principal, accédez à **Configuration** → **Options d'interface**.

2. Activez ou désactivez l'option **Afficher les alertes EDR**.

3. Cliquez sur **Enregistrer**.

Lorsque l'option **Afficher les alertes EDR** est activée, la console affiche la sous-section **Alerte** dans la section **Surveillance** du menu principal. Dans la sous-section **Alerte**, vous pouvez voir des informations sur les détections de menaces sur les appareils des points de terminaison.

Vous pouvez également ajouter un widget qui affiche des informations à propos des alertes.

Pour afficher correctement les informations détaillées sur les menaces détectées dans la fiche d'alertes, vous devez installer le plug-in de Kaspersky Endpoint Agent et la version compatible du plug-in Kaspersky Endpoint Security (Kaspersky Endpoint Security for Linux 12.1 ou version ultérieure, Kaspersky Endpoint Security for Mac 12.1 ou version ultérieure ou Kaspersky Endpoint Security for Windows 12.6 ou version ultérieure).

Utilisez le menu **Filtre** pour filtrer les alertes sur la base de la date et de la valeur des champs.

Le champ **Type d'objet** contient les valeurs suivantes :

- inconnu
- Lien de phishing
- virus
- cheval de Troie
- outil malveillant
- cheval de Troie de l'administration à distance

- ver
- autre application
- Applications publicitaires
- Programme pornographique
- Paquet de programmes dangereux
- Comportement dangereux

Le champ **Réponse automatique** contient les valeurs suivantes :

- Objet malveillant détecté
- L'objet est supprimé
- L'objet est désinfecté
- Échec de la désinfection de l'objet
- Objet placé en quarantaine
- Archive protégée par mot de passe détectée
- Virus détecté

Intégrations pour la réponse aux alertes

Si vous disposez de la licence pour Kaspersky Next XDR Optimum, vous pouvez configurer des intégrations avec les solutions suivantes afin de répondre aux menaces :

- Kaspersky Automated Security Awareness Platform
- Kaspersky Threat Intelligence Portal Sandbox
- Active Directory

Ces intégrations sont disponibles si vous avez activé le Serveur d'administration avec une licence pour Kaspersky Next XDR Optimum.
Pour effectuer des actions de réponse, vous devez déployer la clé de licence Kaspersky Next XDR Optimum sur vos applications administrées.
Lorsque vous utilisez la fonctionnalité Kaspersky Next XDR Optimum avec une licence d'évaluation, vous devez d'abord ajouter un Serveur d'administration secondaire physique, activer ce Serveur d'administration secondaire avec la licence d'évaluation, puis déployer la clé de licence sur vos appareils gérés par ce Serveur d'administration.

Si vous utilisez la licence pour Kaspersky Next EDR Optimum, vous n'avez pas besoin d'activer les applications installées sur vos appareils administrés sous la licence pour Kaspersky Next XDR Optimum. Vous devez le faire uniquement pour les nouveaux appareils, le cas échéant.

Étant donné que la licence Kaspersky Next XDR Optimum prend en charge la multilocation, vous pouvez distribuer de manière centralisée la clé de licence aux applications gérées. La distribution automatique de la licence aux Serveurs d'administration virtuels et secondaires n'est pas prise en charge.

Pour configurer les intégrations, vous devez disposer des droits **de lecture** et **d'écriture** pour la zone fonctionnelle **Fonctionnalités générales : Intégration d'applications**.

Configuration de l'intégration à Active Directory pour l'exécution des actions de réponse

L'intégration à Active Directory vous permet d'exécuter des actions de réponse pour les utilisateurs d'Active Directory affectés par l'alerte ou impliqués dans celle-ci.

Pour configurer l'intégration à Active Directory afin de répondre aux alertes, vous devez utiliser la version 15.4 ou une version ultérieure du Serveur d'administration de Kaspersky Security Center Linux.

L'intégration à Active Directory pour répondre aux alertes et les paramètres d'analyse du contrôleur de domaine Active Directory (l'adresse et les identifiants utilisateur du contrôleur de domaine) que vous spécifiez lors de la configuration d'un sondage du contrôleur de domaine sont deux paramètres distincts. Étant donné que vous devez vous assurer que l'utilisateur pour lequel une action de réponse doit être exécutée dispose d'un compte Active Directory, vous devez configurer les deux intégrations, pour l'analyse et pour la réponse. L'ordre est sans importance.

Les paramètres d'intégration ne sont pas hérités et s'appliquent uniquement au Serveur d'administration (physique ou virtuel) sur lequel vous configurez ces paramètres.

Pour configurer l'intégration à Active Directory afin de répondre aux alertes, procédez comme suit :

1. Dans le menu principal, cliquez sur le nom du Serveur d'administration.

   La fenêtre des propriétés du Serveur d'administration s'ouvre avec l'onglet **Général** sélectionné.

2. Exécutez une des actions suivantes :

   - Sélectionnez la section **Points de distribution**, cliquez sur le nom du point de distribution requis, puis dans la fenêtre des propriétés qui s'ouvre, sélectionnez la section **Active Directory**.

   - Sélectionnez la section **Réponse d'Active Directory**.

3. Dans le volet droit, activez le commutateur **Intégration d'Active Directory**.

   Par la suite, si vous souhaitez désactiver l'intégration, vous ne pouvez le faire que pour toutes les connexions, en désactivant le commutateur **Intégration d'Active Directory**. Vous ne pouvez pas désactiver l'intégration pour une connexion spécifique. À la place, vous pouvez supprimer la connexion.

   > Lorsque vous activez ou désactivez le commutateur **Intégration d'Active Directory**, le paramètre est appliqué à la fois à la section **Réponse d'Active Directory** et à la section **Points de distribution**.

4. Créez une connexion au contrôleur de domaine Active Directory en cliquant sur le bouton **Ajouter**.

5. Dans la fenêtre qui s'ouvre, précisez les paramètres suivants pour la connexion :

   - **Adresse du contrôleur de domaine**

Nom de l'ordinateur, par exemple : `server.mycompany.com`.

Vous pouvez spécifier plusieurs adresses. Tous les contrôleurs de domaine dont vous spécifiez les adresses doivent appartenir au même domaine.

- **Nom de domaine Active Directory**

  Nom de domaine DNS complet, par exemple : `mycompany.com`

  Vous pouvez également spécifier un nom SAM ou NetBIOS, par exemple : `mycompany`

  Utilisez des lettres minuscules. Si vous créez plusieurs connexions pour le Serveur d'administration ou un point de distribution, spécifiez des noms différents pour chaque connexion.

  > Pour que les mesures de réponse puissent être exécutées, le nom de domaine Active Directory que vous indiquez dans ce champ doit correspondre au nom de domaine Active Directory spécifié dans l'alerte.

- **Identifiant**

  Identifiant du compte Active Directory disposant des privilèges d'administrateur et sous lequel les actions de réponse doivent être exécutées.

- **Mot de passe**

  Mot de passe du compte Active Directory disposant des privilèges d'administrateur et sous lequel les actions de réponse doivent être exécutées.

6. Si vous souhaitez vérifier l'état de la connexion, cliquez sur le bouton **Analyser la connexion**.

   Si la connexion est établie avec succès, l'état **Connecté** s'affiche. Sinon, l'état indiqué est **Échec**, et un message d'erreur s'affiche avec les contrôleurs de domaine auxquels vous n'avez pas réussi à vous connecter.

> Vous devez tenir compte du mode de connexion à Active Directory : **à partir d'un appareil Linux ou à partir d'un appareil Windows**.

Connexion à partir d'un appareil Linux

Par défaut, lors de la connexion et de l'authentification auprès d'un contrôleur de domaine à partir d'un appareil Linux, la logique est la suivante :

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

   Une vérification stricte du certificat du serveur LDAP est effectuée.

2. Vous placez la partie publique du certificat du contrôleur de domaine dans le stockage des certificats système pour valider le certificat.

   Le chemin d'accès à l'autorité de certification (CA) du système dépendant du système d'exploitation permet d'accéder à la chaîne de certification.

Par exemple :

- /etc/ssl/certs/ca-certificates.crt : chemin d'accès pour les systèmes d'exploitation basés sur Debian (Debian, Ubuntu, Astra).
- /etc/pki/ca-trust/extracted/pem/tls-ca-bundle.pem : chemin d'accès pour CentOS ou Red Hat.

3. Si la connexion LDAPS échoue, une erreur se produit et aucun autre protocole de connexion n'est utilisé.

   En cas de problème avec LDAPS, vous pouvez contacter le support technique de Kaspersky.

Si vous ne souhaitez pas installer le certificat dans le stockage des certificats système, vous pouvez définir le chemin d'accès au certificat du contrôleur de domaine à l'aide de l'indicateur KLNAG_LDAP_SSL_CACERT. Pour ce faire, exécutez la commande :

```
klscflag -fset -pv klnagent -n KLNAG_LDAP_SSL_CACERT -t s -v "</path/to/domain-controller/cert>"
```

où `</path/to/domain-controller/cert>` est le chemin d'accès à la partie publique du certificat du contrôleur de domaine.

Par exemple, si le chemin d'accès est `"/var/opt/kaspersky/ldap_cert.crt"`, la commande est `klscflag -fset -pv klnagent -n KLNAG_LDAP_SSL_CACERT -t s -v "/var/opt/kaspersky/ldap_cert.crt"`

Connexion à partir d'un appareil Windows

Lors de la connexion et de l'authentification auprès d'un contrôleur de domaine à partir d'un appareil Windows, les paramètres de connexion sont définis par le domaine.

Vous devez simplement vous assurer que :

- LDAPS est activé et le port 636 est disponible sur l'appareil.
- Vous autorisez les connexions au contrôleur de domaine via un pare-feu ou un serveur proxy.

7. Cliquez sur **Enregistrer**.

La fenêtre se ferme et la connexion s'affiche dans le tableau des connexions.

Dans le tableau des connexions, vous pouvez effectuer l'une des opérations suivantes :

- Modifier les paramètres de connexion.

  Pour ce faire, cliquez sur le lien avec le paramètre **Adresse du contrôleur de domaine** pour la connexion requise. Dans la fenêtre qui s'ouvre, modifiez les paramètres requis, puis cliquez sur le bouton **Enregistrer**.

  Vous pouvez uniquement modifier les paramètres **Identifiant** et **Mot de passe** .

- Supprimer des connexions.

  Pour ce faire, cochez la case en regard de la connexion que vous souhaitez supprimer, cliquez sur le bouton **Supprimer** dans la barre d'outils, puis confirmez la suppression de la connexion.

Configuration de l'intégration à Kaspersky Automated Security Awareness Platform

L'intégration à Kaspersky Automated Security Awareness Platform (ci-après également appelé KASAP) vous permet d'assigner des cours de formation KASAP aux utilisateurs associés à des alertes.

Les paramètres d'intégration ne sont pas hérités et s'appliquent uniquement au Serveur d'administration (physique ou virtuel) sur lequel vous configurez ces paramètres.

> Avant de configurer une intégration dans Kaspersky Security Center Web Console, vous devez créer un jeton d'autorisation et obtenir une URL pour les requêtes API dans KASAP.

Pour configurer l'intégration à Kaspersky Automated Security Awareness Platform, procédez comme suit :

1. Dans le menu principal, cliquez sur le nom du Serveur d'administration.

   La fenêtre des propriétés du Serveur d'administration s'ouvre avec l'onglet **Général** sélectionné.

2. Sélectionnez la section **KASAP**.

3. Dans le volet droit, activez le commutateur **Intégration KASAP**.

4. Spécifiez les paramètres à utiliser pour la connexion à KASAP :

   - **Jeton d'API** : jeton que vous avez créé pour accéder à KASAP Open API.

   - **URL** : URL pour les requêtes API que vous avez obtenue lors de la création du jeton API.

   - **Utiliser un serveur proxy** : commutateur qui active l'utilisation d'un serveur proxy lors de la connexion à KASAP.

     Le commutateur est désactivé par défaut.

5. Si nécessaire, vérifiez les paramètres que vous avez spécifiés en cliquant sur le bouton **Analyser la connexion**.

   L'état de la connexion s'affiche.

6. Cliquez sur le bouton **Enregistrer**.

L'intégration à Kaspersky Automated Security Awareness Platform est configurée.

Une fois les paramètres d'intégration à KASAP enregistrés, vous pouvez afficher la liste des groupes de formation KASAP en cliquant sur le bouton **Afficher les groupes**.

Si nécessaire, lorsque la liste des groupes s'affiche, vous pouvez la mettre à jour en cliquant sur le bouton **Actualiser les groupes**.

> Vous ne pouvez pas masquer la liste après l'avoir ouverte. Si vous désactivez le commutateur **Intégration KASAP**, la liste des groupes KASAP ne s'affiche pas.

Configuration de l'intégration à Kaspersky Threat Intelligence Portal Sandbox

L'intégration à Kaspersky Threat Intelligence Portal (ci-après également appelé Kaspersky TIP) vous permet d'exécuter les fichiers déplacés vers la section **Quarantaine** en utilisant Kaspersky Sandbox, un environnement sécurisé isolé du réseau de votre entreprise.

Les paramètres d'intégration ne sont pas hérités et s'appliquent uniquement au Serveur d'administration (physique ou virtuel) sur lequel vous configurez ces paramètres.

> Avant de configurer l'intégration, vous devez obtenir un jeton d'autorisation pour les requêtes API sur Kaspersky TIP.

Pour configurer l'intégration à Kaspersky TIP Sandbox, procédez comme suit :

1. Dans le menu principal, cliquez sur le nom du Serveur d'administration.

   La fenêtre des propriétés du Serveur d'administration s'ouvre avec l'onglet **Général** sélectionné.

2. Sélectionnez **Kaspersky TIP**.

3. Dans le volet droit, activez le commutateur **Intégration**.

   Les paramètres de connexion à Kaspersky TIP s'affichent.

   > Si, après avoir configuré et enregistré les paramètres d'intégration, vous désactivez le commutateur **Intégration**, les paramètres ne sont pas supprimés, mais la réponse ne peut pas être exécutée.

4. Cliquez sur le bouton **Ajouter un jeton** et, dans la fenêtre qui s'affiche, spécifiez le jeton obtenu précédemment auprès de Kaspersky TIP, puis cliquez sur le bouton **Ajouter**.

   La fenêtre se ferme et le jeton API est ajouté.

5. Si vous souhaitez utiliser un serveur proxy lors de la connexion à Kaspersky TIP, activez le commutateur **Utiliser un serveur proxy**.

   Le commutateur est désactivé par défaut.

6. Cliquez sur **Enregistrer**.

L'intégration à Kaspersky TIP Sandbox est configurée.

Vous pouvez désormais envoyer des fichiers depuis la section **Quarantaine** vers Kaspersky TIP Sandbox à des fins d'analyse des menaces. La taille maximale d'un fichier est de 100 Mo.

Étant donné que la licence pour Kaspersky Next XDR Optimum prend en charge la multilocation, les fichiers placés en **Quarantaine** sont répartis entre les locataires. Cette répartition entre les locataires s'applique également lors de l'envoi de fichiers vers Kaspersky TIP Sandbox et de l'affichage des résultats si l'administrateur utilise un compte TIP dédié et un jeton API associé à chaque locataire. Cependant, la gestion centralisée de la section **Quarantaine** pour tous les locataires n'est pas possible, car la liste de quarantaine n'affiche pas les objets selon la hiérarchie des serveurs.

Regroupement des alertes par attributs

L'agrégation des alertes permet d'identifier les alertes qui peuvent être liées au même incident, ce qui simplifie le processus d'enquête.

Pour activer la fonctionnalité d'agrégation des alertes, vous devez procéder comme suit :

- Activez la sous-section **Alerte** dans le menu principal.
- Activez le Serveur d'administration sous une licence pour Kaspersky Next XDR Optimum, puis déployez la clé de licence pour Kaspersky Next XDR Optimum dans les applications que vous administrez.

  Lorsque vous utilisez une fonctionnalité Kaspersky Next XDR Optimum sous licence d'évaluation en mode test, il faut d'abord ajouter un Serveur d'administration physique secondaire, puis activer ce serveur sous cette licence.

Si vous utilisez la licence pour Kaspersky Next EDR Optimum, vous n'avez pas besoin d'activer les applications installées sur vos appareils administrés sous la licence pour Kaspersky Next XDR Optimum. Vous devez le faire uniquement pour les nouveaux appareils, le cas échéant.
Étant donné que la licence Kaspersky Next XDR Optimum prend en charge la multilocation, vous pouvez distribuer de manière centralisée la clé de licence aux applications gérées. La distribution automatique de la licence aux Serveurs d'administration virtuels et secondaires n'est pas prise en charge.

Vous pouvez regrouper les alertes par nom d'appareil, compte ou nom du hachage (SHA256).

> Les alertes sont agrégées par un attribut uniquement si cet attribut n'est pas vide.

Les alertes sont agrégées si elles partagent au moins un attribut et si elles se produisent dans les 24 heures suivant toute autre alerte du groupe.

Pour agréger les alertes par attributs, procédez comme suit :

1. Dans le menu principal, accédez à **Surveillance** → **Alerte**.
2. Exécutez une des actions suivantes :
   - Activez le commutateur **Agrégation des alertes**, puis sélectionnez au moins un attribut pour agréger les alertes par :
     - **Nom de l'appareil**
     - **Compte utilisateur**
     - **Hachage du fichier**Nom du hachage (SHA256)

Les attributs **Nom de l'appareil** et **Compte utilisateur** sont sélectionnés par défaut.

- Cliquez sur l'icône des Paramètres (⚙). Dans le volet **Paramètres du tableau** qui s'ouvre, accédez à l'onglet **Groupe**. Sélectionnez **Identifiant du groupe d'agrégation** et cliquez sur **Appliquer**.

Lorsque l'agrégation est activée, les alertes sont triées par **Heure de l'événement**, du plus récent au plus ancien. Les options de tri supplémentaires ne sont pas prises en charge. La sélection d'une autre option de regroupement désactivera l'agrégation.

Le tableau affiche les alertes agrégées par attributs. Les alertes non regroupées s'affichent en bas du tableau.

Chaque alerte est attribuée à un seul groupe après agrégation.

Cloud Discovery

Kaspersky Security Center Linux vous permet de surveiller l'utilisation des services cloud sur les appareils administrés sous Windows et de bloquer l'accès aux services cloud que vous considérez comme indésirables. La fonctionnalité Cloud Discovery suit les tentatives des utilisateurs d'accéder à ces services via les navigateurs et les applications de bureau. Cette fonctionnalité suit également les tentatives des utilisateurs d'accéder aux services cloud via des connexions non chiffrées (par exemple, en utilisant le protocole HTTP). Cette fonctionnalité vous permet de détecter et d'interrompre l'utilisation des services cloud sous la forme de Shadow IT.

La fonction de blocage est disponible uniquement si vous avez activé Kaspersky Security Center Linux sous une licence Kaspersky Next EDR Optimum ou Kaspersky Next XDR Expert.

La fonctionnalité de blocage est disponible uniquement si vous utilisez Kaspersky Endpoint Security 11.2 for Windows ou une version ultérieure. Les versions antérieures de l'application de sécurité vous permettent uniquement de surveiller l'utilisation des services cloud.

Vous pouvez activer la fonctionnalité Cloud Discovery et sélectionner les stratégies ou les profils de sécurité pour lesquels vous souhaitez activer la fonctionnalité. Vous pouvez également activer ou désactiver la fonctionnalité séparément dans chaque stratégie ou profil de sécurité. Vous pouvez bloquer l'accès aux services cloud auxquels vous ne souhaitez pas que les utilisateurs accèdent.

Pour pouvoir interdire l'accès aux services cloud indésirables, assurez-vous que les conditions préalables suivantes sont remplies :

- Vous utilisez Kaspersky Endpoint Security 11.2 for Windows ou une version ultérieure. Les versions antérieures de l'application de sécurité vous permettent uniquement de surveiller l'utilisation des services cloud.

- Vous avez acheté un niveau de licence Kaspersky Next qui offre la possibilité de bloquer l'accès aux services cloud indésirables. Pour en savoir plus, consultez l'aide de Kaspersky Next.

Le widget Cloud Discovery et les rapports Cloud Discovery affichent des informations sur les tentatives d'accès aux services cloud réussies et bloquées. Le widget affiche également le niveau de risque de chaque service cloud. Kaspersky Security Center Linux obtient les informations sur l'utilisation des services cloud pour tous les appareils administrés qui sont protégés uniquement par des profils de sécurité pour lesquelles la fonctionnalité est activée.

Activation de Cloud Discovery à l'aide du widget

La fonctionnalité Cloud Discovery vous permet d'obtenir des informations sur l'utilisation des services cloud par tous les appareils administrés protégés uniquement par des stratégies de sécurité pour lesquelles la fonctionnalité est activée. Vous pouvez activer ou désactiver Cloud Discovery uniquement pour la stratégie Kaspersky Endpoint Security for Windows.

Il existe deux manières d'activer la fonctionnalité Cloud Discovery :

- En utilisant le widget Cloud Discovery.
- Dans les propriétés de la stratégie Kaspersky Endpoint Security for Windows.

  Pour en savoir plus sur l'activation de la fonctionnalité Cloud Discovery dans les propriétés de la stratégie Kaspersky Endpoint Security for Windows, veuillez consulter la section Cloud Discovery de l'aide de Kaspersky Endpoint Security for Windows.

Notez que vous pouvez désactiver la fonctionnalité Cloud Discovery dans les paramètres de la stratégie Kaspersky Endpoint Security for Windows uniquement.

Pour activer Cloud Discovery, vous devez disposer du droit **Écrire** dans la zone fonctionnelle **Caractéristiques générales : fonctionnalité de base**.

Pour activer la fonctionnalité Cloud Discovery à l'aide du widget Cloud Discovery, procédez comme suit :

1. Accédez à Kaspersky Security Center Linux.
2. Dans le menu principal, accédez à **Surveillance** → **Tableau de bord**.
3. Sur le widget **Cloud Discovery**, cliquez sur le bouton **Activer**.

   Si Kaspersky Endpoint Security for Windows version 12.4 est installé, activez la fonctionnalité Cloud Discovery dans les propriétés de la stratégie de Kaspersky Endpoint Security for Windows. Pour en savoir plus, consultez la section Cloud Discovery de l'aide de Kaspersky Endpoint Security for Windows.

   Si vous disposez d'une version de Kaspersky Endpoint Security for Windows antérieure à la version 12.4, mettez à jour le plug-in Kaspersky Endpoint Security for Windows vers la version 12.5.

4. Dans la fenêtre **Nom de la stratégie** qui s'ouvre, sélectionnez les stratégies de sécurité pour lesquelles vous souhaitez activer la fonctionnalité, puis cliquez sur le bouton **Activer**.

   Les paramètres de stratégie suivants seront activés automatiquement : **Implanter un script dans le trafic Internet pour interagir avec les pages Internet**, **Moniteur de session Internet** et **Analyse des connexions chiffrées**.

La fonctionnalité Cloud Discovery est activée, et le widget est ajouté au tableau de bord.

Ajout du widget Cloud Discovery au tableau de bord

Vous pouvez ajouter le widget **Cloud Discovery** au tableau de bord pour surveiller l'utilisation des services cloud sur les appareils administrés.

Pour ajouter le widget Cloud Discovery à votre tableau de bord, vous devez disposer du droit **Écrire** dans la zone fonctionnelle **Caractéristiques générales : fonctionnalité de base**.

Pour ajouter le widget Cloud Discovery au tableau de bord, procédez comme suit :

1. Accédez à Kaspersky Security Center Linux.
2. Dans le menu principal, accédez à **Surveillance** → **Tableau de bord**.
3. Cliquez sur le bouton **Ajouter ou restaurer un widget**.
4. Dans la liste des widgets disponibles, cliquez sur l'icône en forme de chevron (>) en regard de la catégorie **Autres**.
5. Sélectionnez le widget **Cloud Discovery**, puis cliquez sur le bouton **Ajouter**.

   Si la fonctionnalité Cloud Discovery est désactivée, suivez les instructions de la section Activation de Cloud Discovery à l'aide du widget.

Le widget sélectionné est ajouté à la fin du tableau de bord.

Affichage d'informations sur l'utilisation des services cloud

Vous pouvez afficher le widget **Cloud Discovery** qui affiche des informations sur les tentatives d'accès aux services cloud. Le widget affiche également le niveau de risque de chaque service cloud. Kaspersky Security Center Linux obtient des informations sur l'utilisation des services cloud auprès de tous les appareils administrés protégés uniquement par des profils de sécurité pour lesquels cette fonctionnalité est activée.

Avant d'afficher les informations, assurez-vous que :

- le widget Cloud Discovery est ajouté au tableau de bord.
- la fonctionnalité Cloud Discovery est activée.
- le droit **Lecture** figure dans la zone fonctionnelle **Caractéristiques générales : fonctionnalité de base**.

Pour afficher le widget Cloud Discovery :

1. Accédez à Kaspersky Security Center Linux.
2. Dans le menu principal, accédez à **Surveillance** → **Tableau de bord**.

   Le widget **Cloud Discovery** s'affiche sur le tableau de bord.

3. Dans la partie gauche du widget **Cloud Discovery**, sélectionnez une catégorie de services cloud.

   Le tableau à droite du widget affiche jusqu'à cinq services, issus de la catégorie sélectionnée, auxquels les utilisateurs tentent le plus souvent d'accéder. Les tentatives réussies et bloquées sont comptabilisées.

4. Dans la partie droite du widget, sélectionnez un service spécifique.

   Le tableau ci-dessous affiche une dizaine d'appareils qui tentent le plus souvent d'accéder au service. Ce tableau permet de créer deux types de rapports : le rapport sur les tentatives d'accès réussies et le rapport sur les tentatives d'accès bloquées.

   De plus, ce tableau permet de bloquer l'accès au service cloud pour un appareil défini.

Le widget affiche les informations demandées.

À partir du widget affiché, vous pouvez effectuer les opérations suivantes :

- Passer à la section **Surveillance** → **Rapports** pour consulter les rapports de Cloud Discovery.
- Interdire ou autoriser l'accès au service cloud sélectionné.

> La fonction de blocage est disponible uniquement si vous avez activé Kaspersky Security Center Linux sous une licence Kaspersky Next EDR Optimum ou Kaspersky Next XDR Expert.
> La fonction de blocage est disponible que si vous utilisez Kaspersky Endpoint Security 11.2 for Windows ou suivant. Les versions antérieures de l'application de sécurité vous permettent uniquement de surveiller l'utilisation des services cloud.

Niveau de risque d'un service cloud

Cloud Discovery indique un niveau de risque pour chaque service cloud. Le niveau de risque vous aide à déterminer les services qui ne correspondent pas aux exigences de sécurité de votre organisation. Par exemple, vous souhaiterez peut-être prendre en considération le niveau de risque lorsque vous déciderez d'interdire ou non l'accès à un service.

> Le niveau de risque est un indice estimé et ne dit rien sur la qualité d'un service cloud ou sur le fabricant du service. Le niveau de risque est simplement une recommandation des experts de Kaspersky.

Le widget Cloud Discovery affiche les niveaux de risque des services cloud dans la liste de tous les services cloud surveillés.

Blocage de l'accès aux services cloud indésirables

Vous pouvez bloquer l'accès aux services cloud auxquels vous ne souhaitez pas que les utilisateurs accèdent. Vous pouvez également autoriser l'accès à des services cloud qui ont été précédemment bloqués.

Entre autres considérations, vous souhaiterez peut-être prendre en compte le niveau de risque lorsque vous décidez de bloquer l'accès à un certain service.

Vous pouvez interdire ou autoriser l'accès aux services cloud pour une stratégie ou un profil de sécurité.

Il existe deux manières de bloquer l'accès aux services cloud indésirables :

- En utilisant le widget Cloud Discovery.

  Dans ce cas, vous pouvez bloquer l'accès aux services un par un.

- Dans les propriétés de la stratégie Kaspersky Endpoint Security for Windows.

  Dans ce cas, vous pouvez interdire l'accès aux services un par un ou interdire l'ensemble d'une catégorie à la fois.

  Pour en savoir plus sur l'activation de la fonctionnalité Cloud Discovery dans les propriétés de la stratégie Kaspersky Endpoint Security for Windows, veuillez consulter la section Cloud Discovery de l'aide de Kaspersky Endpoint Security for Windows.

Pour interdire ou autoriser l'accès à un service cloud en utilisant le widget, procédez comme suit :

1. Ouvrez le widget Cloud Discovery, puis sélectionnez le service cloud requis.

2. Dans le **Les 10 principaux appareils qui utilisent le service**, trouvez la stratégie ou le profil de sécurité pour lequel vous souhaitez interdire ou autoriser le service.

3. Sur la ligne requise, dans la colonne **État d'accès dans la stratégie/le profil**, exécutez une des actions suivantes :

   - Pour bloquer le service, sélectionnez **Bloqué** dans la liste déroulante.

   - Pour autoriser le service, sélectionnez **Autorisé** dans la liste déroulante.

4. Cliquez sur le bouton **Enregistrer**.

L'accès au service sélectionné est bloqué ou autorisé pour la stratégie ou le profil de sécurité.

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 d'événements vers des systèmes SIEM par l'une des méthodes suivantes : exportation vers n'importe quel système SIEM utilisant le format Syslog, exportation vers les systèmes QRadar, Splunk, ArcSight SIEM utilisant les formats LEEF et CEF ou exportation d'événements vers les systèmes SIEM directement depuis la base de données Kaspersky Security Center. Une fois ce scénario terminé, le Serveur d'administration envoie automatiquement les événements au système SIEM.

Prérequis

Avant de lancer l'exportation de la configuration des événements vers Kaspersky Security Center 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, UDP ou TLS sur TCP.
  - Exportation des événements directement depuis la base de données de Kaspersky Security Center. La base de données de Kaspersky Security Center contient un ensemble de vues publiques ; vous trouverez une description de ces vues 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.

Prérequis

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.

Modes d'envoi des événements de Kaspersky Security Center Linux

Il existe trois modes d'envoi des événements depuis Kaspersky Security Center Linux vers les systèmes externes :

- Envoi des événements via le protocole Syslog à n'importe quel système SIEM.

  Le protocole Syslog permet de transmettre n'importe quel événement survenu sur le Serveur d'administration de Kaspersky Security Center et dans les applications de Kaspersky installées sur les appareils administrés. Le protocole Syslog est un protocole standard d'enregistrement de messages. Vous pouvez l'utiliser pour exporter des événements vers n'importe quel système SIEM.

  Pour cela, vous devez marquer les événements que vous souhaitez relayer au système SIEM. Vous pouvez marquer les événements dans Kaspersky Security Center Web Console. Seuls les événements marqués seront relayés au système SIEM. Si vous n'avez rien coché, aucun événement ne sera relayé.

- Envoi des événements via les protocoles CEF et LEEF vers les systèmes QRadar, Splunk et ArcSight.

  Vous pouvez utiliser les protocoles CEF et LEEF pour exporter des événements généraux. Dans le cadre de l'exportation des événements via les protocoles CEF et LEEF, vous ne pouvez pas sélectionner les événements à exporter. Tous les événements généraux sont exportés. Pour convertir les événements de Kaspersky Security Center Linux en événements au format CEF et LEEF, vous devez utiliser le fichier siem_conversion_rules.xml. Ce fichier contient la liste des attributs d'événements de Kaspersky Security Center Linux et les attributs correspondants des événements au format CEF et LEEF. De plus, le fichier siem_conversion_rules.xml contient les règles de génération de messages correspondant aux événements. Ce fichier figure dans le kit de distribution de Kaspersky Security Center Linux.

  A la différence du protocole Syslog, les protocoles CEF et LEEF ne sont pas universels. CEF et LEEF sont destinés aux systèmes SIEM correspondants (QRadar, Splunk et ArcSight). Par conséquent, quand vous décidez d'exporter des événements via un de ces protocoles, vous devez utiliser l'analyseur requis dans le système SIEM.

- Directement depuis la base de données de Kaspersky Security Center Linux vers n'importe quel système SIEM.

  Ce mode d'exportation des événements peut être utilisé pour obtenir des événements directement depuis les représentations publiques de la base de données avec l'l'aide des de requêtes SQL. Les résultats de l'exécution de la requête sont enregistrés dans le fichier .xml qui peut être utilisé pour les données d'entrée du système externe. L'exportation directe depuis la base de données concerne uniquement les événements accessibles dans les représentations publiques.

Réception des événements par le système SIEM

Le système SIEM doit accepter et analyser correctement les événements en provenance de Kaspersky Security Center Linux. Pour ce faire, vous devez configurer correctement 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**

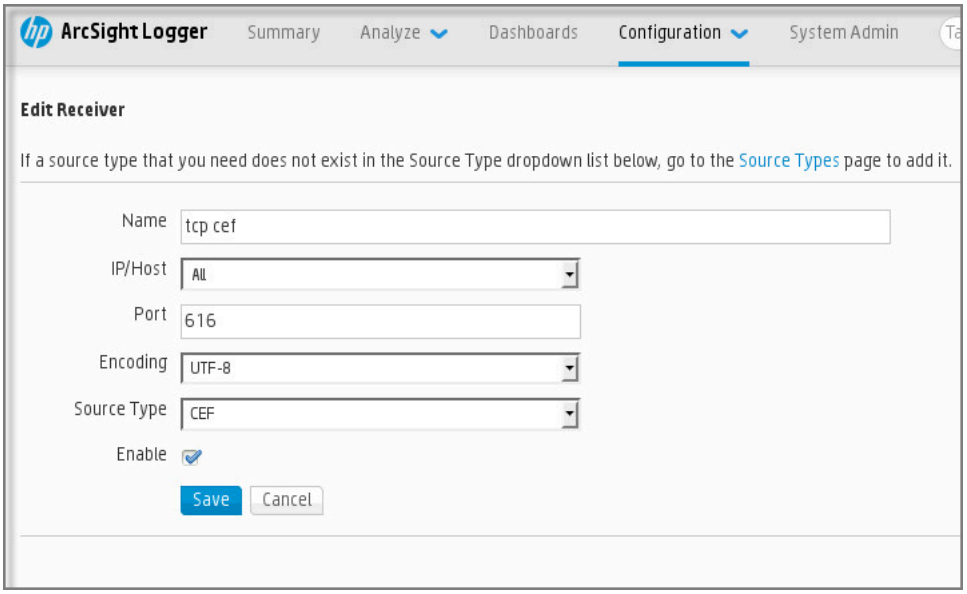
  Indiquez le numéro de port pour vous connecter à Kaspersky Security Center Linux. Il est nécessaire d'indiquer le même numéro de port que celui qui a été choisi dans Kaspersky Security Center Linux lors de la configuration avec un système SIEM.

- **Format de données**

  Spécifiez le format Syslog, CEF ou LEEF.

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. Un analyseur est ensuite appliqué à ces messages afin de garantir que les informations sur les événements puissent être utilisées par le système SIEM. L'analyseur des messages fait partie du système SIEM ; il permet de décomposer le contenu du message en champs tels que le code de l'événement, la gravité, la description et les 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.

À propos de l'exportation des événements via les formats CEF et LEEF

Vous pouvez utiliser les formats CEF et LEEF pour exporter vers les systèmes SIEM des événements généraux, ainsi que les événements transférés par les applications Kaspersky vers le Serveur d'administration. L'ensemble des événements à exporter est défini préalablement et il est impossible de sélectionner les événements à exporter. Avant d'envoyer des événements au système SIEM (QRadar, ArcSight ou Splunk), il est nécessaire d'interpréter les événements de Kaspersky Security Center Linux en événements au format CEF et LEEF en utilisant les règles indiquées dans le fichier siem_conversion_rules.xml.

Choisissez le format d'exportation en fonction du système SIEM que vous utilisez. Le tableau suivant reprend les systèmes SIEM et les formats d'exportation qui leur correspond.

Formats d'exportation des événements dans le système SIEM

Système SIEM	Format d'exportation
QRadar	LEEF
ArcSight	CEF
Splunk	CEF

- LEEF (Log Event Extended Format) est un format d'événement spécialisé pour IBM Security QRadar SIEM. QRadar peut recevoir, identifier et traiter les événements transmis via le protocole LEEF. Le protocole LEEF requiert l'utilisation du codage UTF-8. Pour en savoir plus sur le protocole LEEF, consultez la page Internet du IBM Knowledge Center.

- CEF est un standard d'administration de type " journal ouvert " qui améliore la compatibilité des informations du système de sécurité de différents appareils et applications réseau. Le protocole CEF permet d'utiliser le format général du journal des événements pour que les systèmes d'administration de l'entreprise puissent recevoir et regrouper facilement les données pour l'analyse. Le protocole CEF requiert l'utilisation du codage UTF-8.

Lors de l'exportation automatique, Kaspersky Security Center Linux envoie les événements généraux au système SIEM. L'exportation automatique des événements dès l'activation. Cette section décrit la procédure d'activation de l'exportation des événements automatique.

Conversion d'événements au format CEF ou LEEF

Avant d'envoyer des événements au système SIEM (QRadar, ArcSight ou Splunk), il est nécessaire d'interpréter les événements de Kaspersky Security Center Linux en événements au format CEF et LEEF en utilisant les règles indiquées dans le fichier siem_conversion_rules.xml. Ce fichier figure dans le kit de distribution de Kaspersky Security Center Linux.

Le fichier siem_conversion_rules.xml contient les règles d'interprétation prédéfinies pour convertir les événements au format CEF et LEEF. Si vous souhaitez utiliser d'autres règles d'interprétation d'événements, vous pouvez les ajouter manuellement au fichier.

Le fichier siem_conversion_rules.xml comprend les sections suivantes :

- `<product name="SP_QRADAR" vendor="IBM">`

  Cette section contient des règles pour générer des événements au format LEEF, qui peuvent être exportés vers le système SIEM QRadar.

- `<product name="SP_ARCSIGHT" vendor="HP">`.

  Cette section contient des règles pour générer des événements au format CEF, qui peuvent être exportés vers le système SIEM ArcSight ou Splunk.

Chaque section contient la sous-section `<common>` dans laquelle se trouvent les attributs d'événements de Kaspersky Security Center Linux et les attributs correspondants des événements au format LEEF. Ces attributs communs sont utilisés pour tous les types d'événements pouvant être exportés.

De plus, chaque section contient les sous-sections `<event>`. Chaque sous-section `<event>` contient des attributs supplémentaires qui s'ajoutent à ceux répertoriés dans la section `<common>`.

Vous pouvez ajouter manuellement une nouvelle règle de génération d'événements au fichier siem_conversion_rules.xml.

Pour ajouter une nouvelle règle de génération d'événements :

1. Ajoutez une nouvelle sous-section `<event>` à la section `<product name="SP_QRADAR" vendor="IBM">` ou `<product name="SP_ARCSIGHT" vendor="HP">`, puis indiquez les attributs d'événement supplémentaires, si nécessaire.

2. Si un événement est constitué uniquement d'attributs communs, la sous-section `<event>` sera vide.

siem_conversion_rules.xml

```
<conversion_rules>
    <product name="SP_QRADAR" vendor="IBM">
        <common> <!-- Common Kaspersky Security Center Linux event attributes and corresponding LEEF event
attributes -->
            <param name="KLSPLG_HOST_DISP_NAME" type="STRING_T">
                <attr name="EVC_EV_DISP_HOST_NAME" type="AT_STRING" limit="255"/>
            </param>
            ...
        </common>
        <event id="GNRL_EV_VIRUS_FOUND"> <!-- Generation rule for the GNRL_EV_VIRUS_FOUND event with additional
attributes -->
            <param name="GNRL_EA_PARAM_1" type="STRING_T">
                <attr name="EVC_EV_SHA256" type="AT_STRING" limit="255"/>
            </param>
            ...
        </event>
...
</product>
    <product name="SP_ARCSIGHT" vendor="HP">
        <common> <!-- Common Kaspersky Security Center Linux event attributes and corresponding LEEF event
attributes -->
            <param name="KLSPLG_HOST_DISP_NAME" type="STRING_T">
                <attr name="dhost" type="AT_STRING" limit="1023"/>
            </param>
            ...
        </common>
        <event id="GNRL_EV_VIRUS_FOUND">
            <param name="GNRL_EA_PARAM_1" type="STRING_T">
                <attr name="cs4" type="AT_STRING" limit="255"/>
                <attr name="cs4Label" type="AT_STRING" val="SHA256"/>
            </param>
            ...
</product>
</conversion_rules>
```

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 **Gestion des ressources** → **Stratégies**.
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 **Gestion des ressources** → **Ressources (Appareils)**.

   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**.

> 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.

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. Dans le menu principal, exécutez une des actions suivantes :
   - Cliquez sur le nom du Serveur d'administration.
   - Accédez à **Gestion des ressources** → **Stratégies**, 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**.

> 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.

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.

Avant d'envoyer des événements au système SIEM (QRadar, ArcSight ou Splunk), il est nécessaire d'interpréter les événements de Kaspersky Security Center en événements au format CEF et LEEF en utilisant les règles indiquées dans le fichier siem_conversion_rules.xml.

Pour configurer l'exportation vers les systèmes SIEM dans Kaspersky Security Center Web Console :

1. Dans le menu principal, cliquez sur le nom du Serveur d'administration.

   La fenêtre des propriétés du Serveur d'administration s'ouvre.

2. Sous l'onglet **Général**, sélectionnez la section **Exporter vers SIEM**.

3. Cliquez sur le lien **Configuration**.

   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 sur 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 une authentification 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 une authentification 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**. Chargez un fichier contenant un certificat dans le champ **Fichier avec certificat** et un fichier contenant une clé privée dans le champ **Fichier avec clé**. Les deux fichiers sont indépendants l'un de l'autre. L'ordre de chargement des fichiers n'a pas d'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.

- **Format de données**

  Vous pouvez sélectionner les formats System log, CEF ou LEEF, selon les exigences du système SIEM.

  Si vous sélectionnez le format de données du journal système, vous devez indiquer la **Taille maximale du message en octets**

  Indiquez la taille maximale en octets d'un message transmis au système SIEM. Chaque événement entraîne l'envoi d'un message. Si la longueur réelle du message dépasse la valeur indiquée, le message est tronqué et vous risquez de perdre des données. Par défaut, la taille du message est de 2048 octets. Ce champ est accessible uniquement si vous avez choisi le format System log dans le champ **Protocole**.

5. Si vous le souhaitez, vous pouvez exporter des événements archivés à partir de la base de données du Serveur d'administration et définir la date de début à partir de laquelle vous souhaitez lancer l'exportation des événements archivés :

   a. Cliquez sur le lien **Définir la date de début de l'exportation**.

   b. Dans la section qui s'ouvre, indiquez la date de début dans le champ **Date de début de l'exportation**.

   c. Cliquez sur le bouton **OK**.

6. Basculez l'option en position **Exporter automatiquement les événements dans la base du système SIEM Activé**.

7. Pour vérifier que la connexion au système SIEM a été configurée, cliquez sur le bouton **Analyser la connexion**.

   La connexion avec le serveur système SIEM est établie et un événement de test est envoyé. L'état de la connexion s'affiche.

8. 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 <nom d'utilisateur> -p <mot de passe> -o result.xml`

   où `<nom d'utilisateur>` et `<mot de passe>` sont les identifiants du compte qui a accès à la base de données.

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 le nom du Serveur d'administration.

   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.

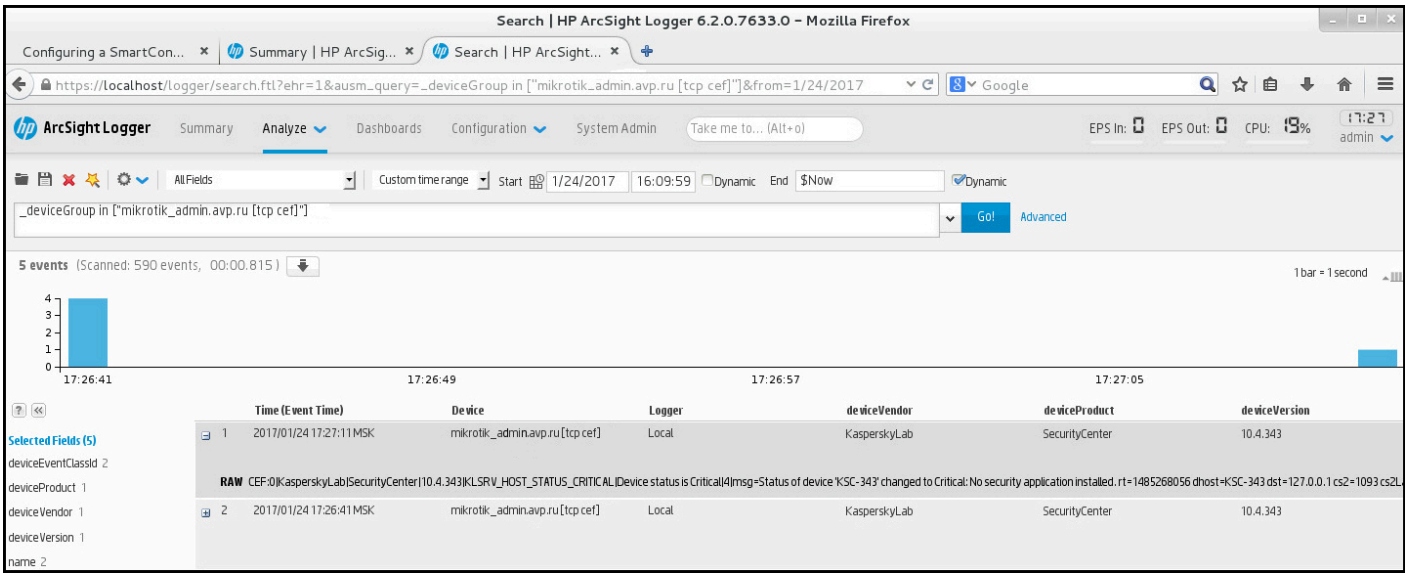
Consultation des résultats de l'exportation

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.

La *révision* est l'état d'un objet à un moment donné. Chaque fois que vous créez ou modifiez un objet, une nouvelle révision de cet objet est créée. Chaque révision contient tous les paramètres de l'objet tels qu'ils sont au moment où la révision est créée ou enregistrée.

Voici les objets compatibles avec la gestion des révisions :

- Propriétés du Serveur d'administration
- Stratégies
- Tâches
- Groupes d'administration
- Comptes utilisateurs
- Paquets d'installation

Vous pouvez réaliser les opérations suivantes avec les révisions d'objets :

- Afficher la révision sélectionnée (disponible uniquement pour les stratégies)
- Annuler les modifications d'un objet jusqu'à la révision sélectionnée
- Enregistrer les révisions dans un fichier JSON (disponible uniquement pour les stratégies)

La section **Historique des révisions** de la fenêtre des propriétés des objets compatibles avec la gestion des révisions reprend une liste des révisions avec les informations suivantes :

- **Révision** – le numéro de la révision de l'objet.
- **Heure** – la date et l'heure de modification de l'objet.
- **Utilisateur** – le nom de l'utilisateur ayant modifié l'objet.
- **Adresse IP de l'appareil de l'utilisateur** – l'adresse IP de l'appareil à partir duquel lequel l'objet a été modifié.
- **Adresse IP de la Web Console** – l'adresse IP de Kaspersky Security Center Web Console avec laquelle l'objet a été modifié.
- **Action** – l'action exécutée avec l'objet.
- **Description** – la description de la révision de modification des paramètres de l'objet.

  Par défaut, la description de la révision de l'objet n'est pas remplie. Pour ajouter une description de la révision, choisissez la révision requise, puis cliquez sur le bouton **Modifier la description**. Dans la fenêtre qui s'ouvre, saisissez un texte correspondant à la description de la révision.

Affichage et enregistrement d'une révision de la stratégie

Kaspersky Security Center Linux permet de consulter les modifications apportées à une stratégie au cours d'une période donnée et d'enregistrer les informations sur ces modifications dans un fichier.

> L'affichage et l'enregistrement d'une révision de la stratégie sont disponibles si le plug-in Internet d'administration correspondant prend en charge cette fonctionnalité.

Pour consulter la révision d'une stratégie, procédez comme suit :

1. Dans le menu principal, accédez à **Gestion des ressources** → **Stratégies**.
2. Cliquez sur la stratégie de la révision que vous souhaitez consulter, puis passez à la section **Historique des révisions**.
3. Dans la liste des révisions de la stratégie, cliquez sur le numéro de la révision que vous souhaitez consulter.

   Si la taille de la révision est supérieure à 10 Mo, vous ne pourrez pas la consulter à l'aide de Kaspersky Security Center Web Console. Vous serez invité à enregistrer la révision sélectionnée dans un fichier JSON.

Si la taille de la révision ne dépasse pas 10 Mo, un rapport au format HTML avec les paramètres de la révision de la stratégie sélectionnée s'affiche. Comme le rapport s'affiche dans une fenêtre contextuelle, assurez-vous que les fenêtres contextuelles sont autorisées dans votre navigateur !

Pour les stratégies de Kaspersky Endpoint Security for Windows et de Kaspersky Endpoint Security for Mac, le rapport ne contiendra aucune information concernant les profils de stratégie.

Pour enregistrer une révision de la stratégie dans un fichier JSON, procédez comme suit :

Dans la liste des révisions de la stratégie, sélectionnez la révision que vous souhaitez enregistrer, puis cliquez sur **Enregistrer dans le fichier**.

La révision est enregistrée dans un fichier JSON.

Si nécessaire, vous pouvez comparer les révisions des stratégies. Cette option est disponible pour les stratégies du Serveur d'administration, de l'Agent d'administration, de Kaspersky Endpoint Security for Windows (à partir de la version 14.0 du plug-in Internet) et de Kaspersky Endpoint Security for Mac (à partir de la version 12.2.1 Correctif A du plug-in Internet).

Comparaison des révisions de stratégies

Vous pouvez comparer les anciennes révisions d'une stratégie avec sa révision actuelle, comparer différentes révisions sélectionnées dans la liste, ou comparer la révision d'une stratégie avec la révision d'une autre. Les options sont disponibles pour les stratégies du Serveur d'administration, de l'Agent d'administration, de Kaspersky Endpoint Security for Windows (à partir de la version 14.0 du plug-in Internet) et de Kaspersky Endpoint Security for Mac (à partir de la version 12.2.1 Correctif A du plug-in Internet).

Pour comparer les révisions d'une stratégie, procédez comme suit :

1. Dans le menu principal, accédez à **Gestion des ressources** → **Stratégies**.
2. Cliquez sur la stratégie dont vous souhaitez comparer les révisions.

   La fenêtre des paramètres de la stratégie s'ouvre.
3. Accédez à l'onglet **Historique des révisions**, puis cochez les cases en regard des révisions à comparer.
4. Dans la barre d'outils, cliquez sur le bouton **Comparer**, puis dans la liste déroulante, sélectionnez l'une des options suivantes :

   - **Avec la révision actuelle**, si vous souhaitez comparer la révision que vous avez sélectionnée à l'étape 3 avec la dernière révision enregistrée de la même stratégie.
   - **Révisions sélectionnées**, si vous souhaitez comparer les deux révisions dont vous avez coché les cases à l'étape 3.

     L'ordre dans lequel vous cochez les cases n'a aucune incidence sur les résultats de la comparaison. Par défaut, la version antérieure de la révision sélectionnée est comparée à la version la plus récente. Par exemple, si vous cochez les cases en regard des révisions 5 et 1, la révision 1 est comparée à la révision 5. Le rapport contiendra des informations sur les paramètres de la révision 1 qui ont été ajoutés, supprimés ou modifiés par rapport à la révision 5.

- **Avec une autre révision de la stratégie**, si vous souhaitez comparer les révisions de deux stratégies différentes.

  Dans le volet droit qui s'ouvre, réalisez les opérations suivantes :

  a. Dans le champ **Nom de l'application**, sélectionnez la partie dont vous souhaitez comparer la stratégie : Agent d'administration ou Serveur d'administration.

  b. Dans le champ **Nom de la stratégie**, indiquez le nom de la stratégie dont vous souhaitez comparer la révision avec celle que vous avez sélectionnée à l'étape 3.

  La liste des révisions de la stratégie s'affiche.

  c. Sélectionnez la révision souhaitée, puis cliquez sur le bouton **Comparer**.

Un rapport comparatif des révisions s'affiche au format HTML dans un nouvel onglet de votre navigateur.

Si le résultat de la comparaison dépasse 10 Mo, la boîte de dialogue correspondante s'affiche. Vous pouvez soit cliquer sur le bouton **Enregistrer dans un fichier** pour enregistrer le rapport dans un fichier, soit annuler l'opération.

Le rapport s'affiche dans la langue d'interface de Kaspersky Security Center Web Console. Vous pouvez développer certaines sections du rapport en cliquant sur l'icône en forme de flèche vers le bas (▼) en regard de la section ou réduire la section en cliquant sur la flèche vers le haut (▲).

Le rapport contient les informations suivantes :

- Le logo de Kaspersky.
- Le nom du rapport.
- La date et l'heure de création du rapport.
- Le nom de la stratégie, le Serveur d'administration et le groupe d'administration qui inclut la stratégie (les stratégies) dont les révisions ont été comparées.
- Le bouton **Enregistrer au format HTML**. Si vous cliquez sur le bouton, le rapport sera enregistré sur votre ordinateur.
- La section **Résumé** qui affiche des informations générales sur les révisions comparées : nom de la ou des stratégies, numéro de révision, heure et date de sauvegarde de la révision, nom de l'utilisateur ayant enregistré la révision et description de la révision.

  Pour les stratégies héritées, l'utilisateur ne s'affiche pas.

- Différences entre les révisions comparées. Les différences sont affichées dans les sections suivantes :
  - **Paramètres ajoutés**
  - **Paramètres supprimés**
  - **Paramètres modifiés**

- **Paramètres uniquement disponibles pour l'objet 1** (si vous avez comparé les révisions de deux stratégies différentes)
- **Paramètres uniquement disponibles pour l'objet 2** (si vous avez comparé les révisions de deux stratégies différentes)

Une section ne s'affiche pas si elle ne contient aucune donnée.

Pour les stratégies de Kaspersky Endpoint Security for Windows et de Kaspersky Endpoint Security for Mac, le rapport de comparaison des révisions ne contiendra aucune information concernant les profils de stratégie.

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.

Menaces actives

Les informations sur les fichiers non traités détectés sur les appareils clients se trouvent dans le dossier **Stockages**, dans le sous-dossier **Menaces actives**.

Le traitement différé et la désinfection des fichiers de l'application de sécurité sont effectués à la demande ou après la survenue d'un événement déterminé. Vous pouvez configurer les paramètres de désinfection différée des fichiers.

Désinfection d'un fichier non traité

Pour lancer la désinfection d'un fichier non traité, procédez comme suit :

1. Dans le menu principal, accédez à **Opérations** → **Stockages** → **Menaces actives**.
2. Exécutez une des actions suivantes :
   - Cochez la case en regard du fichier à désinfecter.
   - Cliquez sur le nom du fichier à désinfecter.
3. Lancez la désinfection du fichier en cliquant sur le bouton **Réparer**.

   La tentative de désinfection du fichier sélectionné est alors lancée.

Si le fichier est réparé, l'application de sécurité installée sur l'appareil client le restaure dans le dossier d'origine. L'entrée correspondant au fichier est supprimée de la liste dans la section **Menaces actives**. Si la désinfection du fichier est impossible, l'application de sécurité installée sur l'appareil supprime le fichier de l'appareil. L'entrée correspondant au fichier est supprimée de la liste dans la section **Menaces actives**.

> La capacité de désinfection et de suppression des fichiers peut varier en fonction de l'application de sécurité installée, de la version et des paramètres de l'application.

Téléchargement d'un fichier non traité

Kaspersky Security Center Linux permet de télécharger des copies des fichiers non traités sur les appareils clients. Il s'agit des fichiers traités ou supprimés par l'application. Les fichiers sont téléchargés dans le dossier spécifié sur l'appareil sur lequel Kaspersky Security Center Linux est installé.

Vous pouvez télécharger des copies de fichiers si ceux-ci ont été modifiés ou supprimés lors de la désinfection et si ces copies sont stockées dans le stockage de Kaspersky Endpoint Security for Linux sur l'appareil administré.

Pour télécharger une copie d'un fichier non traité, procédez comme suit :

1. Dans le menu principal, accédez à **Opérations** → **Stockages** → **Menaces actives**.
2. Exécutez une des actions suivantes :
   - Cochez la case en regard du fichier à télécharger.
   - Cliquez sur le nom du fichier à télécharger.
3. Lancez le téléchargement en cliquant sur le bouton **Télécharger**.

Ainsi, l'application de sécurité de l'appareil client sur lequel le fichier non traité a été détecté télécharge une copie du fichier dans le dossier indiqué.

Suppression des fichiers de la section Menaces actives

*Pour supprimer un fichier de la section **Menaces actives**, procédez comme suit :*

1. Dans le menu principal, accédez à **Opérations** → **Stockages** → **Menaces actives**.
2. Exécutez une des actions suivantes :
   - Cochez la case en regard du fichier à supprimer.
   - Cliquez sur le nom du fichier à supprimer.
3. Supprimez les fichiers en cliquant sur le bouton **Supprimer**.
4. Dans la fenêtre qui s'ouvre, cliquez sur **Supprimer**.

   Ainsi, les applications de sécurité qui ont placé les fichiers sélectionnés dans les stockages sur les appareils clients suppriment les fichiers de ces stockages. Les enregistrements des fichiers sont supprimés de la liste dans la section **Menaces actives**.

Suppression d'objets

Cette section fournit des informations sur la suppression d'objets.

Vous pouvez supprimer les objets suivants :

- Stratégies
- Tâches
- Paquets d'installation
- Serveurs d'administration virtuels
- Utilisateurs
- Groupes de sécurité
- Groupes d'administration

Pour supprimer un objet, procédez comme suit :

1. Ouvrez la section requise de Kaspersky Security Center Web Console, puis sélectionnez l'objet.
2. Dans la barre d'outils, cliquez sur le bouton **Supprimer**.
3. Dans la fenêtre qui s'ouvre, cliquez **OK** pour confirmer votre choix.

   L'objet sélectionné est supprimé.

Quand vous supprimez un objet, les informations à son sujet demeurent dans la base de données. La durée de stockage des informations relatives aux objets supprimés est identique à la période de stockage des révisions de l'objet (la période recommandée est de 90 jours). Vous pouvez modifier la durée de conservation uniquement si vous possédez la permission **Modifier** dans la zone de privilèges **Objets supprimés**.

À propos de la suppression des appareils clients

Lorsque vous supprimez un appareil administré d'un groupe d'administration, l'application place l'appareil dans le groupe Appareils non définis. Après la suppression de l'appareil, les applications Kaspersky installées (Agent d'administration et toute application de sécurité, par exemple, Kaspersky Endpoint Security) restent sur l'appareil.

Kaspersky Security Center 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.

> Dans VDI, si vous disposez d'un appareil avec des disques chiffrés, les informations contenues sur le disque chiffré sont supprimées après la suppression de l'appareil.

Lorsque vous supprimez manuellement un appareil du groupe Appareils non définis, l'application supprime l'appareil de la liste. Après la suppression de l'appareil, les applications Kaspersky installées (le cas échéant) restent sur l'appareil. Ensuite, si l'appareil est toujours visible pour le Serveur d'administration et que vous avez configuré le sondage du réseau régulier, Kaspersky Security Center 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 des fichiers de la Quarantaine et de la Sauvegardes de fichiers

Cette section explique comment télécharger et supprimer des fichiers de la Quarantaine et de la Sauvegardes de fichiers dans Kaspersky Security Center Web Console.

Téléchargement de fichiers à partir de la Quarantaine et des Sauvegardes de fichiers

Vous ne pouvez télécharger des fichiers depuis la Quarantaine et les Sauvegardes de fichiers 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 de la Sauvegardes de fichiers 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** → **Sauvegardes de fichiers**.

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 stockages Quarantaine, Sauvegardes de fichiers 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**, **Sauvegardes de fichiers**, ou alors **Menaces actives** dans Kaspersky Security Center Linux. Lorsque vous ouvrez l'une de ces sections, vous pouvez supprimer l'objet requis.

Pour la section **Sauvegardes de fichiers** ou **Menaces actives**, sélectionnez un objet dans la liste et cliquez sur le bouton **Supprimer**.

Pour la section **Quarantaine**, vous pouvez effectuer l'une des opérations suivantes :

- Cochez la case en regard du nom de l'objet à supprimer, puis dans la barre d'outils, cliquez sur le bouton **Supprimer**.
- Cliquez sur le nom de l'objet à supprimer, puis dans la fenêtre de détails qui s'ouvre, cliquez sur le bouton **Supprimer** dans la barre d'outils.

  Dans ce cas, l'objet est supprimé, une notification correspondante s'affiche à l'écran, et la fenêtre de détails se ferme.

Kaspersky Security Center Linux supprime l'objet sélectionné de la liste ou le supprime du stockage. 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**.

Pour en savoir plus sur les actions à effectuer, consultez la documentation de l'application Kaspersky.

Gestion des applications via le protocole SNMP

Cette section explique comment obtenir des informations à partir du Serveur d'administration en utilisant le protocole SNMP (Simple Network Management Protocol) sous Linux.

SNMP est un protocole permettant de gérer les appareils réseau.

Pour fonctionner via le protocole SNMP, Kaspersky Security Center Linux utilise le service snmpd intégré au système d'exploitation ainsi qu'un agent SNMP afin de surveiller les performances du Serveur d'administration et d'envoyer des données à des applications tierces à l'aide d'identificateurs d'objets (OID). Kaspersky Security Center Linux peut transmettre ces informations sous forme de statistiques ou de traps SNMP, qui sont des notifications concernant les événements liés aux applications.

Le protocole SNMP vous permet d'accéder aux informations suivantes concernant l'application :

- Informations générales
- Statistiques de Kaspersky Security Center Linux depuis l'installation de l'application
- Informations sur les événements de Kaspersky Security Center Linux

Un accès en lecture seule est accordé.

Les informations relatives aux traps SNMP et aux statistiques transmises via le protocole SNMP sont stockées dans le fichier adminkit.mib. Par défaut, le fichier adminkit.mib se trouve dans le dossier /opt/kaspersky/ksc64/share/snmp/.

Le service snmpd local sur chaque nœud du cluster fait office de serveur SNMP chargé de recevoir les statistiques. L'interaction avec un serveur SNMP externe n'est pas prise en charge. Les traps SNMP peuvent être reçus localement sur chaque nœud du cluster à l'aide du service snmptrapd, ou bien redirigés vers un serveur externe.

Pour les opérations via le protocole SNMP, préconfigurez le service snmpd dans le système d'exploitation de chaque nœud du cluster.

Configuration du service snmpd dans le système d'exploitation

Avant de procéder à la configuration, assurez-vous que le service snmpd est installé sur votre système d'exploitation.

Création d'un compte utilisateur pour accéder aux données

Avant de créer le compte, arrêtez le service snmpd en exécutant la commande suivante :

```
bash
sudo systemctl stop snmpd
```

Pour garantir la sécurité de l'accès aux données via le protocole SNMPv3 avec authentification et chiffrement, vous devez créer un compte utilisateur du côté du service snmpd en utilisant les informations suivantes :

- Nom d'utilisateur (sensible à la casse)
- Algorithme d'authentification (MD5 ou SHA – SHA est recommandé)
- Mot de passe d'authentification
- Algorithme de chiffrement (uniquement AES pris en charge)
- Mot de passe de chiffrement

Vous pouvez créer un compte utilisateur comme suit :

- A l'aide de l'utilitaire net-snmp-create-v3-user, s'il est disponible dans le système d'exploitation.
- Manuellement en ajoutant la directive appropriée dans le fichier de configuration du service snmpd.

Pour créer un compte utilisateur à l'aide de l'utilitaire net-snmp-create-v3-user, exécutez la commande suivante :

```
net-snmp-create-v3-user -ro -a <algorithme d'authentification> -x <algorithme de chiffrement> <nom d'utilisateur>
```

Les mots de passe d'authentification et de chiffrement sont demandés de façon interactive.

Par exemple :

```
net-snmp-create-v3-user -ro -a SHA -x AES MonitoringUser
```

Pour créer manuellement un compte utilisateur, procédez comme suit :

1. Créez le fichier de configuration /var/lib/snmp/snmpd.conf en exécutant la commande suivante :

```
touch /var/lib/snmp/snmpd.conf
```

2. Ajoutez les lignes suivantes au fichier de configuration :

```
createUser <nom d'utilisateur> <algorithme d'authentification> "<mot de passe d'authentification>" <algorithme
de chiffrement> "<mot de passe de chiffrement>"
```

   Par exemple :

```
createUser MonitoringUser SHA "MonitoringAuthSecret" AES "MonitoringPrivSecret"
```

Création d'un compte utilisateur pour la réception de traps SNMP

Pour recevoir des traps SNMP via le protocole SNMPv3 avec authentification et chiffrement, vous devez créer un compte au niveau du système de surveillance dans le cadre du service correspondant (généralement le service snmptrapd).

Le compte doit contenir les informations suivantes :

- Nom d'utilisateur.
- Algorithme d'authentification
- Mot de passe d'authentification
- Algorithme de chiffrement
- Mot de passe de chiffrement

> Pour des raisons de sécurité, utilisez des comptes utilisateurs distincts pour l'accès aux données et pour la réception des traps SNMP.

Pour en savoir plus sur la création d'un compte utilisateur permettant de recevoir des traps SNMP, consultez la documentation de votre système de surveillance.

Configuration du service snmpd

La configuration du service snmpd est enregistrée dans le fichier /etc/snmp/snmpd.conf. Vous pouvez ajouter les informations nécessaires à un fichier de configuration existant ou créer un autre fichier de configuration et y ajouter les lignes ci-dessous, dans l'ordre indiqué.

Si vous choisissez de créer un autre fichier de configuration, assurez-vous que seul l'administrateur y a accès. Si les autorisations d'accès requises ne sont pas définies, configurez-les en exécutant les commandes suivantes dans l'ordre indiqué :

```
chown root:root /etc/snmp/snmpd.conf
chmod 600 /etc/snmp/snmpd.conf
```

Pour configurer le service snmpd, procédez comme suit :

1. Dans le fichier de configuration, indiquez le protocole, l'adresse de l'interface réseau et le numéro de port sur lesquels le service snmpd doit écouter les requêtes entrantes.

   - Si vous souhaitez écouter les requêtes sur toutes les interfaces réseau, ajoutez les lignes suivantes au fichier de configuration :

     ```
     agentAddress udp:161
     ```

   - Si vous souhaitez écouter les demandes uniquement sur l'interface réseau locale, par exemple si le système de surveillance est installé sur la même machine, ajoutez les lignes suivantes au fichier de configuration :

     ```
     agentAddress udp:127.0.0.1:161
     ```

2. Configurez l'interaction entre Kaspersky Security Center Linux et le service snmpd. Vous pouvez utiliser soit un socket UNIX, soit un socket TCP.

   - Si vous utilisez un socket UNIX :

     a. Indiquez le chemin d'accès et les autorisations pour le socket UNIX. Pour cela, ajoutez les lignes suivantes dans le fichier de configuration :

     ```
     master agentx
     agentXSocket unix:/var/run/agentx-master.socket
     agentXPerms 770 770 kluser klusers
     ```

     b. Ajoutez le groupe klusers en tant que groupe supplémentaire pour le compte {'KLSRV_UNATT_KLSVCUSER'}.

   - Si vous utilisez un socket TCP, indiquez le port et l'adresse du socket TCP. Pour cela, ajoutez les lignes suivantes dans le fichier de configuration :

     ```
     master agentx
     agentXSocket tcp:127.0.0.1:705,tcp6:[::1]:705
     ```

3. Définissez le délai d'attente minimum de réponse sur au moins 30 secondes. Pour cela, ajoutez les lignes suivantes dans le fichier de configuration :

```
agentxTimeout 30
```

4. Si nécessaire, vous pouvez fournir une description du serveur sur lequel SNMP est configuré, l'emplacement du système et les coordonnées de l'administrateur. Pour cela, ajoutez les lignes suivantes dans le fichier de configuration :

```
sysDescr <description du serveur>
sysLocation <localisation du serveur>
sysContact <adresse de contact de l'administrateur>
sysServices 72
```

5. Précisez la portée de l'arborescence OID que vous souhaitez rendre accessible à votre système de surveillance via le protocole SNMP. Pour cela, ajoutez les lignes suivantes dans le fichier de configuration :

```
view monitoring included .1.3.6.1.4.1.23668.1093.1

view systemonly included .1.3.6.1.4.1.23668.1093.1
```

6. Si nécessaire, vous pouvez également définir la portée de l'arborescence OID contenant les informations relatives au système d'exploitation qui sont stockées par le service snmpd. Cette portée sera disponible pour votre système de surveillance.

   Les informations relatives au système d'exploitation comprennent, par exemple, des données sur l'utilisation du processeur et de la mémoire vive, l'espace libre sur les partitions de disque, la charge des interfaces réseau, une liste des logiciels installés, une liste des connexions réseau actives et une liste des processus en cours d'exécution. Certaines de ces informations peuvent être confidentielles.

   - Si vous souhaitez autoriser l'accès uniquement aux informations générales du système et aux informations concernant l'utilisation de la mémoire vive, du processeur et des appareils de stockage, ajoutez les lignes suivantes au fichier de configuration :

     ```
     # SNMPv2-MIB - Basic system information
     view monitoring included .1.3.6.1.2.1.1
     # HOST-RESOURCES-MIB - CPU, Memory, Filesystems
     view monitoring included .1.3.6.1.2.1.25.1
     view monitoring included .1.3.6.1.2.1.25.2
     view monitoring included .1.3.6.1.2.1.25.3
     view monitoring included .1.3.6.1.2.1.25.5
     # UCD-SNMP-MIB - Memory and CPU usage
     view monitoring included .1.3.6.1.4.1.2021.4
     view monitoring included .1.3.6.1.4.1.2021.10
     view monitoring included .1.3.6.1.4.1.2021.11
     # UCD-SNMP-DISKIO-MIB - Block devices I/O statistics
     view monitoring included .1.3.6.1.4.1.2021.13
     # IF-MIB - Network interfaces I/O statistics
     view monitoring included .1.3.6.1.2.1.2
     view monitoring included .1.3.6.1.2.1.31
     ```

   - Si vous souhaitez autoriser l'accès à toutes les informations système, ajoutez la ligne suivante au fichier de configuration :

     ```
     view monitoring included .1
     ```

7. Précisez le mode d'accès et l'étendue des informations pour le compte utilisateur créé. Pour cela, ajoutez les lignes suivantes dans le fichier de configuration :

```
rouser <user name> priv -V monitoring
```

8. Pour envoyer des traps SNMP, indiquez l'adresse IP du système de surveillance ainsi que les identifiants de l'utilisateur chargé de les recevoir. Pour cela, ajoutez les lignes suivantes dans le fichier de configuration :

```
trapsess -Ci -v3 -t0.1 -r1 -l authPriv -u <nom d'utilisateur pour la réception des traps> -a <algorithme
d'authentification> -A "<mot de passe utilisateur pour la réception des traps>" -x <algorithme de chiffrement>
-X "<mot de passe de chiffrement>" udp:<adresse IP>:162
```

Le service snmpd est configuré.

Pour assurer l'intégration avec plusieurs systèmes de surveillance, créez un compte utilisateur distinct pour chaque système, définissez l'étendue des informations disponibles pour chaque compte utilisateur (directives " view " et " rouser ") et configurez l'envoi de traps SNMP (directive " trapsess ").

Lancement du service snmpd avec la nouvelle configuration

Pour appliquer la nouvelle configuration, procédez comme suit :

1. Redémarrez le service snmpd :

```
systemctl restart snmpd
```

2. Vérifiez l'état du service snmpd :

```
systemctl status snmpd
```

L'état doit être le suivant : `running`.

3. Autorisez le démarrage automatique du service au lancement du système d'exploitation :

```
systemctl enable snmpd
```

4. Si vous utilisez un pare-feu dans votre système d'exploitation ou vos équipements réseau, ajoutez des règles pour autoriser le passage des paquets SNMP.

Le service snmpd est en cours d'exécution.

Si le service klcssnmp était en cours d'exécution au moment de la configuration du service snmpd, redémarrez également le service klcssnmp.

Vérification de l'état du service snmpd

Pour tester le service snmpd, configurez l'utilisation du protocole SNMP dans Kaspersky Security Center Linux, puis faites une demande de données SNMP à l'aide de l'utilitaire snmpwalk.

Pour connaître l'étendue des données SNMP fournies par Kaspersky Security Center Linux,

exécutez la commande suivante :

```
snmpwalk -v3 -l authPriv -u <nom d'utilisateur> -a <algorithme d'authentification> -A "<mot de passe
d'authentification>" -x <algorithme de chiffrement> -X "<mot de passe de chiffrement>" <adresse IP>
.1.3.6.1.4.1.23668.1093.1
```

Par exemple :

```
snmpwalk -v3 -l authPriv -u MonitoringUser -a SHA -A "MonitoringAuthSecret" -x AES -X "MonitoringPrivSecret"
127.0.0.1 .1.3.6.1.4.1.23668.1093.1
```

Activation et désactivation des notifications via le protocole SNMP

Kaspersky Security Center Linux envoie les notifications concernant les événements du Serveur d'administration sous forme de traps SNMP.

Par défaut, les notifications SNMP relatives aux événements de Kaspersky Security Center Linux sont désactivées.

Pour activer ou désactiver les notifications SNMP concernant les événements de Kaspersky Security Center Linux :

1. Dans le menu principal, cliquez sur le nom du Serveur d'administration.

   La fenêtre des **Propriétés du Serveur d'administration** s'ouvre.

2. Dans l'onglet **Configuration des événements** de la fenêtre des propriétés, cliquez sur le type d'événement pour lequel vous souhaitez recevoir les notifications SNMP.

3. Dans le panneau qui s'ouvre, activez ou désactivez le commutateur **Notifier via SNMP**.

   Cette option est disponible uniquement si l'option **Envoyer les statistiques par SNMP** est activée.

Les notifications SNMP pour les événements de Kaspersky Security Center Linux sont activées ou désactivées selon vos préférences.

Activation et désactivation du protocole SNMP dans Kaspersky Security Center Linux

Par défaut, l'envoi de statistiques via le protocole SNMP est activé. Pour envoyer des traps SNMP, configurez le service snmpd.

Pour activer ou désactiver l'envoi de statistiques via le protocole SNMP, procédez comme suit :

1. Dans le menu principal, cliquez sur le nom du Serveur d'administration.

   La fenêtre des **Propriétés du Serveur d'administration** s'ouvre.

2. Sous l'onglet **Général**, sélectionnez la section **par SNMP**.

3. Activez ou désactivez le commutateur **Envoyer les statistiques par SNMP**.

4. Cliquez sur **Enregistrer**.

L'envoi de statistiques via le protocole SNMP est activé ou désactivé selon vos préférences.

Valeurs des identificateurs d'objet pour SNMP

Dans le tableau ci-dessous figurent les valeurs et descriptions des identificateurs d'objet (également connu sous le nom de d'OID), utilisés pour transférer des informations sur les performances du Serveur d'administration vers des applications tierces.

Valeurs et descriptions des identificateurs d'objet pour SNMP

Valeur de l'identificateur d'objet	Type de données numériques	OID	Description
`deploymentStatus`	`INTEGER { ok(0), info(1), warning(2), critical(3) }`	.1.3.6.1.4.1.23668.1093.1.1.1	État du déploiement. L'état peut correspondre à l'un des cas de figure ci-après : • **Information**. La licence n'est plus valide pour N appareils. • **Avertissement**. Une des licences suivantes : Les applications Kaspersky sont installées sur M appareils sur un total de N appareils des groupes du Serveur d'administration (N > M). La licence L expire pour N appareils dans M jours. La tâche T d'installation des applications a été effectuée avec succès pour N appareils et un redémarrage est nécessaire pour les M appareils. • **Critique** Licence expirée pour N appareils. • **OK**. Aucune de ces réponses.
`noAntivirusSoftware`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.1.2.1	[[deploymentStatus]] indique que le groupe du Serveur d'administration contient trop d'appareils sans applications administrées. La valeur est égale à 1 si quelques appareils ne comportent pas d'application administrée et à 0 dans le cas contraire.
`remoteInstallTaskFailed`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.1.2.2	[[deploymentStatus]] indique que la tâche d'installation à distance a échoué sur certains appareils. Le nombre de ces appareils peut être obtenu par `hostsRemoteInstallFailed`.

Valeur de l'identificateur d'objet	Type de données numériques	OID	Description
`licenceExpiring`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.1.2.3	[[deploymentStatus]] indique que la licence pour certains appareils va expirer au cours des 7 jours suivants. Le nombre de ces appareils peut être obtenu via `hostsLicenseExpiring`.
`licenceExpired`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.1.2.4	[[deploymentStatus]] indique que la licence a expiré pour certains appareils. Vous pouvez obtenir le nombre de ces appareils via `hostsLicenseExpired`.
`hostsInGroups`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.1.3	Nombre d'appareils dans les groupes du Serveur d'administration.
`hostsWithAntivirus`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.1.4	Nombre d'appareils dans les groupes de Serveur d'administration avec des applications administrées installées
`hostsRemoteInstallFailed`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.1.5	Nombre d'appareils pour lesquels la tâche de l'installation à distance a échoué.
`licenceExpiringSerial`	`OCTET STRING`	.1.3.6.1.4.1.23668.1093.1.1.6	ID d'une clé de licence qui expire dans moins de 7 jours.
`licenceExpiredSerial`	`OCTET STRING`	.1.3.6.1.4.1.23668.1093.1.1.7	ID de la clé de licence expirée.
`licenceExpiringDays`	`Unsigned32`	.1.3.6.1.4.1.23668.1093.1.1.8	Nombre de jours restants avant l'expiration de la licence. Pour ce paramètre, la licence est considérée comme expirée s'il reste moins de 7 jours avant son expiration. S'il reste plus de 7 jours avant la date d'expiration, la valeur est 0.
`hostsLicenceExpiring`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.1.9	Nombre d'appareils dont la licence expire dans moins de 7 jours.
`hostsLicenceExpired`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.1.10	Nombre d'appareils dont la licence a expiré.
`updatesStatus`	`INTEGER { ok(0), info(1), warning(2), critical(3) }`	.1.3.6.1.4.1.23668.1093.1.2.1	État actuel de la mise à jour des bases antivirus. L'état peut correspondre à l'un des cas de figure ci-après : • **Information**. Les bases antivirus sur le Serveur d'administration ou sur les appareils n'ont pas été mises à jour depuis plus d'un jour et moins d'un jour s'est écoulé depuis l'installation de l'application. • **Avertissement**. Les bases antivirus sur le Serveur d'administration ou sur les appareils n'ont pas été mises à jour depuis plus de trois jours. Cette valeur peut être modifiée dans les paramètres du groupe. • **Critique** Les bases antivirus sur le Serveur d'administration ou sur les appareils n'ont pas été mises à jour depuis plus de sept jours. Cette valeur peut être modifiée dans les paramètres du groupe. • **OK**. Aucune de ces réponses.
`serverNotUpdated`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.2.2.1	Une mise à jour du Serveur d'administration n'a pas été effectuée depuis longtemps. La période considérée comme longue est spécifiée dans `updatesStatus`.
`notUpdatedHosts`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.2.2.2	Certains appareils n'ont pas été mis à jour depuis un certain temps (par défaut, 7 jours ou plus pour **Critique** et 3 jours pour **Avertissement**). Vous pouvez obtenir le nombre de ces appareils via `hostsNotUpdated`.
`lastServerUpdateTime`	`Hex-STRING`	.1.3.6.1.4.1.23668.1093.1.2.3	Mise à jour la plus récente des bases antivirus sur le Serveur d'administration.
`hostsNotUpdated`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.2.4	Nombre d'appareils contenant des bases antivirus qui n'ont pas été mises à jour depuis longtemps (par défaut, 7 jours ou plus pour **Critique** et 3 jours pour **Avertissement**). S'il existe des appareils avec l'état de mise à jour **Critique**, seuls ces appareils sont comptabilisés. Vous pouvez obtenir l'état de la mise à jour via `updatesStatus`.

Valeur de l'identificateur d'objet	Type de données numériques	OID	Description
`protectionStatus`	`INTEGER { ok(0), warning(2), critical(3) }`	.1.3.6.1.4.1.23668.1093.1.3.1	État de la protection en temps réel. Une des licences suivantes : • **Avertissement**. Une des licences suivantes : une faille de sécurité est détectée sur un appareil appartenant au groupe de Serveur d'administration. Des erreurs de chiffrement ont conduit certains appareils à modifier l'état de la protection. Une analyse complète n'a pas été effectuée depuis longtemps. • **Critique** La protection antivirus ne fonctionne pas sur certains appareils des groupes de Serveur d'administration. • **OK**. Aucune de ces réponses.
`antivirusNotRunning`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.3.2.1	Une application de sécurité n'est pas exécutée sur certains appareils. Vous pouvez obtenir le nombre de ces appareils via `hostsAntivirusNotRunning`.
`realtimeNotRunning`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.3.2.2	La protection en temps réel n'est pas exécutée sur certains appareils. Vous pouvez obtenir le nombre de ces appareils via `hostsRealtimeNotRunning`.
`psRealtimeLevelChanged`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.3.2.3	Le niveau de protection pendant l'exécution diffère de celui défini par l'administrateur sur les ordinateurs N appartenant aux groupes d'administration.
`notCuredFound`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.3.2.4	Des appareils contiennent des objets non désinfectés. Vous pouvez obtenir le nombre de ces appareils via `hostsNotCuredObject`.
`tooManyThreats`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.3.2.5	Des menaces ont été détectées sur certains appareils. Vous pouvez obtenir le nombre de ces appareils via `hostsTooManyThreats`.
`virusOutbreak`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.3.2.6	L'état de la propagation du virus dans le système. La valeur est égale à 1 si une certaine quantité de virus a été détectée pendant un certain temps, et à 0 dans le cas contraire. La quantité de virus et la durée sont spécifiées sur le Serveur d'administration, en utilisant les paramètres d'`Virus attack`.
`psVulnerabilitiesFound`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.3.2.7	Des vulnérabilités ont été détectées.
`psEncryptionFaultsFound`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.3.2.8	Des erreurs de chiffrement ayant modifié l'état de protection de l'appareil ont été détectées.
`psVulnerableHostsFound`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.3.2.9	Des vulnérabilités ont été détectées sur certains appareils.
`psNotScannedLately`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.3.2.10	Des appareils n'ayant pas fait l'objet d'une analyse complète depuis longtemps ont été détectés.
`psNagentsNotRunningUntilReboot`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.3.2.11	Des appareils sur lesquels l'Agent d'administration ne démarre qu'après un redémarrage ont été détectés.
`hostsAntivirusNotRunning`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.3.3	Nombre d'appareils dont les applications de sécurité ne fonctionnent pas.
`hostsRealtimeNotRunning`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.3.4	Nombre d'appareils pour lesquels la protection en temps réel ne fonctionne pas.
`hostsRealtimeLevelChanged`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.3.5	Le nombre d'appareils dont le niveau de protection en temps réel n'est pas acceptable.
`hostsNotCuredObject`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.3.6	Nombre d'appareils contenant des objets non désinfectés.

Valeur de l'identificateur d'objet	Type de données numériques	OID	Description
`hostsTooManyThreats`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.3.7	Nombre d'appareils contenant des menaces.
`fullscanStatus`	`INTEGER { ok(0), info(1), warning(2), critical(3) }`	.1.3.6.1.4.1.23668.1093.1.4.1	L'état de l'analyse complète dans le cadre de la recherche de virus est l'un des suivants : • **Information**. Moins de 7 jours se sont écoulés depuis le moment où l'application a été installée. • **Avertissement**. L'analyse complète de l'antivirus n'a pas été effectuée depuis plus de 7 jours à compter du moment de l'installation de l'application. • **Critique** L'analyse complète de l'antivirus n'a pas été effectuée depuis plus de 14 jours à compter du moment de l'installation de l'application. • **OK**. Aucune de ces réponses.
`notScannedLately`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.4.2.1	Certains appareils n'ont pas été analysés depuis un certain temps. Vous pouvez obtenir le nombre de ces appareils via `hostsNotScannedLately`. La durée est spécifiée dans `fullScanStatus`.
`hostsNotScannedLately`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.4.3	Nombre d'appareils qui n'ont pas été analysés depuis un certain temps. La durée est spécifiée dans `fullScanStatus`.
`logicalNetworkStatus`	`INTEGER { ok(0), warning(1), critical(2) }`	.1.3.6.1.4.1.23668.1093.1.5.1	État du réseau logique du Serveur d'administration. Une des licences suivantes : • **Avertissement**. S'il existe des appareils inaccessibles dont l'état est " avertissement " qui ne sont pas accessibles ou lorsque des appareils n'appartiennent à aucun groupe du Serveur d'administration. • **Critique** Lorsqu'il existe des appareils dont le Serveur d'administration a perdu le contrôle, ou des appareils dont l'état est critique et qui ne sont pas accessibles. • **OK**. Aucune de ces réponses.
`notConnectedLongTime`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.5.2.1	Certains appareils ne sont pas connectés au Serveur d'administration depuis longtemps (7 jours ou plus pour un appareil dont l'état est **Avertissement** et 4 jours pour un appareil dont l'état est **Critique**). Vous pouvez obtenir le nombre de ces appareils via `hostsNotConnectedLongTime`.
`controlLost`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.5.2.2	Il existe des appareils dont le Serveur d'administration a perdu le contrôle. Vous pouvez obtenir le nombre de ces appareils via `hostsControlLost`.
`hostsFound`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.5.3	Nombre d'appareils détectés par le Serveur d'administration qui n'appartiennent à aucun groupe de Serveur d'administration.
`groupsCount`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.5.4	Nombre de groupes sur le Serveur d'administration.
`hostsNotConnectedLongTime`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.5.5	Nombre d'appareils qui n'ont pas été connectés au Serveur d'administration depuis longtemps. La période considérée comme longue est spécifiée dans `notConnectedLongTime`.
`hostsControlLost`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.5.6	Nombre d'appareils qui ne sont pas contrôlés par le Serveur d'administration.

Valeur de l'identificateur d'objet	Type de données numériques	OID	Description
`eventsStatus`	`INTEGER { ok(0), info(1), warning(2), critical(3) }`	.1.3.6.1.4.1.23668.1093.1.6.1	L'état du sous-système d'événements est l'un des suivants : • **Avertissement**. Une des licences suivantes : Les appareils du groupe du Serveur d'administration n'ont pas recherché de mises à jour Windows depuis longtemps. Il existe des appareils présentant des problèmes d'état. • **Critique** L'un des cas suivants : Il y a un événement " critique " sur au moins un appareil. Il y a un événement de niveau " Erreur " sur au moins un appareil. Un échec de l'exécution de la tâche est survenu sur au moins un appareil. Les appareils du groupe du Serveur d'administration n'ont pas recherché de mises à jour Windows depuis longtemps. Il existe des appareils présentant des problèmes d'état. • **Info** L'un des cas suivants : Moins d'une semaine s'est écoulée depuis la dernière recherche de virus complète effectuée sur tous les appareils. Les tâches d'installation à distance sont terminées et aucun appareil ne doit être redémarré. Moins d'une semaine s'est écoulée depuis la dernière mise à jour du Serveur d'administration. Le Serveur d'administration n'a pas été mis à jour depuis longtemps, mais une mise à jour est actuellement en cours. • **OK**. Aucune de ces réponses.
`criticalEventOccured`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.6.2.1	[[eventsStatus]] indique que des événements critiques sont survenus sur le Serveur d'administration. Vous pouvez obtenir le nombre de ces événements via `criticalEventsCount`. La valeur est égale à 1 lorsqu'au moins un événement critique est survenu sur un appareil, quel qu'il soit, et à 0 dans le cas contraire.
`criticalEventsCount`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.6.3	Nombre d'événements critiques sur le Serveur d'administration.

Utilisation de Kaspersky Security Center Linux sous licence pour Kaspersky Next XDR Optimum

Si vous avez acheté une licence pour Kaspersky Next XDR Optimum dans le cadre d'une licence de l'application EPP et d'une licence pour Kaspersky Security Center Linux, vous pourrez utiliser les fonctionnalités de Kaspersky Next XDR Optimum après avoir exécuté la configuration initiale.

Si, après l'installation et l'activation des applications Kaspersky sur les appareils, vous avez acheté la licence pour Kaspersky Next XDR Optimum séparément en tant qu'extension d'une licence achetée précédemment, vous devez réactiver Kaspersky Security Center Linux sur les appareils à l'aide du nouveau code d'activation ou du nouveau fichier clé, selon la manière dont vous avez acheté la licence pour Kaspersky Next XDR Optimum. Ensuite, vous pouvez exécuter la configuration initiale.

Vous pouvez également utiliser la fonctionnalité de Kaspersky Next XDR Optimum en mode test. Pour ce faire, vous devez d'abord ajouter un Serveur d'administration physique secondaire, puis activer ce Serveur sous votre licence d'évaluation Kaspersky Next XDR Optimum. La fonctionnalité de Kaspersky Next XDR Optimum sera disponible sur le Serveur secondaire pendant la durée de votre licence d'évaluation.

Après avoir activé le Serveur d'administration sous votre licence Kaspersky Next XDR Optimum et déployé la clé de licence sur les appareils gérés par le Serveur d'administration concerné, vous pouvez effectuer les opérations suivantes :

- Réagir aux menaces à l'aide d'intégrations à Kaspersky Automated Security Awareness Platform, Kaspersky Threat Intelligence Portal Sandbox et Active Directory.
- Regrouper les alertes par attributs.

Pour en savoir plus sur les fonctionnalités activées par la licence pour Kaspersky Next XDR Optimum, consultez l'Aide de Kaspersky Endpoint Detection and Response Optimum.

Intégrations pour la réponse aux alertes

Si vous disposez de la licence pour Kaspersky Next XDR Optimum, vous pouvez configurer des intégrations avec les solutions suivantes afin de répondre aux menaces :

- Kaspersky Automated Security Awareness Platform
- Kaspersky Threat Intelligence Portal Sandbox
- Active Directory

Ces intégrations sont disponibles si vous avez activé le Serveur d'administration avec une licence pour Kaspersky Next XDR Optimum.
Pour effectuer des actions de réponse, vous devez déployer la clé de licence Kaspersky Next XDR Optimum sur vos applications administrées.
Lorsque vous utilisez la fonctionnalité Kaspersky Next XDR Optimum avec une licence d'évaluation, vous devez d'abord ajouter un Serveur d'administration secondaire physique, activer ce Serveur d'administration secondaire avec la licence d'évaluation, puis déployer la clé de licence sur vos appareils gérés par ce Serveur d'administration.

Si vous utilisez la licence pour Kaspersky Next EDR Optimum, vous n'avez pas besoin d'activer les applications installées sur vos appareils administrés sous la licence pour Kaspersky Next XDR Optimum. Vous devez le faire uniquement pour les nouveaux appareils, le cas échéant.

Étant donné que la licence Kaspersky Next XDR Optimum prend en charge la multilocation, vous pouvez distribuer de manière centralisée la clé de licence aux applications gérées. La distribution automatique de la licence aux Serveurs d'administration virtuels et secondaires n'est pas prise en charge.

Pour configurer les intégrations, vous devez disposer des droits **de lecture** et **d'écriture** pour la zone fonctionnelle **Fonctionnalités générales : Intégration d'applications**.

Configuration de l'intégration à Active Directory pour l'exécution des actions de réponse

L'intégration à Active Directory vous permet d'exécuter des actions de réponse pour les utilisateurs d'Active Directory affectés par l'alerte ou impliqués dans celle-ci.

Pour configurer l'intégration à Active Directory afin de répondre aux alertes, vous devez utiliser la version 15.4 ou une version ultérieure du Serveur d'administration de Kaspersky Security Center Linux.

L'intégration à Active Directory pour répondre aux alertes et les paramètres d'analyse du contrôleur de domaine Active Directory (l'adresse et les identifiants utilisateur du contrôleur de domaine) que vous spécifiez lors de la configuration d'un sondage du contrôleur de domaine sont deux paramètres distincts. Étant donné que vous devez vous assurer que l'utilisateur pour lequel une action de réponse doit être exécutée dispose d'un compte Active Directory, vous devez configurer les deux intégrations, pour l'analyse et pour la réponse. L'ordre est sans importance.

Les paramètres d'intégration ne sont pas hérités et s'appliquent uniquement au Serveur d'administration (physique ou virtuel) sur lequel vous configurez ces paramètres.

Pour configurer l'intégration à Active Directory afin de répondre aux alertes, procédez comme suit :

1. Dans le menu principal, cliquez sur le nom du Serveur d'administration.

   La fenêtre des propriétés du Serveur d'administration s'ouvre avec l'onglet **Général** sélectionné.

2. Exécutez une des actions suivantes :

   - Sélectionnez la section **Points de distribution**, cliquez sur le nom du point de distribution requis, puis dans la fenêtre des propriétés qui s'ouvre, sélectionnez la section **Active Directory**.

   - Sélectionnez la section **Réponse d'Active Directory**.

3. Dans le volet droit, activez le commutateur **Intégration d'Active Directory**.

   Par la suite, si vous souhaitez désactiver l'intégration, vous ne pouvez le faire que pour toutes les connexions, en désactivant le commutateur **Intégration d'Active Directory**. Vous ne pouvez pas désactiver l'intégration pour une connexion spécifique. À la place, vous pouvez supprimer la connexion.

   > Lorsque vous activez ou désactivez le commutateur **Intégration d'Active Directory**, le paramètre est appliqué à la fois à la section **Réponse d'Active Directory** et à la section **Points de distribution**.

4. Créez une connexion au contrôleur de domaine Active Directory en cliquant sur le bouton **Ajouter**.

5. Dans la fenêtre qui s'ouvre, précisez les paramètres suivants pour la connexion :

   - **Adresse du contrôleur de domaine**

     Nom de l'ordinateur, par exemple : `server.mycompany.com`.

     Vous pouvez spécifier plusieurs adresses. Tous les contrôleurs de domaine dont vous spécifiez les adresses doivent appartenir au même domaine.

   - **Nom de domaine Active Directory**

     Nom de domaine DNS complet, par exemple : `mycompany.com`

     Vous pouvez également spécifier un nom SAM ou NetBIOS, par exemple : `mycompany`

     Utilisez des lettres minuscules. Si vous créez plusieurs connexions pour le Serveur d'administration ou un point de distribution, spécifiez des noms différents pour chaque connexion.

     > Pour que les mesures de réponse puissent être exécutées, le nom de domaine Active Directory que vous indiquez dans ce champ doit correspondre au nom de domaine Active Directory spécifié dans l'alerte.

   - **Identifiant**

     Identifiant du compte Active Directory disposant des privilèges d'administrateur et sous lequel les actions de réponse doivent être exécutées.

   - **Mot de passe**

     Mot de passe du compte Active Directory disposant des privilèges d'administrateur et sous lequel les actions de réponse doivent être exécutées.

6. Si vous souhaitez vérifier l'état de la connexion, cliquez sur le bouton **Analyser la connexion**.

   Si la connexion est établie avec succès, l'état **Connecté** s'affiche. Sinon, l'état indiqué est **Échec**, et un message d'erreur s'affiche avec les contrôleurs de domaine auxquels vous n'avez pas réussi à vous connecter.

Vous devez tenir compte du mode de connexion à Active Directory : **à partir d'un appareil Linux ou à partir d'un appareil Windows**.

Connexion à partir d'un appareil Linux

Par défaut, lors de la connexion et de l'authentification auprès d'un contrôleur de domaine à partir d'un appareil Linux, la logique est la suivante :

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

   Une vérification stricte du certificat du serveur LDAP est effectuée.

2. Vous placez la partie publique du certificat du contrôleur de domaine dans le stockage des certificats système pour valider le certificat.

   Le chemin d'accès à l'autorité de certification (CA) du système dépendant du système d'exploitation permet d'accéder à la chaîne de certification.

   Par exemple :

   - /etc/ssl/certs/ca-certificates.crt : chemin d'accès pour les systèmes d'exploitation basés sur Debian (Debian, Ubuntu, Astra).
   - /etc/pki/ca-trust/extracted/pem/tls-ca-bundle.pem : chemin d'accès pour CentOS ou Red Hat.

3. Si la connexion LDAPS échoue, une erreur se produit et aucun autre protocole de connexion n'est utilisé.

   En cas de problème avec LDAPS, vous pouvez contacter le support technique de Kaspersky.

Si vous ne souhaitez pas installer le certificat dans le stockage des certificats système, vous pouvez définir le chemin d'accès au certificat du contrôleur de domaine à l'aide de l'indicateur KLNAG_LDAP_SSL_CACERT. Pour ce faire, exécutez la commande :

```
klscflag -fset -pv klnagent -n KLNAG_LDAP_SSL_CACERT -t s -v "</path/to/domain-controller/cert>"
```

où `</path/to/domain-controller/cert>` est le chemin d'accès à la partie publique du certificat du contrôleur de domaine.

Par exemple, si le chemin d'accès est `"/var/opt/kaspersky/ldap_cert.crt"`, la commande est `klscflag -fset -pv klnagent -n KLNAG_LDAP_SSL_CACERT -t s -v "/var/opt/kaspersky/ldap_cert.crt"`

Connexion à partir d'un appareil Windows

Lors de la connexion et de l'authentification auprès d'un contrôleur de domaine à partir d'un appareil Windows, les paramètres de connexion sont définis par le domaine.

Vous devez simplement vous assurer que :

- LDAPS est activé et le port 636 est disponible sur l'appareil.
- Vous autorisez les connexions au contrôleur de domaine via un pare-feu ou un serveur proxy.

7. Cliquez sur **Enregistrer**.

La fenêtre se ferme et la connexion s'affiche dans le tableau des connexions.

Dans le tableau des connexions, vous pouvez effectuer l'une des opérations suivantes :

- Modifier les paramètres de connexion.

  Pour ce faire, cliquez sur le lien avec le paramètre **Adresse du contrôleur de domaine** pour la connexion requise. Dans la fenêtre qui s'ouvre, modifiez les paramètres requis, puis cliquez sur le bouton **Enregistrer**.

  Vous pouvez uniquement modifier les paramètres **Identifiant** et **Mot de passe** .

- Supprimer des connexions.

  Pour ce faire, cochez la case en regard de la connexion que vous souhaitez supprimer, cliquez sur le bouton **Supprimer** dans la barre d'outils, puis confirmez la suppression de la connexion.

Configuration de l'intégration à Kaspersky Automated Security Awareness Platform

L'intégration à Kaspersky Automated Security Awareness Platform (ci-après également appelé KASAP) vous permet d'assigner des cours de formation KASAP aux utilisateurs associés à des alertes.

Les paramètres d'intégration ne sont pas hérités et s'appliquent uniquement au Serveur d'administration (physique ou virtuel) sur lequel vous configurez ces paramètres.

Avant de configurer une intégration dans Kaspersky Security Center Web Console, vous devez créer un jeton d'autorisation et obtenir une URL pour les requêtes API dans KASAP.

Pour configurer l'intégration à Kaspersky Automated Security Awareness Platform, procédez comme suit :

1. Dans le menu principal, cliquez sur le nom du Serveur d'administration.

   La fenêtre des propriétés du Serveur d'administration s'ouvre avec l'onglet **Général** sélectionné.

2. Sélectionnez la section **KASAP**.

3. Dans le volet droit, activez le commutateur **Intégration KASAP**.

4. Spécifiez les paramètres à utiliser pour la connexion à KASAP :

   - **Jeton d'API** : jeton que vous avez créé pour accéder à KASAP Open API.
   - **URL** : URL pour les requêtes API que vous avez obtenue lors de la création du jeton API.
   - **Utiliser un serveur proxy** : commutateur qui active l'utilisation d'un serveur proxy lors de la connexion à KASAP.

     Le commutateur est désactivé par défaut.

5. Si nécessaire, vérifiez les paramètres que vous avez spécifiés en cliquant sur le bouton **Analyser la connexion**.

   L'état de la connexion s'affiche.

6. Cliquez sur le bouton **Enregistrer**.

L'intégration à Kaspersky Automated Security Awareness Platform est configurée.

Une fois les paramètres d'intégration à KASAP enregistrés, vous pouvez afficher la liste des groupes de formation KASAP en cliquant sur le bouton **Afficher les groupes**.

Si nécessaire, lorsque la liste des groupes s'affiche, vous pouvez la mettre à jour en cliquant sur le bouton **Actualiser les groupes**.

> Vous ne pouvez pas masquer la liste après l'avoir ouverte. Si vous désactivez le commutateur **Intégration KASAP**, la liste des groupes KASAP ne s'affiche pas.

Configuration de l'intégration à Kaspersky Threat Intelligence Portal Sandbox

L'intégration à Kaspersky Threat Intelligence Portal (ci-après également appelé Kaspersky TIP) vous permet d'exécuter les fichiers déplacés vers la section **Quarantaine** en utilisant Kaspersky Sandbox, un environnement sécurisé isolé du réseau de votre entreprise.

Les paramètres d'intégration ne sont pas hérités et s'appliquent uniquement au Serveur d'administration (physique ou virtuel) sur lequel vous configurez ces paramètres.

> Avant de configurer l'intégration, vous devez obtenir un jeton d'autorisation pour les requêtes API sur Kaspersky TIP.

Pour configurer l'intégration à Kaspersky TIP Sandbox, procédez comme suit :

1. Dans le menu principal, cliquez sur le nom du Serveur d'administration.

   La fenêtre des propriétés du Serveur d'administration s'ouvre avec l'onglet **Général** sélectionné.

2. Sélectionnez **Kaspersky TIP**.

3. Dans le volet droit, activez le commutateur **Intégration**.

   Les paramètres de connexion à Kaspersky TIP s'affichent.

Si, après avoir configuré et enregistré les paramètres d'intégration, vous désactivez le commutateur **Intégration**, les paramètres ne sont pas supprimés, mais la réponse ne peut pas être exécutée.

4. Cliquez sur le bouton **Ajouter un jeton** et, dans la fenêtre qui s'affiche, spécifiez le jeton obtenu précédemment auprès de Kaspersky TIP, puis cliquez sur le bouton **Ajouter**.

   La fenêtre se ferme et le jeton API est ajouté.

5. Si vous souhaitez utiliser un serveur proxy lors de la connexion à Kaspersky TIP, activez le commutateur **Utiliser un serveur proxy**.

   Le commutateur est désactivé par défaut.

6. Cliquez sur **Enregistrer**.

L'intégration à Kaspersky TIP Sandbox est configurée.

Vous pouvez désormais envoyer des fichiers depuis la section **Quarantaine** vers Kaspersky TIP Sandbox à des fins d'analyse des menaces. La taille maximale d'un fichier est de 100 Mo.

Étant donné que la licence pour Kaspersky Next XDR Optimum prend en charge la multilocation, les fichiers placés en **Quarantaine** sont répartis entre les locataires. Cette répartition entre les locataires s'applique également lors de l'envoi de fichiers vers Kaspersky TIP Sandbox et de l'affichage des résultats si l'administrateur utilise un compte TIP dédié et un jeton API associé à chaque locataire. Cependant, la gestion centralisée de la section **Quarantaine** pour tous les locataires n'est pas possible, car la liste de quarantaine n'affiche pas les objets selon la hiérarchie des serveurs.

Regroupement des alertes par attributs

L'agrégation des alertes permet d'identifier les alertes qui peuvent être liées au même incident, ce qui simplifie le processus d'enquête.

Pour activer la fonctionnalité d'agrégation des alertes, vous devez procéder comme suit :

- Activez la sous-section **Alerte** dans le menu principal.

- Activez le Serveur d'administration sous une licence pour Kaspersky Next XDR Optimum, puis déployez la clé de licence pour Kaspersky Next XDR Optimum dans les applications que vous administrez.

  Lorsque vous utilisez une fonctionnalité Kaspersky Next XDR Optimum sous licence d'évaluation en mode test, il faut d'abord ajouter un Serveur d'administration physique secondaire, puis activer ce serveur sous cette licence.

Si vous utilisez la licence pour Kaspersky Next EDR Optimum, vous n'avez pas besoin d'activer les applications installées sur vos appareils administrés sous la licence pour Kaspersky Next XDR Optimum. Vous devez le faire uniquement pour les nouveaux appareils, le cas échéant.
Étant donné que la licence Kaspersky Next XDR Optimum prend en charge la multilocation, vous pouvez distribuer de manière centralisée la clé de licence aux applications gérées. La distribution automatique de la licence aux Serveurs d'administration virtuels et secondaires n'est pas prise en charge.

Vous pouvez regrouper les alertes par nom d'appareil, compte ou nom du hachage (SHA256).

Les alertes sont agrégées par un attribut uniquement si cet attribut n'est pas vide.

Les alertes sont agrégées si elles partagent au moins un attribut et si elles se produisent dans les 24 heures suivant toute autre alerte du groupe.

Pour agréger les alertes par attributs, procédez comme suit :

1. Dans le menu principal, accédez à **Surveillance** → **Alerte**.

2. Exécutez une des actions suivantes :

   - Activez le commutateur **Agrégation des alertes**, puis sélectionnez au moins un attribut pour agréger les alertes par :

     - **Nom de l'appareil**

     - **Compte utilisateur**

     - **Hachage du fichier**Nom du hachage (SHA256)

     Les attributs **Nom de l'appareil** et **Compte utilisateur** sont sélectionnés par défaut.

   - Cliquez sur l'icône des Paramètres (⚙). Dans le volet **Paramètres du tableau** qui s'ouvre, accédez à l'onglet **Groupe**. Sélectionnez **Identifiant du groupe d'agrégation** et cliquez sur **Appliquer**.

   Lorsque l'agrégation est activée, les alertes sont triées par **Heure de l'événement**, du plus récent au plus ancien. Les options de tri supplémentaires ne sont pas prises en charge. La sélection d'une autre option de regroupement désactivera l'agrégation.

   Le tableau affiche les alertes agrégées par attributs. Les alertes non regroupées s'affichent en bas du tableau.

Chaque alerte est attribuée à un seul groupe après agrégation.

Intégration entre Kaspersky Security Center Web Console et d'autres solutions Kaspersky

Cette section décrit comment configurer l'accès de Kaspersky Security Center Web Console à une autre application Kaspersky, comme Kaspersky Managed Detection and Response. Cette section décrit également comment configurer l'exportation vers des systèmes SIEM.

Établissement d'une connexion en arrière-plan

Pour configurer l'interaction entre Kaspersky Security Center Linux et une autre application ou solution de Kaspersky, par exemple, Kaspersky Managed Detection and Response (également appelée MDR), vous devez établir une connexion en arrière-plan entre Kaspersky Security Center Web Console et le Serveur d'administration. Vous ne pouvez établir cette connexion que si votre compte dispose du droit Modifier les ACL des objets de la zone fonctionnelle **Fonctions générales : Autorisations utilisateur**.

> Vous pouvez configurer l'interaction uniquement entre Kaspersky Managed Detection and Response et la version Windows de Kaspersky Security Center.

Pour établir une connexion en arrière-plan :

1. Dans le menu principal, accédez à **Paramètres** → **Intégration**.
2. Sélectionnez l'onglet **Paramètres du serveur proxy de Web Console**.
3. Dans la section **Intégration**, réglez le commutateur de connexion en arrière-plan sur **Connexion en arrière-plan pour l'intégration Activé**.
4. Dans la section **Activer une connexion en arrière-plan** ouverte, cliquez sur le bouton **OK**.

La connexion en arrière-plan entre Kaspersky Security Center Web Console et le Serveur d'administration est établie. Le Serveur d'administration crée un compte pour la connexion en arrière-plan, et ce compte est utilisé comme compte de service pour maintenir l'interaction entre Kaspersky Security Center Linux et une autre application ou solution de Kaspersky. Le nom de ce compte de service contient le préfixe NWCSvcUser. Pour des raisons de sécurité, le Serveur d'administration modifie automatiquement le mot de passe du compte de service une fois tous les 30 jours. Vous ne pouvez pas supprimer le compte de service manuellement. Le Serveur d'administration supprime ce compte automatiquement lorsque vous désactivez une connexion interservices. Le Serveur d'administration crée un compte de service unique pour chaque Kaspersky Security Center Web Console et Console d'administration et attribue tous les comptes de service au groupe de sécurité avec le nom ServiceNwcGroup. Le Serveur d'administration crée automatiquement ce groupe de sécurité lors du processus d'installation de Kaspersky Security Center Linux. Vous ne pouvez pas supprimer ce groupe de sécurité manuellement.

Configuration de la connexion au serveur proxy

Pour configurer une connexion au serveur proxy pour Kaspersky Security Center Web Console et les plug-ins Internet, procédez comme suit :

1. Dans le menu principal, accédez à **Paramètres** → **Intégration**.
2. Sélectionnez l'onglet **paramètres du serveur proxy de Web Console**.
3. Activez l'option **Utiliser un serveur proxy**.
4. Spécifiez les paramètres de connexion au serveur proxy :
   - **Adresse du serveur proxy**
   - **Numéro de port**
   - **Authentification du serveur proxy**
   - **Nom d'utilisateur** (requis si vous activez l'option **Authentification du serveur proxy**)
   - **Mot de passe** (requis si vous activez l'option **Authentification du serveur proxy**)
5. Cliquez sur le bouton **Enregistrer** pour enregistrer les paramètres de connexion au serveur proxy

Si vous disposez d'une hiérarchie de Serveurs d'administration, les paramètres de connexion au serveur proxy ne sont pas propagés aux instances Web Console qui gèrent les Serveurs d'administration secondaires. Vous devez configurer la connexion au serveur proxy séparément pour chaque instance de Kaspersky Security Center Web Console.

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 **Gestion des ressources** → **Ressources (Appareils)**.
   - 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 l'onglet **Avancé**, 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 **Gestion 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 **Traçages**, 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 options suivantes sont proposées :

   - **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 **Gestion 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 **Gestion 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 **Traçages**, cliquez sur le bouton **Fichiers de traçage**.

   Cette action permet d'ouvrir la fenêtre **Journaux de traçage des appareils**, où une liste des fichiers de traçage s'affiche.

5. Dans la liste des fichiers de traçage, sélectionnez le fichier que vous souhaitez télécharger.

6. Exécutez une des actions suivantes :

   - Téléchargez le fichier sélectionné en cliquant sur **Télécharger**. Vous pouvez sélectionner un ou plusieurs fichiers à télécharger.

   - Téléchargez une partie du fichier sélectionné :

     a. Cliquez sur **Télécharger une partie**.

     Il est impossible de télécharger des parties de plusieurs fichiers à la fois. Si vous sélectionnez plusieurs fichiers de traçage, le bouton **Télécharger une partie** est désactivé.

     b. Dans la fenêtre qui s'ouvre, indiquez le nom et la partie de fichier à télécharger, en fonction de vos besoins.

     Pour les appareils basés sur Linux, la modification du nom de la partie du fichier n'est pas disponible.

     c. Cliquez sur **Télécharger**.

Le fichier sélectionné, ou une partie de celui-ci, est téléchargé à l'emplacement que vous définissez.

Suppression de fichiers de traçage

Vous pouvez supprimer les fichiers de traçage qui ne sont plus nécessaires.

Pour supprimer un fichier de traçage, procédez comme suit :

1. Ouvrez la fenêtre de diagnostic à distance d'un l'appareil client.

2. Dans la fenêtre de diagnostic à distance qui s'ouvre, sélectionnez l'onglet **Journaux des événements**.

3. Dans la section **Fichiers de traçage**, cliquez sur **Journaux du service Windows Update** ou **Journaux d'installation à distance**, en fonction des fichiers de traçage que vous souhaitez supprimer.

   Le lien **Journaux du service Windows Update** est disponible uniquement pour les appareils clients Windows.

   Cette action permet d'ouvrir la fenêtre **Journaux de traçage des appareils**, où une liste des fichiers de traçage s'affiche.

4. Dans la liste des fichiers de traçage, sélectionnez un ou plusieurs fichiers que vous souhaitez supprimer.

5. Cliquez sur le bouton **Supprimer**.

Les fichiers de traçage sélectionnés sont supprimés.

Téléchargement des paramètres de l'application

Pour télécharger les paramètres des applications à partir d'un appareil client, procédez comme suit :

1. Ouvrez la fenêtre de diagnostic à distance d'un l'appareil client.
2. Dans la fenêtre de diagnostic à distance, sélectionnez l'onglet **Applications Kaspersky**.
3. Dans la section **Paramètres de l'application**, cliquez sur le bouton **Télécharger** pour télécharger les informations relatives aux paramètres des applications installées sur l'appareil client.

L'archive ZIP contenant les informations est téléchargée à l'emplacement indiqué.

Téléchargement des 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 **Gestion 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 **Gestion 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.

Si vous souhaitez exécuter un script personnalisé sur l'appareil client, vous pouvez utiliser la variable d'environnement `KLACDT_SAVE_SETTING` pour déterminer le chemin d'accès où les résultats de l'exécution seront enregistrés. Par exemple :

- Pour un appareil fonctionnant sous Windows :

  ```
  @echo some result > %KLACDT_SAVE_SETTING%\res.log
  ```

- Pour un appareil fonctionnant sous Linux :

  ```
  echo some result > $KLACDT_SAVE_SETTING/res.log
  ```

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 champ **Type de l'objet**, sélectionnez le type d'objet que vous souhaitez télécharger :

   - Sélectionnez **Fichier** pour télécharger le fichier exécutable.

   - Sélectionnez **Dossier** pour télécharger le dossier contenant l'application que vous souhaitez exécuter sur l'appareil client.

     Si vous sélectionnez ce type d'objet, le champ **Nom du fichier exécutable à exécuter** apparaît. Dans ce champ, spécifiez le nom du fichier exécutable dans le dossier. Vous pouvez également spécifier le chemin relatif vers le fichier.

   - Sélectionner **Archives** pour télécharger l'archive ZIP contenant l'application que vous souhaitez exécuter sur l'appareil client.

     Si vous sélectionnez ce type d'objet, le champ **Nom du fichier exécutable à exécuter** apparaît. Dans ce champ, spécifiez le nom du fichier exécutable dans le dossier. Vous pouvez également spécifier le chemin relatif vers le fichier.

     > L'archive ZIP doit inclure le dossier des utilitaires. Ce dossier contient le fichier exécutable qui sera lancé sur un appareil distant.

4. Téléchargez l'objet en le sélectionnant dans la fenêtre système ou en le faisant glisser vers le champ de téléchargement.

5. Si nécessaire, dans le champ **Arguments de la ligne de commande**, spécifiez les arguments de ligne de commande à transmettre lors de l'exécution du fichier exécutable.

6. Cliquez sur le bouton **Charger et exécuter** pour lancer l'application indiquée sur l'appareil client.

7. Une fois l'exécution de l'application terminée avec succès, téléchargez les résultats de l'exécution en cliquant sur le bouton **Télécharger les résultats de l'exécution de l'application**.

   > Les résultats d'exécution de l'application sont stockés jusqu'à ce que vous exécutiez un nouveau diagnostic ou fermiez la fenêtre.

Le diagnostic à distance de l'appareil client à l'aide de l'application est terminé.

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 doit être exécuté sur l'appareil client basé sur Linux à diagnostiquer. Un fichier contenant les informations de diagnostic, les informations sur le système de l'appareil, les fichiers de traçage de l'application, les journaux des événements de l'appareil et un fichier de vidage pour les plantages et les processus terminés est alors créé.

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.

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 **Gestion des ressources** → **Tâches**.

   La liste des tâches s'affiche.

2. Cliquez sur **Ajouter**.

   Ceci permet de lancer l'assistant de création d'une tâche. Suivez les étapes de l'Assistant.

3. Sur la page **Paramètres de nouvelle tâche**, dans la liste déroulante **Application**, sélectionnez Kaspersky Endpoint Security for 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 **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**, procédez comme suit :

   a. Sélectionnez un type de règle pour la création de la catégorie :

   - **De la 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.

   - **Sélectionnez le certificat dans le référentiel**

     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.

     Les certificats sont ajoutés au stockage si vous avez créé et lancé une tâche d'inventaire ou coché la case **À propos des applications lancées** dans la stratégie de Kaspersky Endpoint Security. Vous pouvez effectuer les deux actions.

     Les informations sur les certificats ne peuvent être extraites que des fichiers exécutables au format PE (.exe, .dll, .sys).

   - **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.

    Hachage 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 **SHA256**.
    - 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.

Les certificats sont ajoutés au stockage si vous avez créé et lancé une tâche d'inventaire ou coché la case **À propos des applications lancées** dans la stratégie de Kaspersky Endpoint Security. Vous pouvez effectuer les deux actions.

- **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 :

- **Hachage 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.

Les critères **Données méta** et **Certificat** doivent être spécifiés manuellement après le chargement d'un fichier ou d'un dossier archivé si vous souhaitez utiliser ces critères.

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 :

- **Hachage 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.

Les critères **Données méta** et **Certificat** doivent être spécifiés manuellement après le chargement d'un fichier ou d'un dossier archivé si vous souhaitez utiliser ces critères.

b. Si nécessaire, ajoutez un commentaire dans le champ **Description**. Le nombre de symboles ne peut pas dépasser 1 000.

   Vous pourrez modifier ou supprimer le commentaire ultérieurement. Pour ce faire, dans les propriétés de la catégorie d'application, ouvrez l'onglet **Conditions**, puis, dans la colonne **Critère de la condition**, cliquez sur le lien correspondant à la condition dont vous souhaitez modifier ou supprimer le commentaire.

   Lorsque vous sélectionnez le type de règle **De la catégorie KL**, vous pouvez ajouter un commentaire pour toutes les conditions à créer sur la base de ce type de règle. Vous pouvez modifier ou supprimer le commentaire pour chaque condition séparément.

Le critère sélectionné est ajouté à la liste des conditions.

Vous pouvez ajouter autant de critères que nécessaire pour la catégorie d'application en cours de création.

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.

   Si nécessaire, vous pouvez ajouter un commentaire dans le champ **Description**. Le nombre de symboles ne peut pas dépasser 1 000.

   Vous pourrez modifier ou supprimer le commentaire ultérieurement. Pour ce faire, dans les propriétés de la catégorie d'application, ouvrez l'onglet **Exclusions**, puis, dans la colonne **Critère de la condition**, cliquez sur le lien correspondant à la condition dont vous souhaitez modifier ou supprimer le commentaire.

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.

Une fois l'assistant terminé, la catégorie d'application est créée et 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 **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 **SHA256**.

     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 **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 Linux 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 de script dans une catégorie, Kaspersky Security Center Linux peut perdre en performance.

  Celle-ci est décochée par défaut.

- **Algorithme de calcul de la fonction hash** : **Calculer le hash SHA256 pour les fichiers dans la catégorie (pris en charge par Kaspersky Endpoint Security 10 Service Pack 2 for Windows et versions ultérieures)** / **Calculer le hash MD5 pour les fichiers de la catégorie (pris en charge par les versions antérieures à Kaspersky Endpoint Security 10 Service Pack 2 for Windows)**

  En fonction de la version de l'application de sécurité installée sur les appareils de votre réseau, il faut choisir un algorithme de calcul de la fonction hash par l'application Kaspersky Security Center 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 **SHA256**.

  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.

- **Analyse forcée du dossier à la recherche de la présence 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.

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** → **Sélections d'événements**.

   La liste des sélections d'événements s'affiche.

2. Sélectionnez la sélection d'événements pour consulter les événements associés au Contrôle des applications et démarrer cette sélection d'événements.

   Si vous n'avez pas créé de sélection d'événements associée au Contrôle des applications, vous pouvez sélectionner et démarrer une sélection prédéfinie, par exemple, les **Événements récents**.

   La liste des événements s'affiche.

3. Sélectionnez les événements dont vous souhaitez ajouter les fichiers exécutables associés à la catégorie d'applications, puis cliquez sur le bouton **Affecter à une catégorie**.

   L'Assistant de nouvelle catégorie démarre. Parcourez les étapes de l'assistant à l'aide du bouton **Suivant**.

4. Indiquez les paramètres appropriés sur la page de l'assistant :

   - Dans la section **Action sur le fichier exécutable lié à l'événement**, sélectionnez une des options suivantes :

     - **Ajoute une nouvelle catégorie d'applications**

       Sélectionnez cette option si vous souhaitez créer une nouvelle catégorie d'applications basée sur des fichiers exécutables liés par un événement.

       Cette option est sélectionnée par défaut.

       Si vous avez sélectionné cette option, indiquez un nouveau nom de catégorie.

- **Ajouter à une catégorie d'application existante**

  Sélectionnez cette option s'il est nécessaire d'ajouter des fichiers exécutables liés par un événement à une catégorie d'applications existante.

  Par défaut, cette option n'est pas sélectionnée.

  Si vous avez sélectionné cette option, sélectionnez la catégorie d'applications enrichie manuellement à laquelle vous souhaitez ajouter les fichiers exécutables.

- Dans la section **Type de règle**, sélectionnez une des options suivantes :

  - **Règles pour l'ajout aux inclusions**

  - **Règles pour l'ajout aux exclusions**

- Dans la section **Paramètre utilisé comme condition**, sélectionnez une des options suivantes :

  - **Détails du certificat (ou hash SHA256 pour les fichiers sans certificat)**

    Les fichiers peuvent être signés par un certificat. De plus un certificat peut signer plusieurs fichiers. Par exemple, différentes versions d'une application peuvent être signées par un certificat ou plusieurs applications différentes d'un même éditeur peuvent être signées par un même certificat. En cas de sélection du certificat, la catégorie peut reprendre plusieurs versions de l'application ou plusieurs applications d'un même éditeur.

    Chaque fichier possède sa propre fonction de hachage SHA256 unique. En cas de sélection de la fonction hash SHA256, la catégorie reprend uniquement un seul fichier correspondant, par exemple, la version définie de l'application.

    Sélectionnez cette option si vous souhaitez ajouter les données du certificat du fichier exécutable (ou la fonction hash SHA256 pour les fichiers sans certificat) aux règles de la catégorie.

    Cette option est sélectionnée par défaut.

  - **Détails du certificat (les fichiers sans certificat sont ignorés)**

    Les fichiers peuvent être signés par un certificat. De plus un certificat peut signer plusieurs fichiers. Par exemple, différentes versions d'une application peuvent être signées par un certificat ou plusieurs applications différentes d'un même éditeur peuvent être signées par un même certificat. En cas de sélection du certificat, la catégorie peut reprendre plusieurs versions de l'application ou plusieurs applications d'un même éditeur.

    Sélectionnez cette option si vous souhaitez ajouter les données du certificat du fichier exécutable aux règles de la catégorie. Si le fichier exécutable n'a pas de certificat, ce fichier sera ignoré. Les informations le concernant ne seront pas ajoutées dans la catégorie.

  - **SHA256 uniquement (les fichiers sans hash sont ignorés)**

    Chaque fichier possède sa propre fonction de hachage SHA256 unique. En cas de sélection de la fonction hash SHA256, la catégorie reprend uniquement un seul fichier correspondant, par exemple, la version définie de l'application.

    Sélectionnez cette option si vous souhaitez ajouter uniquement les données de la fonction hash SHA256 du fichier exécutable.

- **MD5 uniquement (mode supprimé, uniquement pour Kaspersky Endpoint Security 10 Service Pack 1)**

  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.

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 **Gestion des ressources** → **Stratégies**.

   Une page comportant une liste des stratégies s'affiche.

2. Cliquez sur la stratégie **Kaspersky Endpoint Security for Windows**.

   La fenêtre des paramètres de la stratégie s'ouvre.

3. Accédez à **Paramètres de l'application** → **Contrôles de sécurité** → **Contrôle des applications**.

   La fenêtre **Contrôle des applications** comportant les paramètres du Contrôle des applications s'affiche.

4. L'option **Contrôle des applications** est activée par défaut. 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.

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 **Gestion des ressources** → **Ressources (Appareils)** → **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.

À propos des applications tierces

Kaspersky Security Center Linux peut vous aider à mettre à jour les logiciels tiers installés sur les appareils clients et à corriger les vulnérabilités du logiciel tiers. Kaspersky Security Center Linux peut mettre à jour les logiciels tiers de la version actuelle à la dernière version uniquement.

La liste des logiciels tiers peut être modifiée et est mise à jour dynamiquement. Vous pouvez vérifier si vous pouvez mettre à jour le logiciel tiers (installé sur les appareils des utilisateurs) avec Kaspersky Security Center Linux en consultant la liste des mises à jour disponibles dans Kaspersky Security Center Web Console.

La procédure décrite ci-dessous permet uniquement de consulter la liste des logiciels tiers qui peuvent être mis à jour à l'aide de Kaspersky Security Center Linux. Les étapes sont suivies pour accéder aux informations pertinentes sans lancer de tâches.

Pour afficher la liste des logiciels tiers que vous pouvez mettre à jour avec Kaspersky Security Center Linux, procédez comme suit :

1. Dans le menu principal, accédez à **Gestion des ressources** → **Tâches**.
2. Cliquez sur **Ajouter**.

   Ceci permet de lancer l'assistant de création d'une tâche. Parcourez les étapes de l'assistant à l'aide du bouton **Suivant**.
3. À l'étape **Paramètres de nouvelle tâche** de l'assistant, spécifiez les paramètres suivants :
   a. Dans la liste déroulante **Application**, sélectionnez **Kaspersky Security Center Linux**.
   b. Dans le champ **Type de tâche**, sélectionnez **Installation des mises à jour requises et correction des vulnérabilités**.
4. A l'étape **Zone d'action d'une tâche** de l'Assistant, sélectionnez l'option **Appareils administrés**.
5. À l'étape **Définissez les règles d'installation des mises à jour** du programme d'installation, cliquez sur le bouton **Ajouter**.

   L'Assistant de création de règles se lance. Parcourez les étapes de l'assistant à l'aide du bouton **Suivant**.
6. À l'étape **Sélectionnez le type de règle** de l'assistant, sélectionnez l'option **Règles pour les mises à jour tierces**.
7. À l'étape **Critères généraux** de l'Assistant, sélectionnez l'option **Installer toutes les mises à jour (sauf les mises à jour rejetées)**, puis cliquez sur **Suivant**.

La liste des logiciels tiers s'affiche.

Installation des mises à jour du logiciel tiers

Kaspersky Security Center Linux vous permet de gérer les mises à jour des logiciels tiers installés sur les appareils administrés et de corriger les vulnérabilités dans ces logiciels en installant les mises à jour requises.

Kaspersky Security Center Linux recherche des mises à jour par la tâche *Recherche de vulnérabilités et de mises à jour requises*. Une fois cette tâche terminée, le Serveur d'administration reçoit la liste des vulnérabilités détectées et des mises à jour requises pour les logiciels tiers installés sur les appareils que vous avez spécifiés dans les propriétés de la tâche. Après la consultation des informations sur les mises à jour disponibles, vous pouvez exécuter l'installation des mises à jour sur vos appareils.

La mise à jour de certaines applications Kaspersky Security Center Linux s'effectue par la suppression de la version précédente de l'application et par l'installation d'une nouvelle version.

Une interaction utilisateur peut être requise lorsque vous mettez à jour une application tierce ou corrigez une vulnérabilité dans une application tierce sur un appareil administré. Par exemple, l'utilisateur peut être invité à fermer l'application tierce si elle est actuellement ouverte.

Pour des raisons de sécurité, toutes les mises à jour du logiciel tiers que vous installez à l'aide de la fonction de la gestion des vulnérabilités et des correctifs sont automatiquement analysées à la recherche d'applications malveillantes par les technologies de Kaspersky. Ces technologies sont utilisées pour la vérification automatique des fichiers et incluent la recherche de virus, l'analyse statique, l'analyse dynamique, l'analyse comportementale dans l'environnement sandbox et machine learning.

Les experts de Kaspersky n'effectuent pas d'analyse manuelle des mises à jour du logiciel tiers pouvant être installées par la fonction de la gestion des vulnérabilités et des correctifs. De plus, les experts de Kaspersky ne recherchent pas de vulnérabilités (connues ou inconnues) ou de fonctionnalités non documentées dans ces mises à jour, et n'effectuent pas d'autres types d'analyse des mises à jour que ceux indiqués dans le paragraphe ci-dessus.

Lorsque les métadonnées des mises à jour du logiciel tiers sont téléchargées dans le stockage, vous pouvez installer les mises à jour sur les appareils clients en utilisant la tâche *Installation des mises à jour requises et correction des vulnérabilités*.

> La tâche *Installation des mises à jour requises et correction des vulnérabilités* ne peut être créée que si vous disposez d'une licence pour la fonctionnalité Gestion des vulnérabilités et des correctifs.

Lorsque cette tâche est terminée, les mises à jour sont installées automatiquement sur les appareils administrés. Lorsque les métadonnées des nouvelles mises à jour sont téléchargées dans le stockage du Serveur d'administration, Kaspersky Security Center Linux vérifie si les mises à jour répondent aux critères spécifiés dans les règles de mise à jour. Toutes les nouvelles mises à jour qui répondent aux critères seront téléchargées et installées automatiquement lors de la prochaine exécution de la tâche.

Scénario : mise à jour des logiciels tiers

Cette section fournit un scénario pour la mise à jour des logiciels tiers installés sur les appareils client. Les logiciels tiers comprennent des applications d'autres fournisseurs de logiciels.

Conditions préalables

Pour pouvoir installer les mises à jour logicielles tierces, le Serveur d'administration doit être connecté à Internet.

Étapes

La mise à jour du logiciel tiers s'effectue fait par étapes :

1. **Recherche des mises à jour requises**

   Pour rechercher les mises à jour des logiciels tiers requises pour les appareils administrés, exécutez la tâche *Recherche de vulnérabilités et de mises à jour requises*. Une fois cette tâche terminée, Kaspersky Security Center Linux reçoit la liste des vulnérabilités détectées et des mises à jour requises pour les logiciels tiers installés sur les appareils que vous avez spécifiés dans les propriétés de la tâche.

   La tâche *Recherche de vulnérabilités et de mises à jour requises* est créée automatiquement par l'Assistant de configuration initiale du Serveur d'administration. Si vous n'avez pas exécuté l'assistant, créez la tâche *Recherche de vulnérabilités et de mises à jour requises* ou exécutez l'Assistant de configuration initiale de l'application maintenant.

   > Vous pouvez créer la tâche *Recherche de vulnérabilités et de mises à jour requises* uniquement pour les appareils Windows. Vous ne pouvez pas créer cette tâche pour les appareils fonctionnant sous d'autres systèmes d'exploitation.

2. **Consultation de la liste des mises à jour trouvées**

   Consultez les informations sur les mises à jour logicielles tierces disponibles et décidez quelles mises à jour vous souhaitez installer. Pour consulter les informations détaillées de chaque mise à jour, cliquez sur le nom de la mise à jour dans la liste. Pour chaque mise à jour de la liste, vous pouvez également consulter les statistiques de l'installation de la mise à jour sur les appareils client.

3. **Configuration de l'installation des mises à jour**

   Une fois que Kaspersky Security Center Linux reçoit la liste des mises à jour logicielles tierces, vous pouvez les installer sur les appareils client en créant la tâche *Installation des mises à jour requises et correction des vulnérabilités*.

   > Vous pouvez créer la tâche *Installation des mises à jour requises et correction des vulnérabilités* uniquement pour les appareils Windows. Vous ne pouvez pas créer cette tâche pour les appareils fonctionnant sous d'autres systèmes d'exploitation.

   La tâche *Installation des mises à jour requises et correction des vulnérabilités* est utilisée pour installer les mises à jour des applications de Microsoft, y compris les mises à jour fournies par le service Windows Update et les mises à jour des logiciels d'autres fournisseurs. Notez que la tâche *Installation des mises à jour requises et correction des vulnérabilités* ne peut être créée que si vous disposez d'une licence pour la fonctionnalité Gestion des vulnérabilités et des correctifs.

   Pour installer certaines mises à jour du logiciel, vous devez accepter le Contrat de licence utilisateur final (CLUF) du logiciel en cours d'installation. Si vous refusez le CLUF, la mise à jour logicielle ne sera pas installée.

   Vous pouvez lancer une tâche d'installation de mise à jour selon la planification. Lorsque vous définissez la planification de la tâche, assurez-vous que la tâche d'installation de la mise à jour est lancée une fois que la tâche *Recherche de vulnérabilités et de mises à jour requises* est terminée.

4. **Planification des tâches**

   Pour vous assurer que la liste des mises à jour est toujours d'actualité, planifiez la tâche *Recherche de vulnérabilités et de mises à jour requises* pour exécuter automatiquement la tâche de temps à autre. Par défaut, la tâche *Recherche de vulnérabilités et de mises à jour requises* est configurée pour démarrer manuellement.

Si vous avez créé la tâche *Installation des mises à jour requises et correction des vulnérabilités*, vous pouvez la planifier pour qu'elle soit exécutée à la même fréquence que la tâche *Recherche de vulnérabilités et de mises à jour requises* ou à une fréquence moindre.

Lors de la planification des tâches, assurez-vous qu'une tâche d'installation de la mise à jour est lancée une fois que la tâche *Recherche de vulnérabilités et de mises à jour requises* est terminée.

5. **Approuver et refuser les mises à jour du logiciel tiers (facultatif)**

   Si vous avez créé la tâche *Installation des mises à jour requises et correction des vulnérabilités*, vous pouvez spécifier des règles pour l'installation des mises à jour dans la fenêtre des propriétés de la tâche.

   Pour chaque règle, vous pouvez définir les mises à jour à installer en fonction de l'état de la mise à jour : *Indéfini*, *Approuvé* ou *Rejeté*. Par exemple, vous pouvez créer une tâche spécifique pour les serveurs et définir une règle pour cette tâche afin de n'autoriser l'installation que les mises à jour qui disposent de l'état *Approuvé*. Ensuite, vous définissez manuellement l'état *Approuvé* pour les mises à jour que vous souhaitez installer. Dans ce cas, les mises à jour qui disposent de l'état *Indéfini* ou *Rejeté* ne seront pas installées sur les serveurs que vous avez spécifiés dans la tâche.

   L'utilisation de l'état *Approuvé* pour gérer l'installation des mises à jour est efficace pour un petit nombre de mises à jour. Pour installer plusieurs mises à jour, utilisez les règles que vous pouvez configurer dans la tâche *Installation des mises à jour requises et correction des vulnérabilités*. Nous vous recommandons de définir l'état *Approuvé* uniquement pour les mises à jour particulières qui ne répondent pas aux critères spécifiés dans les règles. Si vous approuvez manuellement un grand nombre de mises à jour, les performances du Serveur d'administration diminuent, ce qui peut entraîner une surcharge du Serveur d'administration.

   Par défaut, les mises à jour du logiciel téléchargées sont à l'état *Indéfini*. Vous pouvez modifier l'état en *Approuvé* ou *Rejeté* dans la liste **Mises à jour du logiciel** (**Opérations** → **Gestion des correctifs** → **Mises à jour du logiciel**).

   Pour en savoir plus, reportez-vous aux instructions concernant l'approbation et le refus des mises à jour logicielles tierces.

6. **Exécution d'une tâche d'installation des mises à jour**

   Lancez la tâche *Installation des mises à jour requises et correction des vulnérabilités*. Lorsque vous démarrez cette tâche, les mises à jour sont téléchargées et installées sur les appareils administrés. Une fois que la tâche est terminée, assurez-vous qu'elle possède le statut *Terminée avec succès* dans la liste des tâches.

7. **Créer un rapport sur les résultats de l'installation des mises à jour (facultatif)**

   Pour consulter les statistiques détaillées concernant l'installation des mises à jour, créez le Rapport sur les résultats de l'installation des mises à jour du logiciel tiers.

Résultats

Si vous avez créé et configuré la tâche *Installation des mises à jour requises et correction des vulnérabilités*, les mises à jour sont installées automatiquement sur les appareils administrés. Lorsque de nouvelles mises à jour sont téléchargées dans le stockage du Serveur d'administration, Kaspersky Security Center Linux vérifie si elles répondent aux critères spécifiés dans les règles de mise à jour. Toutes les nouvelles mises à jour qui répondent aux critères seront installées automatiquement lors de la prochaine exécution de la tâche.

Options d'installation des mises à jour logicielles tierces

Vous pouvez installer les mises à jour logicielles tierces et les mises à jour à partir de Windows Update sur les appareils administrés grâce à la création et à l'exécution de la tâche *Installation des mises à jour requises et correction des vulnérabilités*. La tâche *Installation des mises à jour requises et correction des vulnérabilités* ne peut être créée que si vous disposez d'une licence pour la fonctionnalité Gestion des vulnérabilités et des correctifs. Cette tâche permet d'installer les mises à jour de logiciels d'autres fournisseurs.

> Une interaction utilisateur peut être requise lorsque vous mettez à jour une application tierce ou corrigez une vulnérabilité dans une application tierce sur un appareil administré. Par exemple, l'utilisateur peut être invité à fermer l'application tierce si elle est actuellement ouverte.

Vous pouvez également créer une tâche pour installer les mises à jour requises comme suit :

- En ouvrant la liste des mises à jour, puis en définissant les mises à jour à installer.

  En conséquence, une nouvelle tâche d'installation des mises à jour sélectionnées est créée. En option, vous pouvez ajouter les mises à jour sélectionnées à une tâche existante.

- En exécutant l'Assistant d'installation de la mise à jour.

  > L'Assistant d'installation de la mise à jour est accessible uniquement en présence d'une licence pour le fonctionnement de Gestion des vulnérabilités et des correctifs.

  L'Assistant simplifie la création et la configuration d'une tâche d'installation de mise à jour et vous permet d'éliminer la création de tâches redondantes contenant les mêmes mises à jour à installer.

Installation de mises à jour du logiciel tiers à l'aide de la liste des mises à jour

Pour installer des mises à jour du logiciel tiers à l'aide de la liste des mises à jour, procédez comme suit :

1. Ouvrez la liste des mises à jour en utilisant l'un des chemins d'accès suivants :

   - **Opérations** → **Gestion des correctifs** → **Mises à jour du logiciel**.
   - **Gestion des ressources** → **Ressources (Appareils)** → <nom de l'appareil> → **Avancé** → **Mises à jour non installées**.
   - **Opérations** → **Applications tierces** → **Registre des applications** → <nom de l'application> → **Mises à jour non installées**.

   Une liste des mises à jour disponibles s'affiche.

2. cochez les cases en regard des mises à jour que vous souhaitez installer.

3. Cliquez sur le bouton **Installer les mises à jour**. Si ce bouton n'est pas visible, cliquez sur les points de suspension, puis sélectionnez l'option **Installer les mises à jour** dans la liste déroulante.

   Pour installer certaines mises à jour logicielles, vous devez accepter le Contrat de licence utilisateur final (CLUF). Si vous refusez le CLUF, la mise à jour logicielle n'est pas installée.

4. Sélectionnez l'une des options ci-dessous :

   - **Nouvelle tâche**

     Ceci permet de lancer l'Assistant de création d'une tâche. Si vous disposez d'une licence pour le fonctionnement de Gestion des vulnérabilités et des correctifs, la tâche *Installation des mises à jour requises et correction des vulnérabilités* est présélectionnée. Suivez les étapes de l'assistant pour terminer la création de la tâche.

   - **Installer la mise à jour (ajouter une règle à la tâche indiquée)**

     Sélectionnez une tâche à laquelle vous souhaitez ajouter les mises à jour sélectionnées. Si vous disposez d'une licence pour le fonctionnement de Gestion des vulnérabilités et des correctifs, sélectionnez une tâche *Installation des mises à jour requises et correction des vulnérabilités*. Une nouvelle règle pour installer les mises à jour sélectionnées est automatiquement ajoutée à la tâche sélectionnée. Les mises à jour sélectionnées sont ajoutées aux propriétés de la tâche.

     La fenêtre de propriétés de la tâche s'affiche. Cliquez sur le bouton **Enregistrer** afin d'enregistrer les modifications.

   Si vous avez choisi de créer une tâche, celle-ci est créée et affichée dans la liste des tâches à l'endroit suivant : **Gestion des ressources** → **Tâches**. Si vous avez choisi d'ajouter les mises à jour à une tâche existante, les mises à jour sont enregistrées dans les propriétés de la tâche.

Pour installer les mises à jour logicielles tierces, vous devez démarrer la tâche *Installation des mises à jour requises et correction des vulnérabilités*. Vous pouvez démarrer cette tâche en cliquant sur le bouton **Démarrer** dans la liste des tâches ou en définissant les paramètres de planification dans les propriétés de la tâche que vous démarrez. Lorsque vous définissez la planification de la tâche, assurez-vous que la tâche d'installation de la mise à jour est lancée une fois que la tâche *Recherche de vulnérabilités et de mises à jour requises* est terminée.

Installation de mises à jour logicielles tierces à l'aide de l'Assistant d'installation de la mise à jour

L'Assistant d'installation de la mise à jour est accessible uniquement en présence d'une licence pour le fonctionnement de Gestion des vulnérabilités et des correctifs.

Pour créer une tâche d'installation des mises à jour logicielles tierces à l'aide de l'Assistant d'installation de la mise à jour, procédez comme suit :

1. Dans le menu principal, accédez à **Opérations** → **Gestion des correctifs** → **Mises à jour du logiciel**.

   Une liste des mises à jour disponibles s'affiche.

2. Cochez la case en regard de la mise à jour que vous souhaitez installer.

3. Cliquez sur le bouton **Lancer l'Assistant d'installation des mises à jour**.

L'Assistant d'installation de la mise à jour démarre. La page **Sélection de la tâche d'installation de la mise à jour** affiche la liste de toutes les tâches existantes des types suivants :

- *Installation des mises à jour requises et correction des vulnérabilités*
- *Corriger les vulnérabilités*

4. Si vous souhaitez que l'Assistant affiche uniquement les tâches qui installent la mise à jour que vous avez sélectionnée, activez l'option **Afficher uniquement les tâches d'installation de mise à jour**.

5. Choisissez la manière dont vous voulez procéder :

   - Pour lancer une tâche existante, cochez la case en regard de la tâche *Installation des mises à jour requises et correction des vulnérabilités*, puis cliquez sur le bouton **Démarrer**.

     La tâche se poursuivra en mode arrière-plan. Il n'y a rien d'autre à faire.

   - Pour ajouter une nouvelle règle à une tâche existante :

     a. Cochez la case en regard du nom de la tâche, puis cliquez sur le bouton **Ajouter une règle**.

     > Le bouton **Ajouter une règle** est désactivé si vous sélectionnez plusieurs tâches.

     Vous ne pouvez pas ajouter de règle pour une tâche *Corriger les vulnérabilités*. Si vous sélectionnez une tâche *Corriger les vulnérabilités*, la notification suivante s'affiche : " *Pour installer des mises à jour, utilisez la tâche Installation des mises à jour requises et correction des vulnérabilités.* "

     b. À l'étape **Création d'une règle d'installation de la mise à jour** de l'assistant, configurez la nouvelle règle :

     - **Règle d'installation pour les mises à jour de ce niveau d'importance**

       > Parfois, les mises à jour du logiciel peuvent nuire à l'expérience de l'utilisateur. Dans ce cas, il se peut que vous décidiez d'installer uniquement les mises à jour critiques au fonctionnement du logiciel et d'ignorer les autres.
       >
       > Quand cette option est activée, les mises à jour corrigent uniquement les vulnérabilités dont le niveau de gravité, tel que défini par Kaspersky, est égal ou supérieur au niveau de la mise à jour sélectionnée (**Moyenne**, **Élevé** ou **Critique**). Les vulnérabilités dont le niveau de gravité est inférieur à la valeur sélectionnée ne sont pas corrigées.
       >
       > Si cette option est désactivée, les mises à jour corrigent toutes les vulnérabilités, quel que soit le niveau de gravité.
       >
       > Cette option est Inactif par défaut.

       Cette règle ne s'affiche pas si le niveau d'importance de la mise à jour sélectionnée est *Inconnu*.

     - **Règle d'installation pour les mises à jour de ce niveau d'importance selon MSRC**

       > Parfois, les mises à jour logicielles peuvent nuire à l'expérience de l'utilisateur. Dans ce cas, il se peut que vous décidiez d'installer uniquement les mises à jour critiques au fonctionnement du logiciel et d'ignorer les autres.

Quand cette option est activée (disponible uniquement pour les mises à jour Windows), les mises à jour corrigent uniquement les vulnérabilités dont le niveau de gravité tel que défini par Microsoft Security Response Center (MSRC) est égal ou supérieur à la valeur sélectionnée dans la liste (**Bas**, **Moyen**, **Élevé** ou **Critique**). Les vulnérabilités dont le niveau de gravité est inférieur à la valeur sélectionnée ne sont pas corrigées.

Si cette option est désactivée, les mises à jour corrigent toutes les vulnérabilités, quel que soit le niveau de gravité.

Cette option est Inactif par défaut.

Cette règle s'affiche uniquement pour les mises à jour logicielles Microsoft. Elle ne s'affiche pas si le niveau d'importance de la mise à jour sélectionnée est *Inconnu*.

- **Règle d'installation des mises à jour de cet éditeur**

  Cette option est disponible uniquement pour les mises à jour d'applications tierces. Kaspersky Security Center Linux installe uniquement les mises à jour relatives aux applications créées par le même fournisseur que la mise à jour sélectionnée. Les mises à jour et les mises à jour refusées pour des applications créées par d'autres fournisseurs ne sont pas installées.

  Cette option est Inactif par défaut.

  Cette règle s'affiche uniquement pour les mises à jour logicielles tierces.

- **Règle d'installation des mises à jour de type**

- **Règle d'installation des mises à jour de l'application sélectionnée**

  Cette règle s'affiche uniquement pour les mises à jour logicielles tierces.

- **Règle d'installation pour la mise à jour sélectionnée**

- **Approuver les mises à jour sélectionnées**

  La mise à jour sélectionnée est approuvée pour l'installation. Activez cette option si certaines règles appliquées de l'installation de la mise à jour autorisent l'installation des mises à jour confirmées uniquement.

  Cette option est Inactif par défaut.

- **Installer automatiquement toutes les mises à jour précédentes des applications nécessaires à l'installation des mises à jour sélectionnées**

  Conservez cette option si vous acceptez l'installation de versions de l'application intermédiaires quand l'impose l'installation des mises à jour sélectionnées.

  Si vous désactivez cette option, seules les versions sélectionnées des applications sont installées. Désactivez cette option si vous souhaitez mettre à jour les applications d'une manière directe, sans tenter d'installer les versions successives. S'il est impossible d'installer les mises à jour sélectionnées sans installer les versions antérieures de l'application, la mise à jour de l'application échoue.

  Admettons que la version 3 d'une application est installée sur un appareil et vous souhaitez réaliser la mise à jour jusque la version 5, mais la version 5 de cette application peut être installée uniquement sur la version 4. Quand cette option est installée, le logiciel installe d'abord la version 4, puis la version 5. Si l'option est désactivée, le logiciel ne parvient pas à mettre l'application à jour.

Cette option est activée par défaut.

c. Cliquez sur **Ajouter**.

La fenêtre de propriétés de la tâche s'affiche. La nouvelle règle est déjà ajoutée aux propriétés de la tâche. Vous pouvez afficher ou modifier la règle ou d'autres paramètres de tâche. Cliquez sur le bouton **Enregistrer** afin d'enregistrer les modifications.

- Pour créer une tâche, procédez comme suit :

  a. Cliquez sur le bouton **Nouvelle tâche**.

  b. À l'étape **Création d'une règle d'installation de la mise à jour** de l'assistant, configurez la nouvelle règle :

  - **Règle d'installation pour les mises à jour de ce niveau d'importance**

    Parfois, les mises à jour du logiciel peuvent nuire à l'expérience de l'utilisateur. Dans ce cas, il se peut que vous décidiez d'installer uniquement les mises à jour critiques au fonctionnement du logiciel et d'ignorer les autres.

    Quand cette option est activée, les mises à jour corrigent uniquement les vulnérabilités dont le niveau de gravité, tel que défini par Kaspersky, est égal ou supérieur au niveau de la mise à jour sélectionnée (**Moyenne**, **Élevé** ou **Critique**). Les vulnérabilités dont le niveau de gravité est inférieur à la valeur sélectionnée ne sont pas corrigées.

    Si cette option est désactivée, les mises à jour corrigent toutes les vulnérabilités, quel que soit le niveau de gravité.

    Cette option est Inactif par défaut.

    Cette règle ne s'affiche pas si le niveau d'importance de la mise à jour sélectionnée est *Inconnu*.

  - **Règle d'installation pour les mises à jour de ce niveau d'importance selon MSRC**

    Parfois, les mises à jour logicielles peuvent nuire à l'expérience de l'utilisateur. Dans ce cas, il se peut que vous décidiez d'installer uniquement les mises à jour critiques au fonctionnement du logiciel et d'ignorer les autres.

    Quand cette option est activée (disponible uniquement pour les mises à jour Windows), les mises à jour corrigent uniquement les vulnérabilités dont le niveau de gravité tel que défini par Microsoft Security Response Center (MSRC) est égal ou supérieur à la valeur sélectionnée dans la liste (**Bas**, **Moyen**, **Élevé** ou **Critique**). Les vulnérabilités dont le niveau de gravité est inférieur à la valeur sélectionnée ne sont pas corrigées.

    Si cette option est désactivée, les mises à jour corrigent toutes les vulnérabilités, quel que soit le niveau de gravité.

    Cette option est Inactif par défaut.

    Cette règle s'affiche uniquement pour les mises à jour logicielles Microsoft. Elle ne s'affiche pas si le niveau d'importance de la mise à jour sélectionnée est *Inconnu*.

  - **Règle d'installation des mises à jour de cet éditeur**

    Cette option est disponible uniquement pour les mises à jour d'applications tierces. Kaspersky Security Center Linux installe uniquement les mises à jour relatives aux applications créées par le même fournisseur que la mise à jour sélectionnée. Les mises à jour et les mises à jour refusées pour des applications créées par d'autres fournisseurs ne sont pas installées.

Cette option est Inactif par défaut.

Cette règle s'affiche uniquement pour les mises à jour logicielles tierces.

- **Règle d'installation des mises à jour de type**
- **Règle d'installation des mises à jour de l'application sélectionnée**

  Cette règle s'affiche uniquement pour les mises à jour logicielles tierces.
- **Règle d'installation pour la mise à jour sélectionnée**
- **Approuver les mises à jour sélectionnées**

  La mise à jour sélectionnée est approuvée pour l'installation. Activez cette option si certaines règles appliquées de l'installation de la mise à jour autorisent l'installation des mises à jour confirmées uniquement.

  Cette option est Inactif par défaut.
- **Installer automatiquement toutes les mises à jour précédentes des applications nécessaires à l'installation des mises à jour sélectionnées**

  Conservez cette option si vous acceptez l'installation de versions de l'application intermédiaires quand l'impose l'installation des mises à jour sélectionnées.

  Si vous désactivez cette option, seules les versions sélectionnées des applications sont installées. Désactivez cette option si vous souhaitez mettre à jour les applications d'une manière directe, sans tenter d'installer les versions successives. S'il est impossible d'installer les mises à jour sélectionnées sans installer les versions antérieures de l'application, la mise à jour de l'application échoue.

  Admettons que la version 3 d'une application est installée sur un appareil et vous souhaitez réaliser la mise à jour jusque la version 5, mais la version 5 de cette application peut être installée uniquement sur la version 4. Quand cette option est installée, le logiciel installe d'abord la version 4, puis la version 5. Si l'option est désactivée, le logiciel ne parvient pas à mettre l'application à jour.

  Cette option est activée par défaut.

c. Cliquez sur **Ajouter**.

Continuez la création de la tâche dans l'Assistant de création d'une tâche. La nouvelle règle que vous avez ajoutée dans l'Assistant d'installation de la mise à jour s'affiche dans l'Assistant de création d'une tâche. Lorsque vous terminez l'Assistant, la tâche *Installation des mises à jour requises et correction des vulnérabilités* est ajoutée à la liste des tâches.

La tâche Recherche de vulnérabilités et de mises à jour requises est créée

La tâche *Recherche de vulnérabilités et de mises à jour requises* est créée automatiquement lorsque l'assistant de démarrage rapide de l'application est en cours d'exécution. Si vous n'aviez pas exécuté l'assistant, vous pouvez créer la tâche manuellement.

En plus des paramètres de la tâche générale, vous pouvez indiquer les paramètres suivants lors de la création de la tâche *Recherche de vulnérabilités et de mises à jour requises*, ou plus tard, lorsque vous configurez les propriétés de la tâche créée :

- **Rechercher les vulnérabilités et les mises à jour indiquées par Microsoft**

  Lors de la recherche de vulnérabilités et de mises à jour, Kaspersky Security Center Linux utilise les informations sur les mises à jour Microsoft applicables à partir de la source des mises à jour Microsoft disponibles à ce moment-là.

  Par exemple, pensez à désactiver cette option si vous avez différentes tâches avec différents paramètres pour les mises à jour Microsoft et les mises à jour d'applications tierces.

  Cette option est activée par défaut.

  Les informations sur les mises à jour facultatives de Microsoft Windows Update ne sont pas envoyées au Serveur d'administration.

- **Se connecter au serveur de mise à jour pour mettre à jour les données**

  L'Agent de mises à jour Windows sur un appareil administré se connecte à la source des mises à jour Microsoft. Les serveurs suivants peuvent servir de source de mises à jour Microsoft :

  - Serveur Windows sur lequel Microsoft Windows Server Update Services (WSUS) est déployé dans le réseau de votre organisation
  - Serveurs de mises à jour Microsoft

  Si cette option est activée, l'Agent de mises à jour Windows sur un appareil administré se connecte à la source de mise à jour Microsoft pour actualiser les informations relatives aux mises à jour Microsoft Windows applicables.

  Si cette option est désactivée, l'Agent de mises à jour Windows sur un appareil administré utilise les informations relatives aux mises à jour Microsoft Windows obtenues antérieurement auprès de la source des mises à jour Microsoft.

  La connexion à la source des mises à jour Microsoft peut requérir beaucoup de ressources. Pensez à désactiver cette option si vous définissez une connexion régulière à cette source de mises à jour dans une autre tâche ou dans les propriétés de la stratégie de l'Agent d'administration, dans la section **Mises à jour et vulnérabilités du logiciel**. Si vous ne souhaitez pas désactiver cette option, pour réduire la surcharge, vous pouvez configurer la planification des tâches pour randomiser le délai de démarrage des tâches dans les 360 minutes.

  Cette option est activée par défaut.

La combinaison des options suivantes des paramètres de la stratégie de l'Agent d'administration définit le mode d'obtention des mises à jour :

- L'Agent de mises à jour Windows sur un appareil administré se connecte au serveur de mises à jour pour recevoir les mises à jour uniquement si le paramètre **Se connecter au serveur de mise à jour pour mettre à jour les données** est activé dans les propriétés de la tâche *Recherche de vulnérabilités et de mises à jour requises* et si le **Mode de recherche des mises à jour Windows Update** est défini sur **Actif** dans les paramètres de la stratégie de l'Agent d'administration.

- Si vous n'avez pas besoin de l'Agent d'administration pour établir une connexion à la source des mises à jour Microsoft Windows et télécharger les mises à jour lors de l'exécution de la tâche *Recherche de vulnérabilités*, vous pouvez définir l'option **Mode de recherche des mises à jour Windows Update** sur **Passif**, tandis que l'option **Se connecter au serveur de mise à jour pour mettre à jour les données** doit rester activée. Cela vous permet d'économiser des ressources et d'utiliser les mises à jour de Windows déjà reçues pour vérifier la présence de vulnérabilités. Vous pouvez utiliser le mode passif si vous configurez la réception des mises à jour Microsoft Windows différemment. Si la réception des mises à jour Microsoft Windows n'est pas configurée d'une autre manière, ne définissez pas l'option du **Mode de recherche des mises à jour Windows Update** sur **Passif**, car dans ce cas, les informations sur les mises à jour ne seront jamais reçues.

- Quel que soit l'état de l'option **Se connecter au serveur de mise à jour pour mettre à jour les données** (activé ou désactivé), si l'option **Mode de recherche des mises à jour Windows Update** est définie sur **Désactivé**, Kaspersky Security Center Linux ne demande aucune information sur les mises à jour.

Si le serveur WSUS est utilisé dans le réseau de votre organisation (serveur WSUS local) et que vous souhaitez l'utiliser avec le Serveur d'administration de Kaspersky Security Center, vous devez d'abord vous assurer que le Serveur d'administration de Kaspersky Security Center n'est pas utilisé comme serveur WSUS, puis procéder comme suit :

1. Sur vos appareils administrés sous Windows, spécifiez votre serveur WSUS local pour le service de mises à jour Windows. Vous pouvez le faire manuellement dans le registre Windows ou à l'aide d'une stratégie de groupe Windows.

2. Sur votre serveur WSUS local, spécifiez les classifications requises pour les mises à jour et les applications sur lesquelles la distribution des mises à jour doit avoir lieu.

3. Synchronisez votre serveur WSUS avec le serveur en amont (cela peut être un serveur Microsoft WSUS ou un autre serveur WSUS local en amont).

Après l'exécution de la tâche *Recherche de vulnérabilités et de mises à jour requises* sur l'appareil, l'Agent d'administration utilise le service Windows Update pour lancer une demande de mises à jour Windows applicables à l'appareil. Le service Windows Update obtient l'adresse du serveur WSUS externe à partir du registre et recherche les mises à jour directement à partir de ce serveur WSUS externe. Ensuite, le service Windows Update transmet cette liste au Serveur d'administration via l'Agent d'administration. Ainsi, le Serveur d'administration dispose d'une base à jour.

- **Rechercher les vulnérabilités et les mises à jour de tiers indiquées par Kaspersky**

Si cette option est activée, Kaspersky Security Center Linux recherche des vulnérabilités et les mises à jour requises des produits tiers (applications développées par des éditeurs d'application autres que Kaspersky et Microsoft) dans le Registre Windows et dans les dossiers définis sous **Indiquez les chemins pour la recherche avancée des applications dans le système de fichiers**. La liste complète des produits tiers pris en charge est administrée par Kaspersky.

Si cette option est désactivée, Kaspersky Security Center Linux ne recherche pas les vulnérabilités et les mises à jour requises pour les applications tierces. Par exemple, pensez à désactiver cette option si vous avez différentes tâches avec différents paramètres pour les mises à jour Microsoft Windows et les mises à jour d'applications tierces.

Cette option est activée par défaut.

- **Indiquez les chemins d'accès pour la recherche avancée des applications dans le système de fichiers**

Les dossiers dans lesquels Kaspersky Security Center Linux recherche des produits tiers qui requièrent une correction de la vulnérabilité et l'installation d'une mise à jour. Vous pouvez utiliser des variables système.

Indiquez les dossiers dans lesquels les applications doivent être installées. Par défaut, la liste contient les dossiers système dans lesquels la majorité des applications sont installées.

- **Activer le diagnostic avancé**

Quand cette fonction est activée, l'Agent d'administration enregistre des fichiers de trace même si l'écriture de fichiers de trace est désactivée pour l'Agent d'administration dans l'utilitaire de diagnostic à distance Kaspersky Security Center Linux. Les traces sont enregistrées dans deux fichiers en alternance la taille de chacun de ces fichiers est déterminée par la valeur paramètre **Taille maximale (Mo) des fichiers de diagnostic avancé**. Quand les deux fichiers sont remplis, l'Agent d'administration écrit à nouveau dans ceux-ci. Les fichiers avec les traces sont stockés dans le dossier %WINDIR%\Temp. Ces fichiers sont accessibles dans l'utilitaire de diagnostic à distance, vous pouvez les télécharger ou les supprimer à cet endroit.

Quand cette fonction est désactivée, l'Agent d'administration enregistre les traces conformément aux paramètres définis dans l'utilitaire de diagnostic à distance Kaspersky Security Center Linux. Aucune trace complémentaire n'est écrite.

Lors de la création d'une tâche, il n'est pas nécessaire d'activer le diagnostic avancé. Par contre, vous pouvez activer cette fonction plus tard si, par exemple, une tâche échoue sur certains appareils et que vous souhaitez obtenir des informations complémentaires lors d'une autre exécution de la tâche.

Cette option est Inactif par défaut.

- **Taille maximale (Mo) des fichiers de diagnostic avancé**

La valeur par défaut est de 100 Mo, mais elle peut se situer entre 1 et 2 048 Mo. Il peut arriver qu'un expert du Support Technique de Kaspersky vous demande de modifier la valeur par défaut lorsque les informations reprises dans les fichiers de diagnostic avancés que vous avez envoyés ne suffisent pas pour résoudre le problème.

Recommandations sur la planification des tâches

Lors de la planification de la tâche *Recherche de vulnérabilités et de mises à jour requises*, assurez-vous que les deux options **Lancer les tâches non exécutées** et **Adopter un décalage aléatoire automatique pour les lancements de tâche** sont activées.

Par défaut, la tâche *Recherche de vulnérabilités et de mises à jour requises* est configurée pour démarrer manuellement. Si le règlement de travail de la société prévoit l'arrêt de tous les appareils à ce moment, la tâche *Recherche de vulnérabilités et de mises à jour requises* sera lancée après leur remise sous tension, c'est-à-dire le lendemain 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.

Création de la tâche Recherche de vulnérabilités et des mises à jour requises

Grâce à la tâche *Recherche de vulnérabilités et de mises à jour requises*, Kaspersky Security Center Linux reçoit la liste des vulnérabilités détectées et des mises à jour requises pour les logiciels tiers installés sur les appareils administrés.

> Vous pouvez créer la tâche *Recherche de vulnérabilités et de mises à jour requises* uniquement pour les appareils Windows. Vous ne pouvez pas créer cette tâche pour les appareils fonctionnant sous d'autres systèmes d'exploitation.

La tâche *Recherche de vulnérabilités et de mises à jour requises* est créée automatiquement lorsque l'Assistant de configuration initiale de l'application est en cours d'exécution. Si vous n'aviez pas exécuté l'assistant, vous pouvez créer la tâche manuellement.

Pour créer la tâche Recherche de vulnérabilités et de mises à jour requises, procédez comme suit :

1. Dans le menu principal, accédez à **Gestion des ressources** → **Tâches**.
2. Cliquez sur **Ajouter**.

   Ceci permet de lancer l'Assistant de création d'une tâche. Parcourez les étapes de l'assistant à l'aide du bouton **Suivant**.
3. Pour l'application Kaspersky Security Center, sélectionnez le type de tâche **Recherche de vulnérabilités et de mises à jour requises**.
4. Spécifiez le nom de la tâche créée. Le nom de la tâche ne peut pas contenir plus de 100 symboles et contenir de symboles spéciaux ("*<>?\:|).
5. Sélectionnez les appareils auxquels les tâches seront affectées.
6. Indiquez les modes d'analyse des vulnérabilités et des applications nécessitant des mises à jour :

   - **Rechercher les vulnérabilités et les mises à jour indiquées par Microsoft**

     > Lors de la recherche de vulnérabilités et de mises à jour, Kaspersky Security Center Linux utilise les informations sur les mises à jour Microsoft applicables à partir de la source des mises à jour Microsoft disponibles à ce moment-là.
     >
     > Par exemple, pensez à désactiver cette option si vous avez différentes tâches avec différents paramètres pour les mises à jour Microsoft et les mises à jour d'applications tierces.
     >
     > Cette option est activée par défaut.

Les informations sur les mises à jour facultatives de Microsoft Windows Update ne sont pas envoyées au Serveur d'administration.

- **Se connecter au serveur de mise à jour pour mettre à jour les données**

  L'Agent de mises à jour Windows sur un appareil administré se connecte à la source des mises à jour Microsoft. Les serveurs suivants peuvent servir de source de mises à jour Microsoft :

  - Serveur Windows sur lequel Microsoft Windows Server Update Services (WSUS) est déployé dans le réseau de votre organisation
  - Serveurs de mises à jour Microsoft

  Si cette option est activée, l'Agent de mises à jour Windows sur un appareil administré se connecte à la source de mise à jour Microsoft pour actualiser les informations relatives aux mises à jour Microsoft Windows applicables.

  Si cette option est désactivée, l'Agent de mises à jour Windows sur un appareil administré utilise les informations relatives aux mises à jour Microsoft Windows obtenues antérieurement auprès de la source des mises à jour Microsoft.

  La connexion à la source des mises à jour Microsoft peut requérir beaucoup de ressources. Pensez à désactiver cette option si vous définissez une connexion régulière à cette source de mises à jour dans une autre tâche ou dans les propriétés de la stratégie de l'Agent d'administration, dans la section **Mises à jour et vulnérabilités du logiciel**. Si vous ne souhaitez pas désactiver cette option, pour réduire la surcharge, vous pouvez configurer la planification des tâches pour randomiser le délai de démarrage des tâches dans les 360 minutes.

  Cette option est activée par défaut.

  La combinaison des options suivantes des paramètres de la stratégie de l'Agent d'administration définit le mode d'obtention des mises à jour :

  - L'Agent de mises à jour Windows sur un appareil administré se connecte au serveur de mises à jour pour recevoir les mises à jour uniquement si le paramètre **Se connecter au serveur de mise à jour pour mettre à jour les données** est activé dans les propriétés de la tâche *Recherche de vulnérabilités et de mises à jour requises* et si le **Mode de recherche des mises à jour Windows Update** est défini sur **Actif** dans les paramètres de la stratégie de l'Agent d'administration.
  - Si vous n'avez pas besoin de l'Agent d'administration pour établir une connexion à la source des mises à jour Microsoft Windows et télécharger les mises à jour lors de l'exécution de la tâche *Recherche de vulnérabilités*, vous pouvez définir l'option **Mode de recherche des mises à jour Windows Update** sur **Passif**, tandis que l'option **Se connecter au serveur de mise à jour pour mettre à jour les données** doit rester activée. Cela vous permet d'économiser des ressources et d'utiliser les mises à jour de Windows déjà reçues pour vérifier la présence de vulnérabilités. Vous pouvez utiliser le mode passif si vous configurez la réception des mises à jour Microsoft Windows différemment. Si la réception des mises à jour Microsoft Windows n'est pas configurée d'une autre manière, ne définissez pas l'option du **Mode de recherche des mises à jour Windows Update** sur **Passif**, car dans ce cas, les informations sur les mises à jour ne seront jamais reçues.
  - Quel que soit l'état de l'option **Se connecter au serveur de mise à jour pour mettre à jour les données** (activé ou désactivé), si l'option **Mode de recherche des mises à jour Windows Update** est définie sur **Désactivé**, Kaspersky Security Center Linux ne demande aucune information sur les mises à jour.

Si le serveur WSUS est utilisé dans le réseau de votre organisation (serveur WSUS local) et que vous souhaitez l'utiliser avec le Serveur d'administration de Kaspersky Security Center, vous devez d'abord vous assurer que le Serveur d'administration de Kaspersky Security Center n'est pas utilisé comme serveur WSUS, puis procéder comme suit :

1. Sur vos appareils administrés sous Windows, spécifiez votre serveur WSUS local pour le service de mises à jour Windows. Vous pouvez le faire manuellement dans le registre Windows ou à l'aide d'une stratégie de groupe Windows.

2. Sur votre serveur WSUS local, spécifiez les classifications requises pour les mises à jour et les applications sur lesquelles la distribution des mises à jour doit avoir lieu.

3. Synchronisez votre serveur WSUS avec le serveur en amont (cela peut être un serveur Microsoft WSUS ou un autre serveur WSUS local en amont).

Après l'exécution de la tâche *Recherche de vulnérabilités et de mises à jour requises* sur l'appareil, l'Agent d'administration utilise le service Windows Update pour lancer une demande de mises à jour Windows applicables à l'appareil. Le service Windows Update obtient l'adresse du serveur WSUS externe à partir du registre et recherche les mises à jour directement à partir de ce serveur WSUS externe. Ensuite, le service Windows Update transmet cette liste au Serveur d'administration via l'Agent d'administration. Ainsi, le Serveur d'administration dispose d'une base à jour.

- **Rechercher les vulnérabilités et les mises à jour de tiers indiquées par Kaspersky**

  Si cette option est activée, Kaspersky Security Center Linux recherche des vulnérabilités et les mises à jour requises des produits tiers (applications développées par des éditeurs d'application autres que Kaspersky et Microsoft) dans le Registre Windows et dans les dossiers définis sous **Indiquez les chemins pour la recherche avancée des applications dans le système de fichiers**. La liste complète des produits tiers pris en charge est administrée par Kaspersky.

  Si cette option est désactivée, Kaspersky Security Center Linux ne recherche pas les vulnérabilités et les mises à jour requises pour les applications tierces. Par exemple, pensez à désactiver cette option si vous avez différentes tâches avec différents paramètres pour les mises à jour Microsoft Windows et les mises à jour d'applications tierces.

  Cette option est activée par défaut.

Vous pouvez désactiver ces options après la création d'une tâche dans l'onglet **Paramètres de l'application** de la fenêtre des propriétés de la tâche.

7. **Indiquez les chemins d'accès pour la recherche avancée des applications dans le système de fichiers**

   Les dossiers dans lesquels Kaspersky Security Center Linux recherche des produits tiers qui requièrent une correction de la vulnérabilité et l'installation d'une mise à jour. Vous pouvez utiliser des variables système.

   Indiquez les dossiers dans lesquels les applications doivent être installées. Par défaut, la liste contient les dossiers système dans lesquels la majorité des applications sont installées.

Vous pouvez modifier les chemins d'accès spécifiés après la création de la tâche dans l'onglet **Paramètres de l'application** de la fenêtre des propriétés de la tâche.

8. Si nécessaire, **Activer le diagnostic avancé**.

> Quand cette fonction est activée, l'Agent d'administration enregistre des fichiers de trace même si l'écriture de fichiers de trace est désactivée pour l'Agent d'administration dans l'utilitaire de diagnostic à distance Kaspersky Security Center Linux. Les traces sont enregistrées dans deux fichiers en alternance la taille de chacun de ces fichiers est déterminée par la valeur paramètre **Taille maximale (Mo) des fichiers de diagnostic avancé**. Quand les deux fichiers sont remplis, l'Agent d'administration écrit à nouveau dans ceux-ci. Les fichiers avec les traces sont stockés dans le dossier %WINDIR%\Temp. Ces fichiers sont accessibles dans l'utilitaire de diagnostic à distance, vous pouvez les télécharger ou les supprimer à cet endroit.
>
> Quand cette fonction est désactivée, l'Agent d'administration enregistre les traces conformément aux paramètres définis dans l'utilitaire de diagnostic à distance Kaspersky Security Center Linux. Aucune trace complémentaire n'est écrite.
>
> Lors de la création d'une tâche, il n'est pas nécessaire d'activer le diagnostic avancé. Par contre, vous pouvez activer cette fonction plus tard si, par exemple, une tâche échoue sur certains appareils et que vous souhaitez obtenir des informations complémentaires lors d'une autre exécution de la tâche.
>
> Cette option est Inactif par défaut.

Vous pouvez désactiver cette option après la création d'une tâche dans l'onglet **Paramètres de l'application** de la fenêtre des propriétés de la tâche.

9. Précisez la **Taille maximale (Mo) des fichiers de diagnostic avancé**

> La valeur par défaut est de 100 Mo, mais elle peut se situer entre 1 et 2 048 Mo. Il peut arriver qu'un expert du Support Technique de Kaspersky vous demande de modifier la valeur par défaut lorsque les informations reprises dans les fichiers de diagnostic avancés que vous avez envoyés ne suffisent pas pour résoudre le problème.

Vous devez spécifier cette valeur si vous avez activé les diagnostics avancés à l'étape précédente. Vous pouvez modifier cette valeur après la création d'une tâche dans l'onglet **Paramètres de l'application** de la fenêtre des propriétés de la tâche.

10. Si vous souhaitez modifier les paramètres de la tâche par défaut, activez l'option **Ouvrir les détails de la tâche à la fin de la création** sur la page **Fin de la création de la tâche**. Si vous n'activez pas cette tâche, la tâche est créée selon les paramètres par défaut. Vous pourrez modifier ces paramètres par défaut plus tard, à tout moment.

11. Cliquez sur le bouton **Terminer**.

    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. Pour exécuter la tâche, sélectionnez-la dans la liste des tâches, puis cliquez sur le bouton **Démarrer**.

Recommandations sur la planification des tâches

Lors de la planification de la tâche *Recherche de vulnérabilités et de mises à jour requises*, assurez-vous que les deux options **Lancer les tâches non exécutées** et **Adopter un décalage aléatoire automatique pour les lancements de tâche** sont activées.

Par défaut, la tâche *Recherche de vulnérabilités et de mises à jour requises* est configurée pour démarrer manuellement.

Vous pouvez également planifier le démarrage de la tâche *Recherche de vulnérabilités et de mises à jour requises* à une heure précise. Par exemple, vous pouvez sélectionner le démarrage planifié **Toutes les N heures** dans la liste déroulante **Démarrer la tâche** de l'onglet **Programmation** de la fenêtre de propriétés de la tâche. Dans ce cas, notez que 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 le redémarrage des appareils. 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.

Pour obtenir la description détaillée des paramètres du lancement programmé, consultez les paramètres généraux de la tâche.

Consultation des informations sur les mises à jour du logiciel tiers disponibles

Vous pouvez consulter la liste des mises à jour disponibles pour les logiciels tiers, y compris les logiciels Microsoft installés sur les appareils client.

Pour consulter la liste des mises à jour disponibles pour les applications tierces installées sur les appareils client,

Dans le menu principal, accédez à **Opérations** → **Gestion des correctifs** → **Mises à jour du logiciel**.

Une liste des mises à jour disponibles s'affiche.

Vous pouvez indiquer un filtre pour consulter la liste des mises à jour du logiciel. Cliquez sur l'icône **Filtre** ( ) de la liste des mises à jour du logiciel pour gérer le filtre. Vous pouvez également sélectionner l'un des filtres prédéfinis dans la liste déroulante **Filtres prédéfinis** située au-dessus de la liste des vulnérabilités dans les applications.

Pour consulter les propriétés de la mise à jour, procédez comme suit :

1. Cliquez sur le nom de la mise à jour du logiciel concernée.

2. La fenêtre des propriétés de la mise à jour s'ouvre. Cette fenêtre affiche des informations regroupées sous les onglets suivants :

   - **Général**

     Cet onglet affiche les détails généraux de la mise à jour sélectionnée :

     - Mettre à jour l'état d'approbation (peut être modifié manuellement en sélectionnant un nouvel état dans la liste déroulante)
     - Date et heure d'enregistrement de la mise à jour
     - Date et heure de création de la mise à jour
     - Niveau d'importance de la mise à jour
     - Exigences d'installation imposées par la mise à jour
     - Famille d'applications à laquelle appartient la mise à jour
     - Application à laquelle la mise à jour s'applique
     - Numéro de révision de la mise à jour

   - **Attributs**

     Cet onglet affiche un ensemble d'attributs que vous pouvez utiliser pour en savoir plus à propos de la mise à jour sélectionnée. Cet ensemble diffère selon que la mise à jour est publiée par Microsoft ou par un fournisseur tiers.

     L'onglet affiche les informations suivantes pour une mise à jour Microsoft :

     - Niveau d'importance de la mise à jour, d'après Microsoft Security Response Center (MSRC)
     - Lien vers l'article de Microsoft Knowledge Base décrivant la mise à jour
     - Lien vers l'article de Microsoft Security Bulletin décrivant la mise à jour
     - Identifiant de la mise à jour

     L'onglet affiche les informations suivantes pour une mise à jour tierce :

     - Que la mise à jour soit un correctif ou un paquet de distribution complet
     - Langue de localisation de la mise à jour
     - Si la mise à jour est installée automatiquement ou manuellement

- Si la mise à jour a été révoquée après avoir été appliquée
- Lien pour télécharger la mise à jour

- **Appareils**

  Cet onglet affiche une liste des appareils sur lesquels la mise à jour sélectionnée a été installée.

- **Vulnérabilités à corriger**

  Cet onglet affiche une liste de vulnérabilités que la mise à jour sélectionnée peut corriger.

- **Croisement des mises à jour**

  Cet onglet affiche les croisements possibles entre différentes mises à jour publiées pour la même application, c'est-à-dire si la mise à jour sélectionnée peut remplacer d'autres mises à jour (disponible pour les mises à jour Microsoft uniquement).

- **Tâches d'installation de cette mise à jour**

  Cet onglet affiche une liste de tâches dont la zone d'action comprend l'installation de la mise à jour sélectionnée. L'onglet vous permet également de créer une nouvelle tâche d'installation à distance pour la mise à jour.

Pour consulter les statistiques de l'installation d'une mise à jour :

1. cochez la case à côté de la mise à jour du logiciel requise.
2. Cliquez sur le bouton **Statistiques de l'état de l'installation des mises à jour**.

   Le diagramme des états de l'installation des mises à jour s'affiche. Cliquez sur un état pour ouvrir une liste des appareils affichant l'état sélectionné.

Vous pouvez consulter les informations sur les mises à jour du logiciel disponibles pour les logiciels tiers, y compris les logiciels Microsoft installés sur l'appareil administré sélectionné exécutant Windows.

Pour consulter la liste des mises à jour disponibles pour les logiciels tiers installés sur l'appareil administré sélectionné :

1. Dans le menu principal, accédez à **Gestion des ressources** → **Ressources (Appareils)**.

   La liste des appareils administrés s'affiche.
2. Dans la liste des appareils administrés, cliquez sur le lien portant le nom de l'appareil pour lequel vous souhaitez afficher les mises à jour du logiciel.

   La fenêtre des propriétés de l'appareil sélectionné s'affiche.
3. Dans la fenêtre des propriétés de l'appareil sélectionné, ouvrez l'onglet **Avancé**.
4. Dans le volet gauche, sélectionnez la section **Mises à jour non installées**. Si vous souhaitez uniquement afficher les mises à jour installées, activez l'option **Afficher les mises à jour installées**.

La liste des mises à jour du logiciel tiers disponibles pour l'appareil sélectionné s'affiche.

Exportation de la liste des mises à jour du logiciel disponibles vers un fichier

Vous pouvez exporter la liste des mises à jour du logiciel tiers, y compris les logiciels Microsoft, vers un fichier CSV ou TXT. Vous pouvez par exemple utiliser ces fichiers pour les envoyer à votre responsable de la sécurité de l'information ou les stocker à des fins statistiques.

Pour exporter vers un fichier texte la liste des mises à jour disponibles pour les logiciels tiers installés sur tous les appareils administrés, procédez comme suit :

1. Dans le menu principal, accédez à **Opérations** → **Gestion des correctifs** → **Mises à jour du logiciel**.

   Une liste des mises à jour disponibles s'affiche.

   Si vous souhaitez exporter la liste complète des mises à jour, seules les mises à jour affichées sur la page actuelle seront exportées.

   Si vous souhaitez exporter uniquement certaines mises à jour, cochez les cases en regard des mises à jour requises dans la liste.

2. Cliquez sur le bouton **Exporter vers un fichier TXT** ou **Exporter vers un fichier CSV** en fonction du format que vous préférez exporter. Si l'un de ces boutons n'est pas visible, cliquez sur les points de suspension, puis sélectionnez l'option requise dans la liste déroulante.

Le fichier contenant la liste des mises à jour disponibles pour les logiciels tiers, y compris les logiciels Microsoft, est téléchargé sur votre appareil actuel.

Pour exporter vers un fichier texte la liste des mises à jour disponibles pour les logiciels tiers installés sur les appareils administrés sélectionnés, procédez comme suit :

1. Ouvrez la liste des mises à jour du logiciel tiers disponibles sur l'appareil administré sélectionné.

   Une liste des mises à jour disponibles s'affiche.

   Si vous souhaitez exporter la liste complète des mises à jour, seules les mises à jour affichées sur la page actuelle seront exportées.

   Si vous souhaitez exporter uniquement certaines mises à jour, cochez les cases en regard des mises à jour requises dans la liste.

   Si vous souhaitez uniquement exporter les mises à jour installées, cochez la case **Afficher les mises à jour installées**.

2. Cliquez sur le bouton **Exporter vers un fichier TXT** ou **Exporter vers un fichier CSV** en fonction du format que vous préférez exporter. Si l'un de ces boutons n'est pas visible, cliquez sur les points de suspension, puis sélectionnez l'option requise dans la liste déroulante.

Le fichier contenant la liste des mises à jour disponibles pour les logiciels tiers, y compris les logiciels Microsoft, installés sur l'appareil administré sélectionné est téléchargé sur votre appareil actuel.

Approuver et refuser les mises à jour du logiciel tiers

Lorsque vous configurez la tâche *Installation des mises à jour requises et correction des vulnérabilités*, vous pouvez créer une règle qui exige un état particulier des mises à jour qui doivent être installées. Par exemple, une règle de mise à jour peut permettre l'installation des éléments suivants :

- Les mises à jour approuvées uniquement
- Les mises à jour approuvées et non définies uniquement
- Toutes les mises à jour peu importe l'état de la mise à jour

Vous pouvez approuver les mises à jour à installer et refuser les mises à jour qui ne doivent pas installer.

L'utilisation de l'état *Approuvé* pour gérer l'installation des mises à jour est efficace pour un petit nombre de mises à jour. Pour installer plusieurs mises à jour, utilisez les règles que vous pouvez configurer dans les propriétés de la tâche *Installation des mises à jour requises et correction des vulnérabilités*. Nous vous recommandons de définir l'état *Approuvé* uniquement pour les mises à jour particulières qui ne répondent pas aux critères spécifiés dans les règles. Lorsque vous approuvez manuellement un grand nombre de mises à jour, les performances du Serveur d'administration diminuent, ce qui peut entraîner une surcharge du Serveur d'administration.

Pour approuver ou refuser une ou plusieurs mises à jour :

1. Dans le menu principal, accédez à **Opérations** → **Gestion des correctifs** → **Mises à jour du logiciel**.

   Une liste des mises à jour disponibles s'affiche.

2. Sélectionnez les mises à jour que vous souhaitez approuver ou refuser.

3. Cliquez sur le bouton **Approuver** pour approuver les mises à jour sélectionnées ou sur le bouton **Refuser** pour les refuser. Si l'un de ces boutons n'est pas visible, cliquez sur les points de suspension, puis sélectionnez l'option requise dans la liste déroulante.

   L'état par défaut d'une mise à jour est *Indéfini*.

Les mises à jour sélectionnées ont les états que vous avez définis.

En option, vous pouvez modifier l'état d'approbation dans les propriétés d'une mise à jour en particulier.

Pour approuver ou refuser une mise à jour dans ses propriétés, procédez comme suit :

1. Dans le menu principal, accédez à **Opérations** → **Gestion des correctifs** → **Mises à jour du logiciel**.

   Une liste des mises à jour disponibles s'affiche.

2. Cliquez sur le nom de la mise à jour que vous souhaitez approuver ou refuser.

   La fenêtre de propriétés de la mise à jour s'affiche.

3. Dans la section **Général**, sélectionnez un état pour la mise à jour dans la liste déroulante **État d'approbation de la mise à jour**. Vous pouvez sélectionner l'état *Approuvé*, *Rejeté* ou *Indéfini*.

4. Cliquez sur le bouton **Enregistrer** afin d'enregistrer les modifications.

La mise à jour sélectionnée présente l'état que vous avez défini.

Si vous attribuez l'état *Rejeté* aux mises à jour du logiciel tiers, ces mises à jour ne sont pas installées sur les appareils où elles ont été planifiées mais pas encore installées. Les mises à jour seront conservées sur les appareils où elles ont déjà été installées. Si nécessaire, vous pouvez les supprimer manuellement localement.

Création de la tâche Installer les mises à jour requises et corriger les vulnérabilités

La tâche *Installation des mises à jour requises et correction des vulnérabilités* est accessible uniquement en présence d'une licence pour le fonctionnement de Gestion des vulnérabilités et des correctifs.

La tâche *Installation des mises à jour requises et correction des vulnérabilités* est utilisée pour effectuer les mises à jour et réparer les vulnérabilités dans les applications tierces installées sur les appareils administrés. Cette tâche vous permet d'installer plusieurs mises à jour et de corriger plusieurs vulnérabilités selon les règles que vous spécifiez dans les paramètres de la tâche.

Pour installer des mises à jour ou corriger des vulnérabilités à l'aide de la tâche *Installation des mises à jour requises et correction des vulnérabilités*, vous pouvez effectuer l'une des opérations suivantes :

- Exécutez l'assistant d'installation des mises à jour ou l'assistant de correction des vulnérabilités.
- Créez une tâche *Installation des mises à jour requises et correction des vulnérabilités*.
- Ajoutez une règle pour l'installation de la mise à jour à une tâche *Installation des mises à jour requises et correction des vulnérabilités* existante.

Pour créer une tâche Installation des mises à jour requises et correction des vulnérabilités :

1. Dans le menu principal, accédez à **Gestion des ressources** → **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 **Installation des mises à jour requises et correction des vulnérabilités**.

   Si la tâche ne s'affiche pas, assurez-vous que votre compte dispose des droits **Lire**, **Écrire** et **Exécuter** pour la zone fonctionnelle **Administration du système** : **Gestion des vulnérabilités et des correctifs**. Vous ne pouvez pas créer et configurer la tâche *Installation des mises à jour requises et correction des vulnérabilités* sans ces droits d'accès.

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. À l'étape **Définissez les règles d'installation des mises à jour** de l'assistant, ajoutez des règles pour l'installation des mises à jour.

   > Ces règles sont appliquées à l'installation des mises à jour sur les appareils clients. Si les règles ne sont pas définies, la tâche n'a rien à exécuter. Pour en savoir plus sur l'utilisation des règles, consultez le point Règles pour l'installation de la mise à jour.

   Ces règles sont appliquées à l'installation des mises à jour sur les appareils clients. Si vous ne définissez aucune règle, la tâche n'a rien à exécuter.

8. Définissez les paramètres suivants :

   - **Commencer l'installation au moment du redémarrage ou de l'arrêt de l'appareil**

     > Si cette option est activée, les mises à jour sont installées lors du redémarrage ou de l'arrêt de l'appareil. Dans le cas contraire, les mises à jour sont installées selon la programmation.
     >
     > Utilisez cette option si l'installation des mises à jour peut avoir un impact sur les performances de l'appareil.
     >
     > Cette option est Inactif par défaut.

   - **Installer les modules système général requis**

     > Si cette option est activée, l'application, avant d'installer une mise à jour, installe automatiquement tous les composants généraux système (prérequis) requis pour l'installation de la mise à jour. Par exemple, il peut s'agir des mises à jour du système d'exploitation.
     >
     > Si cette option est désactivée, vous devrez peut-être installer les prérequis manuellement.
     >
     > Cette option est Inactif par défaut.

   - **Autoriser l'installation de nouvelles versions de l'application lors des mises à jour**

     > Si cette option est activée, les mises à jour sont autorisées lorsqu'elles entraînent l'installation d'une nouvelle version d'un logiciel.
     >
     > Si cette option est désactivée, le logiciel n'est pas mis à jour. Vous pouvez alors installer les nouvelles versions du logiciel manuellement ou via un autre tâche. Par exemple, vous pouvez utiliser cette option si l'infrastructure de votre entreprise n'est pas prise en charge par une nouvelle version du logiciel ou si vous souhaitez vérifier une mise à jour dans une infrastructure d'essai.
     >
     > Cette option est activée par défaut.
     >
     > > La mise à jour d'une application peut provoquer un dysfonctionnement des applications dépendantes installées sur les appareils clients.

- **Télécharger les mises à jour sur l'appareil sans les installer**

  Quand cette option est activée, l'application télécharge les mises à jour sur l'appareil, mais ne les installe pas automatiquement. Vous pouvez installer les mises à jour manuellement par la suite.

  Les mises à jour Microsoft sont téléchargées dans le stockage Windows système. Les mises à jour des produits tiers (applications développées par des éditeurs d'application autres que Kaspersky et Microsoft) sont téléchargées dans le dossier indiqué dans le champ **Télécharger les mises à jour sur**.

  Si cette option est désactivée, les mises à jour sont installées automatiquement sur l'appareil.

  Cette option est Inactif par défaut.

  - **Télécharger les mises à jour sur**

    Ce dossier est utilisé dans le cadre du téléchargement des mises à jour de produits tiers (applications développées par des éditeurs de logiciels autres que Kaspersky et Microsoft).

- **Activer le diagnostic avancé**

  Quand cette fonction est activée, l'Agent d'administration enregistre des fichiers de trace même si l'écriture de fichiers de trace est désactivée pour l'Agent d'administration dans l'utilitaire de diagnostic à distance Kaspersky Security Center Linux. Les traces sont enregistrées dans deux fichiers en alternance la taille de chacun de ces fichiers est déterminée par la valeur paramètre **Taille maximale (Mo) des fichiers de diagnostic avancé**. Quand les deux fichiers sont remplis, l'Agent d'administration écrit à nouveau dans ceux-ci. Les fichiers avec les traces sont stockés dans le dossier %WINDIR%\Temp. Ces fichiers sont accessibles dans l'utilitaire de diagnostic à distance, vous pouvez les télécharger ou les supprimer à cet endroit.

  Quand cette fonction est désactivée, l'Agent d'administration enregistre les traces conformément aux paramètres définis dans l'utilitaire de diagnostic à distance Kaspersky Security Center Linux. Aucune trace complémentaire n'est écrite.

  Lors de la création d'une tâche, il n'est pas nécessaire d'activer le diagnostic avancé. Par contre, vous pouvez activer cette fonction plus tard si, par exemple, une tâche échoue sur certains appareils et que vous souhaitez obtenir des informations complémentaires lors d'une autre exécution de la tâche.

  Cette option est Inactif par défaut.

  - **Taille maximale (Mo) des fichiers de diagnostic avancé**

    La valeur par défaut est de 100 Mo, mais elle peut se situer entre 1 et 2 048 Mo. Il peut arriver qu'un expert du Support Technique de Kaspersky vous demande de modifier la valeur par défaut lorsque les informations reprises dans les fichiers de diagnostic avancés que vous avez envoyés ne suffisent pas pour résoudre le problème.

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.)**

  Quand cette option est activée, l'application invite l'utilisateur à redémarrer le système d'exploitation selon la fréquence indiquée.

  Cette option est activée par défaut. L'intervalle par défaut est de 5 minutes. La valeur peut être comprise entre 1 et 1 440 minutes.

  Si cette option est désactivée, l'invite est affichée une seule fois.

- **Redémarrer le système au bout de (min.)**

  Après avoir averti l'utilisateur, l'application force le redémarrage du système d'exploitation à l'issue de l'intervalle défini.

  Cette option est activée par défaut. Le délai par défaut est de 30 minutes. La valeur peut être comprise entre 1 et 1 440 minutes.

- **Délai d'attente avant la fermeture forcée des ap&plications dans les sessions bloquées (min)**

  Arrêt forcé des applications lorsque l'appareil de l'utilisateur est verrouillé (arrêt manuel ou automatique après une période d'inactivité).

  Si cette option est activée, les applications en cours sur l'appareil verrouillé seront fermées de force à la fin du délai indiqué dans le champ situé à côté de la case.

  Si cette option est activée, les applications en cours sur l'appareil verrouillé ne seront pas fermées.

  Cette option est Inactif par défaut.

10. Si, à l'étape **Fin de la création de la tâche** de l'Assistant, vous activez l'option **Ouvrir les détails de la tâche à la fin de la création**, vous pouvez modifier les paramètres par défaut de la tâche.

    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.

11. Cliquez sur le bouton **Terminer**.

L'Assistant de création d'une tâche 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.

12. 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, les mises à jour requises sont installées et les vulnérabilités sont corrigées.

Si le serveur WSUS est utilisé dans le réseau de votre organisation (serveur WSUS local) et que vous souhaitez l'utiliser avec le Serveur d'administration de Kaspersky Security Center, vous devez d'abord vous assurer que le Serveur d'administration de Kaspersky Security Center n'est pas utilisé comme serveur WSUS, puis procéder comme suit :

a. Sur vos appareils administrés sous Windows, spécifiez votre serveur WSUS local pour le service de mises à jour Windows. Vous pouvez le faire manuellement dans le registre Windows ou à l'aide d'une stratégie de groupe Windows.

b. Sur votre serveur WSUS local, spécifiez les classifications requises pour les mises à jour et les applications sur lesquelles la distribution des mises à jour doit avoir lieu.

c. Synchronisez votre serveur WSUS avec le serveur en amont (cela peut être un serveur Microsoft WSUS ou un autre serveur WSUS local en amont).

Après l'exécution de la tâche *Installation des mises à jour requises et correction des vulnérabilités* sur l'appareil, l'Agent d'administration utilise le service Windows Update pour installer les mises à jour Windows. Le service Windows Update obtient l'adresse du serveur WSUS externe à partir du registre et télécharge les mises à jour directement à partir de ce serveur externe.

Ajout de règles pour l'installation de la mise à jour

> Cette fonctionnalité est accessible uniquement en présence d'une licence pour le fonctionnement de Gestion des vulnérabilités et des correctifs.

Lors de l'installation de mises à jour logicielles ou de la correction de vulnérabilités dans les applications à l'aide de la tâche *Installation des mises à jour requises et correction des vulnérabilités*, vous devez définir les règles pour l'installation de la mise à jour. Ces règles déterminent les mises à jour à installer et les vulnérabilités à corriger.

Les paramètres exacts dépendent de l'objet pour lequel vous ajoutez une règle : pour toutes les mises à jour, pour les mises à jour Windows Update ou pour les mises à jour d'applications tierces (applications développées par des éditeurs autres que Kaspersky et Microsoft). Lors de l'ajout d'une règle pour des mises à jour Windows Update ou des mises à jour d'applications tierces, vous pouvez sélectionner des applications spécifiques et les versions de l'application pour lesquelles vous souhaitez installer les mises à jour. Lors de l'ajout d'une règle pour toutes les mises à jour, vous pouvez sélectionner les mises à jour spécifiques que vous souhaitez installer et les vulnérabilités que vous souhaitez éliminer en installant les mises à jour.

Vous pouvez ajouter une règle pour l'installation de la mise à jour comme suit :

- En ajoutant une règle lors de la création d'une nouvelle tâche *Installation des mises à jour requises et correction des vulnérabilités*.
- En ajoutant une règle sous l'onglet **Paramètres de l'application** dans la fenêtre des propriétés d'une tâche *Installation des mises à jour requises et correction des vulnérabilités* existante.
- Via l'assistant d'installation des mises à jour ou l'assistant de correction des vulnérabilités.

Ajout de règles pour toutes les mises à jour

Pour ajouter une nouvelle règle pour toutes les mises à jour, procédez comme suit :

1. Cliquez sur **Ajouter**.

   L'Assistant de création de règles se lance. Parcourez les étapes de l'assistant à l'aide du bouton **Suivant**.

2. À l'étape **Sélectionnez le type de règle** de l'assistant, sélectionnez **Règle pour toutes les mises à jour**.

3. À l'étape **Critères généraux** de l'assistant, spécifiez les paramètres suivants :

   - **Définir les mises à jour à installer**

     Sélectionnez les mises à jour qui doivent être installées sur les appareils clients :

     - **Installer uniquement les mises à jour confirmées**. Cette option installe uniquement les mises à jour confirmées.
     - **Installer toutes les mises à jour (sauf les mises à jour rejetées)**. Cette option installe les mises à jour avec l'état *Approuvé* ou *Indéfini*.
     - **Installer toutes les mises à jour (y compris les mises à jour rejetées)**. Ceci installe toutes les mises à jour, quel que soit leur état d'approbation. Sélectionnez cette option avec prudence. Par exemple, utilisez cette option si vous souhaitez vérifier l'installation de certaines mises à jour rejetées dans une infrastructure d'essai.

   - **Corriger les vulnérabilités de niveau de gravité égal ou supérieur à**

     Parfois, les mises à jour du logiciel peuvent nuire à l'expérience de l'utilisateur. Dans ce cas, il se peut que vous décidiez d'installer uniquement les mises à jour critiques au fonctionnement du logiciel et d'ignorer les autres.

Quand cette option est activée, les mises à jour corrigent uniquement les vulnérabilités dont le niveau de gravité tel que défini par Kaspersky est égal ou supérieur à la valeur sélectionnée dans la liste (**Moyenne**, **Élevé** ou **Critique**). Les vulnérabilités dont le niveau de gravité est inférieur à la valeur sélectionnée ne sont pas corrigées.

Si cette option est désactivée, les mises à jour corrigent toutes les vulnérabilités, quel que soit le niveau de gravité.

Cette option est Inactif par défaut.

Accédez à l'étape suivante de l'Assistant.

4. Sélectionnez les mises à jour à installer :

- **Installer toutes les mises à jour convenables**

  Installez toutes les mises à jour du logiciel qui répondent aux critères définis à l'étape **Critères généraux** de l'Assistant. Sélectionné par défaut.

- **Installer uniquement les mises à jour depuis la liste**

  Installer uniquement les mises à jour du logiciel que vous sélectionnez manuellement dans la liste. Cette liste contient toutes les mises à jour du logiciel disponibles.

  Par exemple, vous pouvez sélectionner des mises à jour spécifiques dans les cas suivants : pour vérifier leur installation dans un environnement d'essai, pour mettre à jour uniquement les applications critiques ou pour mettre à jour uniquement certaines applications.

  - **Installer automatiquement toutes les mises à jour précédentes des applications nécessaires à l'installation des mises à jour sélectionnées**

    Conservez cette option si vous acceptez l'installation de versions de l'application intermédiaires quand l'impose l'installation des mises à jour sélectionnées.

    Si vous désactivez cette option, seules les versions sélectionnées des applications sont installées. Désactivez cette option si vous souhaitez mettre à jour les applications d'une manière directe, sans tenter d'installer les versions successives. S'il est impossible d'installer les mises à jour sélectionnées sans installer les versions antérieures de l'application, la mise à jour de l'application échoue.

    Admettons que la version 3 d'une application est installée sur un appareil et vous souhaitez réaliser la mise à jour jusque la version 5, mais la version 5 de cette application peut être installée uniquement sur la version 4. Quand cette option est installée, le logiciel installe d'abord la version 4, puis la version 5. Si l'option est désactivée, le logiciel ne parvient pas à mettre l'application à jour.

    Cette option est activée par défaut.

Accédez à l'étape suivante de l'Assistant.

5. Sélectionnez les vulnérabilités que seront corrigées suite à l'installation des mises à jour sélectionnées :

- **Corriger toutes les vulnérabilités qui correspondent aux autres critères**

  Corrigez toutes les vulnérabilités qui satisfont les critères définis à la page **Critères généraux** de l'assistant. Sélectionné par défaut.

- **Corriger uniquement les vulnérabilités depuis la liste**

  Corrigez uniquement les vulnérabilités que vous sélectionnez manuellement dans la liste. Cette liste contient toutes les vulnérabilités détectées.

  Par exemple, vous pouvez sélectionner des vulnérabilités spécifiques dans les cas suivants : pour vérifier les corrections dans un environnement d'essai, pour corriger les vulnérabilités uniquement dans les applications critiques ou pour corriger les vulnérabilités uniquement dans certaines applications.

Accédez à l'étape suivante de l'Assistant.

6. Spécifiez le nom de la règle que vous ajoutez. Vous pouvez changer ce nom plus tard dans l'onglet **Paramètres de l'application** de la fenêtre des propriétés de la tâche créée.

La nouvelle règle est créée, configurée et affichée dans le tableau des règles de l'Assistant de création d'une tâche.

Ajout de règles pour les mises à jour depuis Windows Update

Pour ajouter une nouvelle règle pour les mises à jour de Windows Update, procédez comme suit :

1. Cliquez sur **Ajouter**.

   L'Assistant de création de règles se lance. Parcourez les étapes de l'assistant à l'aide du bouton **Suivant**.

2. Sélectionnez **Règle pour les mises à jour Windows Update**.

   Accédez à l'étape suivante de l'Assistant.

3. À l'étape **Critères généraux** de l'assistant, spécifiez les paramètres suivants :

   - **Définir les mises à jour à installer**

     Sélectionnez les mises à jour qui doivent être installées sur les appareils clients :

     - **Installer uniquement les mises à jour confirmées**. Cette option installe uniquement les mises à jour confirmées.
     - **Installer toutes les mises à jour (sauf les mises à jour rejetées)**. Cette option installe les mises à jour avec l'état *Approuvé* ou *Indéfini*.
     - **Installer toutes les mises à jour (y compris les mises à jour rejetées)**. Ceci installe toutes les mises à jour, quel que soit leur état d'approbation. Sélectionnez cette option avec prudence. Par exemple, utilisez cette option si vous souhaitez vérifier l'installation de certaines mises à jour rejetées dans une infrastructure d'essai.

   - **Corriger les vulnérabilités de niveau de gravité égal ou supérieur à**

     Parfois, les mises à jour du logiciel peuvent nuire à l'expérience de l'utilisateur. Dans ce cas, il se peut que vous décidiez d'installer uniquement les mises à jour critiques au fonctionnement du logiciel et d'ignorer les autres.

Quand cette option est activée, les mises à jour corrigent uniquement les vulnérabilités dont le niveau de gravité tel que défini par Kaspersky est égal ou supérieur à la valeur sélectionnée dans la liste (**Moyenne**, **Élevé** ou **Critique**). Les vulnérabilités dont le niveau de gravité est inférieur à la valeur sélectionnée ne sont pas corrigées.

Si cette option est désactivée, les mises à jour corrigent toutes les vulnérabilités, quel que soit le niveau de gravité.

Cette option est Inactif par défaut.

- **Corriger les vulnérabilités qui présentent un niveau de gravité selon MSRC égal ou supérieur à**

  Parfois, les mises à jour du logiciel peuvent nuire à l'expérience de l'utilisateur. Dans ce cas, il se peut que vous décidiez d'installer uniquement les mises à jour critiques au fonctionnement du logiciel et d'ignorer les autres.

  Quand cette option est activée, les mises à jour corrigent uniquement les vulnérabilités dont le niveau de gravité tel que défini par Microsoft Security Response Center (MSRC) est égal ou supérieur à la valeur sélectionnée dans la liste (**Bas**, **Moyenne**, **Élevé** ou **Critique**). Les vulnérabilités dont le niveau de gravité est inférieur à la valeur sélectionnée ne sont pas corrigées.

  Si cette option est désactivée, les mises à jour corrigent toutes les vulnérabilités, quel que soit le niveau de gravité.

  Cette option est Inactif par défaut.

4. Sur la page **Applications**, sélectionnez les applications et les versions des applications pour lesquelles vous voulez installer les mises à jour. Toutes les applications sont cochées par défaut.

5. Sur la page **Catégorie des mises à jour**, sélectionnez les catégories des mises à jour à installer. Ces catégories sont les mêmes que dans le catalogue Microsoft Update. Toutes les catégories sont cochées par défaut.

6. La page **Nom** permet de renseigner le nom de la règle ajoutée. Vous pouvez changer ce nom plus tard dans la section **Partenaires** de la fenêtre des propriétés de la tâche créée.

Une fois que l'assistant de création de règles a terminé, la nouvelle règle est ajoutée et s'affiche dans la liste des règles de l'assistant de création d'une tâche ou dans les propriétés de la tâche.

Ajout de règles pour les mises à jour des applications tierces

Pour ajouter une règle pour les mises à jour des produits tiers, procédez comme suit :

1. Cliquez sur **Ajouter**.

   L'Assistant de création de règles se lance. Parcourez les étapes de l'assistant à l'aide du bouton **Suivant**.

2. À l'étape **Sélectionnez le type de règle** de l'assistant, sélectionnez **Règles pour les mises à jour tierces**.

3. À l'étape **Critères généraux** de l'assistant, spécifiez les paramètres suivants :

   - **Définir les mises à jour à installer**

     Sélectionnez les mises à jour qui doivent être installées sur les appareils clients :

     - **Installer uniquement les mises à jour confirmées**. Cette option installe uniquement les mises à jour confirmées.
     - **Installer toutes les mises à jour (sauf les mises à jour rejetées)**. Cette option installe les mises à jour avec l'état *Approuvé* ou *Indéfini*.
     - **Installer toutes les mises à jour (y compris les mises à jour rejetées)**. Ceci installe toutes les mises à jour, quel que soit leur état d'approbation. Sélectionnez cette option avec prudence. Par exemple, utilisez cette option si vous souhaitez vérifier l'installation de certaines mises à jour rejetées dans une infrastructure d'essai.

   - **Corriger les vulnérabilités de niveau de gravité égal ou supérieur à**

     Parfois, les mises à jour du logiciel peuvent nuire à l'expérience de l'utilisateur. Dans ce cas, il se peut que vous décidiez d'installer uniquement les mises à jour critiques au fonctionnement du logiciel et d'ignorer les autres.

     Quand cette option est activée, les mises à jour corrigent uniquement les vulnérabilités dont le niveau de gravité tel que défini par Kaspersky est égal ou supérieur à la valeur sélectionnée dans la liste (**Moyenne**, **Élevé** ou **Critique**). Les vulnérabilités dont le niveau de gravité est inférieur à la valeur sélectionnée ne sont pas corrigées.

     Si cette option est désactivée, les mises à jour corrigent toutes les vulnérabilités, quel que soit le niveau de gravité.

     Cette option est Inactif par défaut.

   Accédez à l'étape suivante de l'Assistant.

4. Sélectionnez les applications et les versions des applications pour lesquelles vous voulez installer les mises à jour.

   Toutes les applications sont cochées par défaut.

   Accédez à l'étape suivante de l'Assistant.

5. Spécifiez le nom de la règle que vous ajoutez. Vous pouvez changer ce nom plus tard dans l'onglet **Paramètres de l'application** de la fenêtre des propriétés de la tâche créée.

La nouvelle règle est créée, configurée et affichée dans le tableau des règles de l'Assistant de création d'une tâche.

Paramètres de la tâche Installation des mises à jour requises et correction des vulnérabilités spécifiés après la création de la tâche

Après la création de la tâche *Installation des mises à jour requises et correction des vulnérabilités*, vous pouvez spécifier les paramètres suivants dans l'onglet **Paramètres de l'application** de la fenêtre des propriétés de la tâche :

- Dans la section **Installation de contrôle** :

  - **Ne pas analyser**. Sélectionnez cette option si vous ne voulez pas exécuter l'installation de contrôle des mises à jour.

  - **Lancer l'analyse sur les appareils indiqués**. Sélectionnez cette option si vous voulez vérifier l'installation des mises à jour sur certains appareils. Cliquez sur le bouton **Ajouter**, puis sélectionnez les appareils sur lesquels vous devez exécuter une installation de contrôle des mises à jour.

  - **Lancer l'analyse sur les appareils dans le groupe indiqué**. Sélectionnez cette option si vous voulez vérifier l'installation des mises à jour sur le groupe d'appareils. Dans le champ **Définissez le groupe test**, indiquez le groupe d'appareils sur lesquels exécuter l'installation de contrôle.

  - **Lancer l'analyse sur le pourcentage indiqué des appareils**. Sélectionnez cette option si vous voulez vérifier l'installation des mises à jour sur le pourcentage d'appareils. Dans le champ **Pourcentage d'appareils de test par rapport à l'ensemble des appareils cibles**, indiquez le pourcentage des appareils qui requièrent l'exécution de l'installation de contrôle des mises à jour.

  Lors de la sélection de n'importe quelle option autre que **Ne pas analyser**, indiquez dans le champ **Temps nécessaire pour décider si l'installation doit être poursuivie, en heures** le nombre d'heures qui doit s'écouler après l'installation de contrôle des mises à jour avant de lancer l'installation des mises à jour sur tous les appareils.

- La section **Mises à jour à installer** permet de consulter la liste des mises à jour que la tâche installe. Seules les mises à jour qui correspondent aux paramètres de la tâche appliqués sont affichées.

Pour obtenir la description complète des paramètres de la tâche, consultez les paramètres généraux de la tâche.

Mise à jour automatique des applications tierces

Certaines applications tierces peuvent être mises à jour automatiquement. Le fournisseur de l'application définit si l'application prend en charge la fonctionnalité de mise à jour automatique. Si une application tierce installée sur un appareil administré prend en charge la mise à jour automatique, vous pouvez définir le paramètre de mise à jour automatique dans les propriétés de l'application. Une fois que vous avez modifié le paramètre de mise à jour automatique, les Agents d'administration appliquent le nouveau paramètre sur chaque appareil administré sur lequel l'application est installée.

Le paramètre de mise à jour automatique est indépendant des autres objets et paramètres de la fonctionnalité de la gestion des vulnérabilités et des correctifs. Par exemple, ce paramètre ne dépend pas d'un état d'approbation de mise à jour ou des tâches d'installation de mise à jour, comme *Installation des mises à jour requises et correction des vulnérabilités* et *Corriger les vulnérabilités*.

Pour configurer le paramètre de mise à jour automatique pour une application tierce, procédez comme suit :

1. Dans le menu principal, accédez à **Opérations** → **Applications tierces** → **Registre des applications**.

2. Cliquez sur le nom de l'application pour laquelle vous souhaitez modifier le paramètre de mise à jour automatique.

   Pour simplifier la recherche, vous pouvez filtrer la liste par les colonnes **État des mises à jour automatiques** et **Administrer les mises à jour automatiques**.

   La fenêtre de propriétés de l'application s'affiche.

3. Dans la section **Général**, sélectionnez une valeur pour la fonctionnalité suivante :

   État des mises à jour automatiques.

   Sélectionnez l'une des options ci-dessous :

   - **Indéfini**

     La fonctionnalité de mise à jour automatique est désactivée. Kaspersky Security Center Linux installe les mises à jour d'applications tierces à l'aide des tâches suivantes : *Installation des mises à jour requises et correction des vulnérabilités* et *Corriger les vulnérabilités*.

   - **Autorisé(e)**

     Une fois que le fournisseur a publié une mise à jour pour l'application, cette mise à jour est installée automatiquement sur les appareils administrés. Il n'y a rien d'autre à faire.

   - **Bloqué**

     Les mises à jour de l'application ne sont pas installées automatiquement. Kaspersky Security Center Linux installe les mises à jour d'applications tierces à l'aide des tâches suivantes : *Installation des mises à jour requises et correction des vulnérabilités* et *Corriger les vulnérabilités*.

4. Cliquez sur le bouton **Enregistrer** afin d'enregistrer les modifications.

Le paramètre de mise à jour automatique est appliqué à l'application sélectionnée.

Correction des vulnérabilités dans les applications tierces

Cette section décrit les fonctions de Kaspersky Security Center Linux associées à la correction des vulnérabilités dans les logiciels installés sur les appareils administrés.

À propos de la recherche et de la correction des vulnérabilités dans les applications

Kaspersky Security Center Linux détecte et répare les vulnérabilités dans les applications sur les appareils administrés exécutant les systèmes d'exploitation Microsoft Windows. Les vulnérabilités sont détectées dans le système d'exploitation et les logiciels tiers, y compris les logiciels Microsoft.

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

Recherche des vulnérabilités dans les applications

Pour rechercher des vulnérabilités dans les applications, Kaspersky Security Center Linux utilise les caractéristiques de la base de données des vulnérabilités connues. Cette base de données a été créée et est mise à jour par les experts de Kaspersky. Elle contient des informations sur les vulnérabilités, telles que la description, la date de détection et le niveau de gravité de la vulnérabilité. Vous pouvez recevoir des informations sur les vulnérabilités dans les applications sur le site Kaspersky.

Kaspersky Security Center Linux utilise la tâche *Recherche de vulnérabilités et de mises à jour requises* pour détecter d'éventuelles vulnérabilités logicielles.

Correction des vulnérabilités dans les applications

Pour corriger les vulnérabilités dans les applications, Kaspersky Security Center Linux utilise les mises à jour logicielles publiées par les fournisseurs de logiciels. Suite à l'exécution de la tâche *Téléchargement des mises à jour sur le stockage du Serveur d'administration*, les métadonnées des mises à jour logicielles sont téléchargées sur le stockage du Serveur d'administration. Cette tâche est destinée à télécharger les métadonnées des mises à jour pour Kaspersky et les logiciels tiers. Cette tâche est créée automatiquement par l'Assistant de configuration initiale de l'application Kaspersky Security Center Linux. Vous pouvez également créer manuellement la tâche *Téléchargement des mises à jour sur le stockage du Serveur d'administration*.

Les mises à jour du logiciel visant à corriger les vulnérabilités peuvent être représentées sous forme de paquets de distribution complets ou de correctifs. Les mises à jour logicielles qui corrigent des vulnérabilités dans les applications sont appelées *correctifs*. L'installation *des correctifs recommandés* est préconisée par les spécialistes Kaspersky. L'installation *des correctifs utilisateur* est manuellement spécifiée par les utilisateurs. Pour installer un correctif utilisateur, vous devez créer un paquet d'installation contenant ce correctif.

Si vous détenez la licence de Kaspersky Security Center Linux assortie de la fonctionnalité Gestion des vulnérabilités et des correctifs, vous pouvez utiliser la tâche *Installation des mises à jour requises et correction des vulnérabilités*. Cette tâche corrige automatiquement de nombreuses vulnérabilités en installant les correctifs recommandés. Pour cette tâche, vous pouvez configurer manuellement certaines règles pour corriger plusieurs vulnérabilités.

Si vous ne détenez pas la licence de Kaspersky Security Center assortie de la fonctionnalité Gestion des vulnérabilités et des correctifs, vous pouvez utiliser la tâche *Corriger les vulnérabilités*. À l'aide de cette tâche, vous pouvez corriger les vulnérabilités en installant les correctifs recommandés pour les logiciels Microsoft et les correctifs utilisateur pour les autres logiciels tiers.

Pour des raisons de sécurité, toutes les mises à jour du logiciel tiers que vous installez à l'aide de la fonction de la gestion des vulnérabilités et des correctifs sont automatiquement analysées à la recherche d'applications malveillantes par les technologies de Kaspersky. Ces technologies sont utilisées pour la vérification automatique des fichiers et incluent la recherche de virus, l'analyse statique, l'analyse dynamique, l'analyse comportementale dans l'environnement sandbox et machine learning.

Les experts de Kaspersky n'effectuent pas d'analyse manuelle des mises à jour du logiciel tiers pouvant être installées par la fonction de la gestion des vulnérabilités et des correctifs. De plus, les experts de Kaspersky ne recherchent pas de vulnérabilités (connues ou inconnues) ou de fonctionnalités non documentées dans ces mises à jour, et n'effectuent pas d'autres types d'analyse des mises à jour que ceux indiqués dans le paragraphe ci-dessus.

Une interaction utilisateur peut être requise lorsque vous mettez à jour une application tierce ou corrigez une vulnérabilité dans une application tierce sur un appareil administré. Par exemple, l'utilisateur peut être invité à fermer l'application tierce si elle est actuellement ouverte.

Pour corriger certaines vulnérabilités dans les applications, vous devrez accepter le Contrat de licence utilisateur final (CLUF) du logiciel en cours d'installation si l'acceptation du CLUF est demandée. Si vous refusez le CLUF, la vulnérabilité logicielle ne sera pas corrigée.

Scénario : Recherche et correction des vulnérabilités dans les logiciels tiers

Cette section fournit un scénario de recherche et de réparation des vulnérabilités sur les appareils administrés sous Windows. Vous pouvez détecter et corriger les vulnérabilités dans le système d'exploitation et dans les logiciels tiers, y compris les logiciels Microsoft.

Prérequis

- Kaspersky Security Center Linux est déployé dans votre entreprise.
- Il existe des appareils administrés sous Windows dans votre organisation.
- Une connexion Internet est requise pour que le Serveur d'administration 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.

Étapes

La recherche et la correction des vulnérabilités logicielles s'effectuent par étapes :

1. **Recherche de vulnérabilités dans les logiciels installés sur les appareils administrés**

   Pour rechercher les vulnérabilités dans les logiciels installés sur les appareils administrés, exécutez la tâche *Recherche de vulnérabilités et de mises à jour requises*. Une fois cette tâche terminée, Kaspersky Security Center Linux reçoit la liste des vulnérabilités détectées et des mises à jour requises pour les logiciels tiers installés sur les appareils que vous avez spécifiés dans les propriétés de la tâche.

   La tâche *Recherche de vulnérabilités et de mises à jour requises* est créée automatiquement par l'Assistant de configuration initiale de l'application Kaspersky Security Center Linux. Si vous n'aviez pas exécuté l'assistant, démarrez-le maintenant ou créez la tâche manuellement.

   > Vous pouvez créer la tâche *Recherche de vulnérabilités et des mises à jour requises* uniquement pour les appareils Windows. Vous ne pouvez pas créer cette tâche pour les appareils fonctionnant sous d'autres systèmes d'exploitation.

2. **Consultation de la liste des vulnérabilités dans les applications détectées**

   Consultez la liste **Vulnérabilités dans les applications** et décidez quelles vulnérabilités doivent être corrigées. Pour consulter les informations détaillées de chaque vulnérabilité, cliquez sur le nom de la vulnérabilité dans la liste. Pour chaque vulnérabilité de la liste, vous pouvez également consulter les statistiques de la vulnérabilité sur les appareils administrés.

3. **Configuration de la correction de la vulnérabilité**

   Lorsque des vulnérabilités sont détectées dans les applications, vous pouvez les corriger sur les appareils administrés à l'aide de la tâche *Installation des mises à jour requises et correction des vulnérabilités* ou de la tâche *Corriger les vulnérabilités*.

   La tâche *Installation des mises à jour requises et correction des vulnérabilités* est utilisée pour effectuer les mises à jour et réparer les vulnérabilités dans les applications tierces, y compris les logiciels Microsoft, installés sur les appareils administrés. Cette tâche vous permet d'installer plusieurs mises à jour et de corriger différentes vulnérabilités en fonction de certaines règles. Notez que cette tâche ne peut être créée que si vous disposez de la licence pour la fonctionnalité Gestion des vulnérabilités et des correctifs. Pour corriger les vulnérabilités dans les applications, la tâche *Installation des mises à jour requises et correction des vulnérabilités* utilise les mises à jour du logiciel recommandées.

   La tâche *Corriger les vulnérabilités* ne nécessite pas l'option de licence pour la fonction Gestion des vulnérabilités et des correctifs. Pour utiliser cette tâche, vous devez spécifier manuellement les correctifs servant à corriger les vulnérabilités du logiciel tiers répertorié dans les paramètres de la tâche. La tâche *Corriger les vulnérabilités* utilise les correctifs recommandés pour les logiciels Microsoft et les correctifs utilisateur pour les logiciels tiers.

   > Vous pouvez créer les tâches *Installation des mises à jour requises et correction des vulnérabilités* et *Corriger les vulnérabilités* uniquement pour les appareils Windows. Vous ne pouvez pas créer ces tâches pour les appareils fonctionnant sous d'autres systèmes d'exploitation.

   Vous pouvez démarrer l'Assistant de correction des vulnérabilités qui crée automatiquement l'une de ces tâches ou vous pouvez créer l'une de ces tâches manuellement.

Si vous avez créé et configuré la tâche *Installation des mises à jour requises et correction des vulnérabilités*, les vulnérabilités sont corrigées automatiquement sur les appareils administrés. Lorsque la tâche créée est lancée, elle met en corrélation la liste des mises à jour du logiciel disponibles avec les règles spécifiées dans les paramètres de la tâche. Toutes les mises à jour logicielles qui répondent aux critères des règles spécifiées sont téléchargées dans le stockage du Serveur d'administration et sont installées pour corriger les vulnérabilités dans les applications.

Si vous avez créé la tâche *Corriger les vulnérabilités*, seules les vulnérabilités des logiciels Microsoft sont corrigées.

4 **Planification des tâches**

Planifiez l'exécution automatique de la tâche *Recherche de vulnérabilités et de mises à jour requises* périodiquement afin que la liste des vulnérabilités soit à jour. La fréquence recommandée est d'une fois par semaine.

Si vous avez créé la tâche *Installation des mises à jour requises et correction des vulnérabilités*, vous pouvez la planifier pour qu'elle soit exécutée à la même fréquence que la tâche *Recherche de vulnérabilités et de mises à jour requises* ou à une fréquence moindre. Lors de la planification de la tâche *Corriger les vulnérabilités*, notez que vous devez sélectionner des correctifs pour les logiciels Microsoft ou définir des correctifs utilisateur pour les logiciels tiers à chaque fois avant de démarrer la tâche.

Lors de la planification des tâches, assurez-vous qu'une tâche créée pour corriger les vulnérabilités démarre une fois que la tâche *Recherche de vulnérabilités et de mises à jour requises* est terminée.

5 **Ignorer les vulnérabilités dans les applications (facultatif)**

Vous pouvez ignorer certaines vulnérabilités dans une application sur tous appareils administrés ou seulement sur les appareils administrés sélectionnés.

6 **Exécution d'une tâche de correction de la vulnérabilité**

Démarrez la tâche *Installation des mises à jour requises et correction des vulnérabilités* ou la tâche *Corriger les vulnérabilités*. Lorsque la tâche est terminée, assurez-vous qu'elle possède le statut *Terminée avec succès* dans la liste des tâches.

7 **Créer le rapport sur les résultats de la correction des vulnérabilités dans les applications (facultatif)**

Pour consulter les statistiques détaillées concernant la correction des vulnérabilités, générez le rapport sur les vulnérabilités. Ce rapport affiche des informations sur les vulnérabilités dans les applications non corrigées. Il vous permet d'identifier et d'éliminer les vulnérabilités des logiciels tiers, y compris les logiciels Microsoft, utilisés dans votre organisation.

8 **Vérification de la configuration de la recherche et de la correction des vulnérabilités dans les logiciels tiers**

Assurez-vous d'avoir effectué les tâches suivantes :

- Obtenu et vérifié la liste des vulnérabilités logicielles sur les appareils administrés.
- Ignoré certaines vulnérabilités logicielles, si vous le souhaitez.
- Configuré la tâche de correction des vulnérabilités.
- Planifié les tâches de recherche et de correction des vulnérabilités logicielles pour qu'elles démarrent en séquence.
- Vérifié que la tâche de correction des vulnérabilités dans les applications a été lancée.

Correction des vulnérabilités logicielles tierces

Pour rechercher des vulnérabilités dans les logiciels tiers, vous pouvez créer et exécuter la tâche *Recherche de vulnérabilités et de mises à jour requises* et recevoir une liste des vulnérabilités logicielles. Une fois que vous avez obtenu la liste des vulnérabilités, vous pouvez les corriger sur les appareils administrés qui fonctionnent sous Windows.

Vous pouvez corriger les vulnérabilités dans le système d'exploitation et dans les applications tierces, y compris les logiciels Microsoft, en créant et en exécutant la tâche Corriger les vulnérabilités ou la tâche Installation des mises à jour requises et correction des vulnérabilités.

> Une interaction utilisateur peut être requise lorsque vous mettez à jour une application tierce ou corrigez une vulnérabilité dans une application tierce sur un appareil administré. Par exemple, l'utilisateur peut être invité à fermer l'application tierce si elle est actuellement ouverte.

Vous pouvez également créer une tâche pour corriger les vulnérabilités dans les applications comme suit :

- En ouvrant la liste des vulnérabilités et en indiquant les vulnérabilités à corriger.

  En conséquence, une nouvelle tâche de correction des vulnérabilités dans les applications est créée. En option, vous pouvez ajouter les vulnérabilités sélectionnées à une tâche existante.

- En exécutant l'Assistant de correction des vulnérabilités.

  > L'Assistant de correction des vulnérabilités est accessible uniquement en présence d'une licence pour le fonctionnement de Gestion des vulnérabilités et des correctifs.

  L'Assistant simplifie la création et la configuration d'une tâche de correction de vulnérabilité et vous permet d'éliminer la création de tâches redondantes.

Correction des vulnérabilités dans les applications en utilisant la liste des vulnérabilités

Pour corriger les vulnérabilités dans les applications en utilisant la liste des vulnérabilités :

1. Ouvrez la liste des vulnérabilités de l'une des manières suivantes :

   - Dans le menu principal, accédez à **Opérations** → **Gestion des correctifs** → **Vulnérabilités dans les applications**.

   - Dans le menu principal, accédez à **Gestion des ressources** → **Ressources (Appareils)** → <nom de l'appareil> → **Avancé** → **Vulnérabilités dans les applications**.

   - Dans la fenêtre principale de l'application, accédez à la section **Opérations** → **Applications tierces** → **Registre des applications** → <nom de l'application> → **Vulnérabilités**.

   Un tableau contenant la liste des vulnérabilités dans les applications tierces installées sur les appareils administrés s'affiche.

2. Dans la liste des vulnérabilités, cochez les cases en regard des vulnérabilités que vous souhaitez corriger, puis cliquez sur le bouton **Corriger la vulnérabilité**.

   Si une mise à jour logicielle recommandée pour corriger l'une des vulnérabilités sélectionnées ne figure pas dans la liste, un message d'information s'affiche.

   Pour corriger certaines vulnérabilités dans les applications, vous devrez accepter le Contrat de licence utilisateur final (CLUF) du logiciel en cours d'installation si l'acceptation du CLUF est demandée. Si vous refusez le CLUF, la vulnérabilité dans l'application ne sera pas corrigée.

3. Sélectionnez l'une des options ci-dessous :

   - **Nouvelle tâche**

     Ceci permet de lancer l'Assistant de création d'une tâche. Si vous disposez d'une licence pour le fonctionnement de Gestion des vulnérabilités et des correctifs, la tâche Installation des mises à jour requises et correction des vulnérabilités est présélectionnée. Si vous ne disposez pas de licence, la tâche Corriger les vulnérabilités est présélectionnée. Suivez les étapes de l'Assistant pour terminer la création de la tâche.

   - **Corriger la vulnérabilité (ajouter une règle à la tâche indiquée)**

     Sélectionnez une tâche à laquelle vous souhaitez ajouter les vulnérabilités sélectionnées. Si vous disposez d'une licence pour le fonctionnement de Gestion des vulnérabilités et des correctifs, sélectionnez une tâche Installation des mises à jour requises et correction des vulnérabilités. Une nouvelle règle pour corriger les vulnérabilités sélectionnées sera automatiquement ajoutée à la tâche sélectionnée. Si vous ne disposez pas de licence, sélectionnez la tâche Corriger les vulnérabilités. Les vulnérabilités sélectionnées sont ajoutées aux propriétés de la tâche.

     La fenêtre de propriétés de la tâche s'affiche. Cliquez sur le bouton **Enregistrer** afin d'enregistrer les modifications.

   Si vous avez choisi de créer une tâche, la tâche est créée et affichée dans la liste des tâches à l'endroit suivant : **Gestion des ressources** → **Tâches**. Si vous avez choisi d'ajouter les vulnérabilités à une tâche existante, les vulnérabilités sont enregistrées dans les propriétés de la tâche.

Pour corriger les vulnérabilités dans les applications tierces, démarrez la tâche Installation des mises à jour requises et correction des vulnérabilités ou la tâche Corriger les vulnérabilités. Si vous avez créé la tâche Corriger les vulnérabilités, vous devez spécifier manuellement les mises à jour du logiciel énumérées dans les paramètres de la tâche.

Correction de vulnérabilités dans les applications à l'aide de l'Assistant de correction des vulnérabilités

L'Assistant de correction des vulnérabilités est accessible uniquement en présence d'une licence pour le fonctionnement de Gestion des vulnérabilités et des correctifs.

Pour corriger les vulnérabilités dans les applications à l'aide de l'Assistant de correction des vulnérabilités, procédez comme suit :

1. Dans le menu principal, accédez à **Opérations** → **Gestion des correctifs** → **Vulnérabilités dans les applications**.

   Un tableau contenant la liste des vulnérabilités dans les applications tierces installées sur les appareils administrés s'affiche.

2. Cochez la case en regard de la vulnérabilité que vous souhaitez corriger.

3. Cliquez sur le bouton **Lancer l'Assistant de correction des vulnérabilités**.

> Le bouton est désactivé si vous sélectionnez plusieurs vulnérabilités.

L'Assistant de correction des vulnérabilités s'ouvre. La liste des tâches existantes s'affiche. Cette liste peut contenir les types de tâches suivants :

- Installation des mises à jour requises et correction des vulnérabilités
- Corriger les vulnérabilités

Vous ne pouvez pas modifier la tâche Corriger les vulnérabilités pour installer de nouvelles mises à jour. Pour installer de nouvelles mises à jour, vous ne pouvez utiliser que la tâche Installation des mises à jour requises et correction des vulnérabilités.

4. Si vous souhaitez que l'assistant affiche uniquement les tâches qui corrigent la vulnérabilité que vous avez sélectionnée, activez l'option **Afficher uniquement les tâches corrigeant la vulnérabilité sélectionnée**.

5. Exécutez une des actions suivantes :

- Pour démarrer une tâche, cochez la case en regard du nom de la tâche, puis cliquez sur le bouton **Démarrer**.

  Aucune autre action n'est nécessaire. Vous pouvez fermer l'assistant. La tâche se poursuivra en mode arrière-plan.

- Pour ajouter une nouvelle règle à une tâche Installation des mises à jour requises et correction des vulnérabilités existante :

  a. Cochez la case en regard du nom de la tâche, puis cliquez sur le bouton **Ajouter une règle**.

  > Le bouton **Ajouter une règle** est désactivé si vous sélectionnez plusieurs tâches.

  Vous ne pouvez pas ajouter de règle pour une tâche Corriger les vulnérabilités. Si vous sélectionnez une tâche Corriger les vulnérabilités, la notification suivante s'affiche : " Pour installer les mises à jour, utilisez la tâche Installation des mises à jour requises et correction des vulnérabilités. "

  b. Sur la page qui s'ouvre, configurez la nouvelle règle :

  - **Règle de correction des vulnérabilités d'un niveau de gravité défini**

    > Parfois, les mises à jour du logiciel peuvent nuire à l'expérience de l'utilisateur. Dans ce cas, il se peut que vous décidiez d'installer uniquement les mises à jour critiques au fonctionnement du logiciel et d'ignorer les autres.
    >
    > Quand cette option est activée, les mises à jour corrigent uniquement les vulnérabilités dont le niveau de gravité, tel que défini par Kaspersky, est égal ou supérieur au niveau de la mise à jour sélectionnée (**Moyenne**, **Élevé** ou **Critique**). Les vulnérabilités dont le niveau de gravité est inférieur à la valeur sélectionnée ne sont pas corrigées.
    >
    > Si cette option est désactivée, les mises à jour corrigent toutes les vulnérabilités, quel que soit le niveau de gravité.
    >
    > Cette option est Inactif par défaut.

- **Règle de correction des vulnérabilités au moyen de mises à jour du même type que la mise à jour définie comme recommandée pour la vulnérabilité sélectionnée**

  Cette règle s'affiche uniquement pour les vulnérabilités logicielles Microsoft.

- **Règle de correction des vulnérabilités dans les applications du fournisseur sélectionné**

  Cette règle s'affiche uniquement pour les vulnérabilités logicielles tierces.

- **Règle de correction d'une vulnérabilité dans toutes les versions de l'application sélectionnée**

  Cette règle s'affiche uniquement pour les vulnérabilités logicielles tierces.

- **Règle de correction de la vulnérabilité sélectionnée**

- **Approuver les mises à jour qui corrigent la vulnérabilité sélectionnée**

  La mise à jour sélectionnée est approuvée pour l'installation. Activez cette option si certaines règles appliquées de l'installation de la mise à jour autorisent l'installation des mises à jour confirmées uniquement.

  Cette option est Inactif par défaut.

c. Cliquez sur **Ajouter**.

La fenêtre de propriétés de la tâche s'affiche. La nouvelle règle est déjà ajoutée aux propriétés de la tâche. Vous pouvez afficher ou modifier la règle ou d'autres paramètres de tâche. Cliquez sur le bouton **Enregistrer** afin d'enregistrer les modifications.

- Pour créer une tâche, procédez comme suit :

  a. Cliquez sur le bouton **Nouvelle tâche**.

  b. Sur la page qui s'ouvre, configurez la nouvelle règle :

  - **Règle de correction des vulnérabilités d'un niveau de gravité défini**

    Parfois, les mises à jour du logiciel peuvent nuire à l'expérience de l'utilisateur. Dans ce cas, il se peut que vous décidiez d'installer uniquement les mises à jour critiques au fonctionnement du logiciel et d'ignorer les autres.

    Quand cette option est activée, les mises à jour corrigent uniquement les vulnérabilités dont le niveau de gravité, tel que défini par Kaspersky, est égal ou supérieur au niveau de la mise à jour sélectionnée (**Moyenne**, **Élevé** ou **Critique**). Les vulnérabilités dont le niveau de gravité est inférieur à la valeur sélectionnée ne sont pas corrigées.

    Si cette option est désactivée, les mises à jour corrigent toutes les vulnérabilités, quel que soit le niveau de gravité.

    Cette option est Inactif par défaut.

  - **Règle de correction des vulnérabilités au moyen de mises à jour du même type que la mise à jour définie comme recommandée pour la vulnérabilité sélectionnée**

    Cette règle s'affiche uniquement pour les vulnérabilités logicielles Microsoft.

  - **Règle de correction des vulnérabilités dans les applications du fournisseur sélectionné**

    Cette règle s'affiche uniquement pour les vulnérabilités logicielles tierces.

- **Règle de correction d'une vulnérabilité dans toutes les versions de l'application sélectionnée**

  Cette règle s'affiche uniquement pour les vulnérabilités logicielles tierces.

- **Règle de correction de la vulnérabilité sélectionnée**

- **Approuver les mises à jour qui corrigent la vulnérabilité sélectionnée**

  La mise à jour sélectionnée est approuvée pour l'installation. Activez cette option si certaines règles appliquées de l'installation de la mise à jour autorisent l'installation des mises à jour confirmées uniquement.

  Cette option est Inactif par défaut.

c. Cliquez sur **Ajouter**.

d. Continuez la création de la tâche dans l'Assistant de création d'une tâche.

La nouvelle règle que vous avez ajoutée dans l'Assistant de correction des vulnérabilités s'affiche à l'étape **Définissez les règles d'installation des mises à jour** de l'Assistant de création d'une tâche. Lorsque vous terminez l'Assistant, la tâche Installation des mises à jour requises et correction des vulnérabilités est ajoutée à la liste des tâches.

Création de la tâche Correction des vulnérabilités

La tâche *Corriger les vulnérabilités* vous permet de corriger les vulnérabilités dans les applications sur les appareils administrés. Vous pouvez corriger les vulnérabilités dans les applications du logiciel tiers, y compris les logiciels Microsoft.

Vous pouvez créer la tâche *Corriger les vulnérabilités* uniquement pour les appareils Windows. Vous ne pouvez pas créer cette tâche pour les appareils fonctionnant sous d'autres systèmes d'exploitation.

Vous pouvez créer de nouvelles tâches *Corriger les vulnérabilités* uniquement si vous disposez de la licence de gestion des vulnérabilités et des correctifs.

Pour corriger de nouvelles vulnérabilités, vous pouvez les ajouter à une tâche *Corriger les vulnérabilités* existante. Toutefois, il est conseillé d'utiliser la tâche *Installation des mises à jour requises et correction des vulnérabilités* plutôt que la tâche *Corriger les vulnérabilités*. La tâche *Installation des mises à jour requises et correction des vulnérabilités* vous permet d'installer plusieurs mises à jour et de corriger automatiquement plusieurs vulnérabilités, selon les règles que vous définissez.

Une interaction utilisateur peut être requise lorsque vous mettez à jour une application tierce ou corrigez une vulnérabilité dans une application tierce sur un appareil administré. Par exemple, l'utilisateur peut être invité à fermer l'application tierce si elle est actuellement ouverte.

Pour créer la tâche Corriger les vulnérabilités, procédez comme suit :

1. Dans le menu principal, accédez à **Gestion des ressources** → **Tâches**.

   Vous pouvez également créer cette tâche dans l'onglet **Tâches** dans la fenêtre des propriétés de l'appareil.

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. À partir de la liste **Type de tâche**, sélectionnez la tâche **Corriger les vulnérabilités**.

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. Cliquez sur **Ajouter**.

   La liste des vulnérabilités s'ouvre.

8. Dans la liste des vulnérabilités, cochez les cases en regard des vulnérabilités que vous souhaitez corriger, puis cliquez sur le bouton **OK**.

   Les vulnérabilités dans les applications Microsoft ont généralement des correctifs recommandés. Aucune action supplémentaire n'est requise pour celles-ci.

   Pour les vulnérabilités dans les applications d'autres fournisseurs, vous devez d'abord définir un correctif utilisateur pour chaque vulnérabilité que vous souhaitez corriger. Par après, vous pourrez ajouter ces vulnérabilités dans la tâche *Corriger les vulnérabilités*.

   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.)**

  Quand cette option est activée, l'application invite l'utilisateur à redémarrer le système d'exploitation selon la fréquence indiquée.

  Cette option est activée par défaut. L'intervalle par défaut est de 5 minutes. La valeur peut être comprise entre 1 et 1 440 minutes.

  Si cette option est désactivée, l'invite est affichée une seule fois.

- **Redémarrer le système au bout de (min.)**

  Après avoir averti l'utilisateur, l'application force le redémarrage du système d'exploitation à l'issue de l'intervalle défini.

  Cette option est activée par défaut. Le délai par défaut est de 30 minutes. La valeur peut être comprise entre 1 et 1 440 minutes.

- **Forcer la fermeture des applications dans les sessions bloquées**

  Les applications en cours d'exécution peuvent empêcher le redémarrage de l'appareil client. Par exemple, si un document est en train d'être modifié dans un logiciel de traitement de texte et qu'il n'est pas enregistré, l'application n'autorise pas le redémarrage de l'appareil.

  Quand cette option est activée, l'arrêt forcé de ces applications sur un appareil verrouillé doit avoir lieu avant de pouvoir redémarrer l'appareil. Les utilisateurs pourraient perdre toute modification qui n'a pas été enregistrée à ce moment.

  Si cette option est désactivée, un appareil verrouillé n'est pas redémarré. L'état de la tâche sur cet appareil indique qu'il faut redémarrer l'appareil. Les utilisateurs doivent quitter manuellement toutes les applications en cours d'exécution sur les appareils verrouillés, puis redémarrer ces appareils.

  Cette option est Inactif par défaut.

Accédez à l'étape suivante de l'Assistant.

10. Définissez les paramètres du compte :

- **Compte par défaut**

  La tâche sera lancée sous le même compte utilisateur sous lequel l'application, exécutant cette tâche, a été installée et lancée.

  Cette option est sélectionnée par défaut.

- **Indiquer un compte**

  Remplissez les champs **Compte utilisateur** et **Mot de passe** pour définir les détails d'un compte à partir duquel la tâche est exécutée. Le compte doit disposer de droits suffisants pour cette tâche.

- **Compte**

  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.

11. Si, à l'étape **Fin de la création de la tâche** de l'Assistant, vous activez l'option **Ouvrir les détails de la tâche à la fin de la création**, vous pouvez modifier les paramètres par défaut de la tâche.

    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.

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 **Gestion des ressources** → **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 l'exécution de la tâche terminée, les vulnérabilités sélectionnées sont corrigées.

Sélection des correctifs utilisateur pour les vulnérabilités dans le logiciel tiers

Pour utiliser la tâche *Corriger les vulnérabilités*, vous devez spécifier manuellement les mises à jour logicielles visant à corriger les vulnérabilités logicielles tierces répertorié dans les paramètres de la tâche. La tâche *Corriger les vulnérabilités* utilise les correctifs recommandés pour les logiciels Microsoft et les correctifs utilisateur pour d'autres logiciels tiers.

Les correctifs utilisateur sont des mises à jour logicielles que l'administrateur spécifie manuellement pour l'installation afin de corriger des vulnérabilités.

Pour sélectionner les correctifs des vulnérabilités dans les logiciels tiers :

1. Dans le menu principal, accédez à **Opérations** → **Gestion des correctifs** → **Vulnérabilités dans les applications**.

   Un tableau contenant la liste des vulnérabilités dans les applications tierces installées sur les appareils administrés s'affiche.

2. Cliquez sur le lien portant le nom des vulnérabilités dans les applications pour laquelle vous souhaitez spécifier un correctif utilisateur.

   La fenêtre des propriétés de la vulnérabilité sélectionnée s'ouvre.

3. Dans le volet gauche, sélectionnez la section **Correctifs utilisateurs et autres**.

   La liste des correctifs utilisateur pour la vulnérabilité logicielle sélectionnée s'affiche.

4. Cliquez sur **Ajouter**.

   Une liste des paquets d'installation disponibles s'affiche. La liste des paquets d'installation affichés correspond à la liste du dossier **Opérations** → **Stockages** → **Paquets d'installation**.

   Si vous n'avez pas créé de paquet d'installation contenant un correctif utilisateur pour la vulnérabilité sélectionnée, vous pouvez créer le paquet maintenant en cliquant sur le bouton **Nouveau**, puis en suivant les étapes de l'Assistant de création du paquet d'installation.

5. Sélectionnez un ou des paquets d'installation contenant un ou des correctifs utilisateur pour la vulnérabilité sélectionnée.

6. Cliquez sur **Enregistrer**.

Les paquets d'installation contenant les correctifs utilisateur pour la vulnérabilité logicielle sont spécifiés. Lorsque vous lancez la tâche *Corriger les vulnérabilités*, le paquet d'installation est installé et la vulnérabilité logicielle est corrigée.

Consultation des informations relatives aux vulnérabilités dans les applications sur tous les appareils administrés

Une fois que vous avez analysé les applications des appareils administrés à la recherche de vulnérabilités, vous pouvez consulter la liste des vulnérabilités détectées dans les applications. Si vous exécutez la tâche pour la hiérarchie des Serveurs d'administration, vous pouvez consulter la liste des appareils administrés pour lesquels des vulnérabilités ont été détectées uniquement pour le Serveur d'administration sélectionné.

Vous pouvez également générer et consulter le rapport sur les vulnérabilités.

Pour consulter la liste des vulnérabilités dans les applications détectées sur tous les appareils administrés,

Dans le menu principal, accédez à **Opérations** → **Gestion des correctifs** → **Vulnérabilités dans les applications**.

La liste des vulnérabilités dans les applications détectées sur les appareils clients s'affiche.

Pour ajuster la liste des vulnérabilités logicielles, procédez comme suit :

Cliquez sur l'icône **Filtre** ( ) dans le coin supérieur droit de la liste des vulnérabilités dans les applications, puis sélectionnez les filtres requis. Vous pouvez également sélectionner l'un des filtres prédéfinis dans la liste déroulante **Filtres prédéfinis** située au-dessus de la liste des vulnérabilités dans les applications.

Vous pouvez obtenir des informations détaillées sur n'importe quelle vulnérabilité de la liste.

Pour obtenir des informations sur une vulnérabilité dans une application,

Cliquez sur le lien avec le nom de la vulnérabilité dans la liste des vulnérabilités dans les applications.

La fenêtre des propriétés de la vulnérabilité dans l'application s'ouvre.

Consultation des informations relatives aux vulnérabilités dans les applications sur l'appareil administré sélectionné

Vous pouvez consulter les informations relatives aux vulnérabilités dans les applications sur l'appareil administré sélectionné sous Windows.

Pour afficher la liste des vulnérabilités logicielles détectées sur l'appareil administré sélectionné :

1. Dans le menu principal, accédez à **Gestion des ressources** → **Ressources (Appareils)**.

   La liste des appareils administrés s'affiche.

2. Dans la liste des appareils administrés, cliquez sur le lien portant le nom de l'appareil pour lequel vous souhaitez afficher les vulnérabilités dans les applications détectées.

   La fenêtre des propriétés de l'appareil sélectionné s'affiche.

3. Dans la fenêtre des propriétés de l'appareil sélectionné, ouvrez l'onglet **Avancé**.

4. Dans le volet gauche, sélectionnez la section **Vulnérabilités dans les applications**.

La liste des vulnérabilités dans les applications détectées sur l'appareil administré sélectionné s'affiche.

Pour consulter les propriétés de la vulnérabilité dans l'application sélectionnée,

cliquez sur le lien avec le nom de la vulnérabilité dans l'application dans la liste des vulnérabilités dans les applications.

La fenêtre des propriétés de la vulnérabilité dans l'application sélectionnée s'affiche.

Consultation des statistiques relatives aux vulnérabilités sur les appareils administrés

Vous pouvez consulter les statistiques pour chaque vulnérabilité dans les applications des appareils administrés. Les statistiques sont représentées sous forme de diagramme. Le diagramme affiche le nombre d'appareils ayant les états suivants :

- *Ignorée sur : <nombre d'appareils>*. Cet état est attribué si vous avez réglé manuellement l'option d'ignorer la vulnérabilité dans les propriétés de cette dernière.
- *Corrigée sur : <nombre d'appareils>*. Cet état est attribué si la tâche visant à corriger la vulnérabilité est terminée avec succès.
- *Correctif prévu sur : <nombre d'appareils>*. Cet état est attribué si vous avez créé la tâche visant à corriger la vulnérabilité, mais qu'elle n'a pas encore été effectuée.
- *Correctif appliqué sur : <nombre d'appareils>*. Cet état est attribué si vous avez sélectionné manuellement la mise à jour du logiciel pour corriger la vulnérabilité, mais que cette mise à jour n'a pas corrigé la vulnérabilité.
- *Correctif nécessaire sur : <nombre d'appareils>*. Cet état est attribué si la vulnérabilité a été corrigée uniquement sur certains appareils administrés et si la correction de la vulnérabilité est nécessaire sur d'autres appareils.

Pour consulter les statistiques d'une vulnérabilité sur les appareils administrés :

1. Dans le menu principal, accédez à **Opérations** → **Gestion des correctifs** → **Vulnérabilités dans les applications**.

   La page affiche une liste des vulnérabilités pour les applications détectées sur les appareils administrés.

2. Cochez la case à côté d'une vulnérabilité.
3. Cliquez sur le bouton **Statistiques de vulnérabilité sur les appareils**.

   > Le bouton **Statistiques de vulnérabilité sur les appareils** est désactivé si vous sélectionnez plusieurs vulnérabilités.

   Un diagramme des états de la vulnérabilité s'affiche. Cliquer sur un état ouvre une liste des appareils sur lesquels la vulnérabilité possède l'état sélectionné.

Exportation de la liste des vulnérabilités dans les applications vers un fichier

Vous pouvez télécharger la liste des vulnérabilités affichées sous forme de fichier CSV ou TXT. Vous pouvez transmettre ces fichiers au responsable de la sécurité de l'information ou les conserver à des fins statistiques.

Pour exporter la liste des vulnérabilités dans les applications détectées sur tous les appareils administrés dans un fichier texte :

1. Dans le menu principal, accédez à **Opérations** → **Gestion des correctifs** → **Vulnérabilités dans les applications**.

   Une liste des vulnérabilités logicielles dans les applications détectées sur les appareils administrés s'affiche.

   Par défaut, seules les vulnérabilités affichées sur la page actuelle sont exportées.

   Si vous souhaitez exporter uniquement des vulnérabilités particulières, cochez les cases en regard de ces vulnérabilités.

2. Cliquez sur le bouton **Exporter vers un fichier TXT** ou **Exporter vers un fichier CSV** en fonction du format que vous préférez exporter. Si l'un de ces boutons n'est pas visible, cliquez sur les points de suspension, puis sélectionnez l'option requise dans la liste déroulante.

Un fichier contenant la liste des vulnérabilités logicielles est téléchargé sur votre appareil.

Pour afficher la liste des vulnérabilités logicielles détectées sur l'appareil administré sélectionné :

1. Dans le menu principal, accédez à **Gestion des ressources** → **Ressources (Appareils)**.

   La liste des appareils administrés s'affiche.

2. Dans la liste des appareils administrés, cliquez sur le lien portant le nom de l'appareil pour lequel vous souhaitez afficher les vulnérabilités dans les applications détectées.

   La fenêtre des propriétés de l'appareil sélectionné s'affiche.

3. Dans la fenêtre des propriétés de l'appareil sélectionné, ouvrez l'onglet **Avancé**.

4. Dans le volet gauche, sélectionnez la section **Vulnérabilités dans les applications**.

La liste des vulnérabilités dans les applications détectées sur l'appareil administré sélectionné s'affiche.

Par défaut, seules les vulnérabilités affichées sur la page actuelle sont exportées.

Si vous souhaitez exporter uniquement des vulnérabilités particulières, cochez les cases en regard de ces vulnérabilités.

1. Cliquez sur le bouton **Exporter vers un fichier TXT** ou **Exporter vers un fichier CSV** en fonction du format que vous préférez exporter. Si l'un de ces boutons n'est pas visible, cliquez sur les points de suspension, puis sélectionnez l'option requise dans la liste déroulante.

Un fichier contenant la liste des vulnérabilités logicielles est téléchargé sur votre appareil.

Ignorer les vulnérabilités dans les applications

Vous pouvez ignorer les vulnérabilités dans les applications à corriger. Par exemple, les raisons d'ignorer les vulnérabilités dans les applications peuvent être les suivantes :

- Vous ne considérez pas la vulnérabilité dans l'application comme critique pour votre entreprise.
- Vous savez que la correction de la vulnérabilité dans l'application peut endommager les données relatives au logiciel pour lequel la correction de la vulnérabilité était nécessaire.
- Vous êtes sûr que la vulnérabilité dans l'application n'est pas dangereuse pour le réseau de votre entreprise car vous utilisez d'autres mesures pour protéger vos appareils administrés.

Vous pouvez ignorer une vulnérabilité dans une application sur tous appareils administrés ou seulement sur les appareils administrés sélectionnés.

Pour ignorer une vulnérabilité dans une application sur tous les appareils administrés :

1. Dans le menu principal, accédez à **Opérations** → **Gestion des correctifs** → **Vulnérabilités dans les applications**.

   Une liste des vulnérabilités logicielles dans les applications détectées sur les appareils administrés s'affiche.

2. Cliquez sur le lien portant le nom de la vulnérabilité dans une application que vous souhaitez ignorer dans la liste des vulnérabilités dans les applications.

   La fenêtre des propriétés de la vulnérabilité dans l'application s'ouvre.

3. Sous l'onglet **Général**, activez l'option **Ignorer la vulnérabilité**.

4. Cliquez sur **Enregistrer**.

   La fenêtre des propriétés de la vulnérabilité logicielle se ferme.

La vulnérabilité dans l'application est ignorée sur les appareils administrés.

Pour ignorer une vulnérabilité dans l'application sur un appareil administré sélectionné :

1. Dans le menu principal, accédez à **Gestion des ressources** → **Ressources (Appareils)**.

   La liste des appareils administrés s'affiche.

2. Dans la liste des appareils administrés, cliquez sur le lien portant le nom de l'appareil pour lequel vous souhaitez ignorer une vulnérabilité dans une application.

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

3. Dans la fenêtre des propriétés de la Appareil, sélectionnez l'onglet **Avancé**.

4. Dans le volet gauche, sélectionnez la section **Vulnérabilités dans les applications**.

   La liste des vulnérabilités dans les applications détectées sur l'appareil s'affiche.

5. Sélectionnez la vulnérabilité que vous souhaitez ignorer sur l'appareil sélectionné dans la liste des vulnérabilités dans les applications.

   La fenêtre des propriétés de la vulnérabilité dans l'application s'ouvre.

6. Dans la fenêtre des propriétés de la vulnérabilité dans l'application de l'onglet **Général**, activez l'option **Ignorer la vulnérabilité**.

7. Cliquez sur **Enregistrer**.

   La fenêtre des propriétés de la vulnérabilité logicielle se ferme.

8. Fermez la fenêtre des propriétés de l'appareil.

La vulnérabilité dans l'application est ignorée sur l'appareil sélectionné.

La vulnérabilité dans l'application ignorée ne sera pas corrigée après la fin de la tâche *Corriger les vulnérabilités* ou de la tâche *Installation des mises à jour requises et correction des vulnérabilités*. Vous pouvez exclure les vulnérabilités logicielles ignorées de la liste des vulnérabilités à l'aide d'un filtre.

Création d'un paquet d'installation d'une application tierce à partir de la base de données Kaspersky

Kaspersky Security Center Web Console vous permet d'effectuer une installation à distance d'applications tierces à l'aide de paquets d'installation. Ces applications tierces sont incluses dans une base de données Kaspersky dédiée. Cette base de données est créée automatiquement lorsque vous exécutez la tâche *Téléchargement des mises à jour sur le stockage du Serveur d'administration* pour la première fois.

> Vous pouvez créer un paquet d'installation d'une application tierce à partir de la base de données Kaspersky uniquement si vous disposez d'une licence de gestion des vulnérabilités et des correctifs.

Pour créer un paquet d'installation d'une application tierce à partir de la base de données Kaspersky, procédez comme suit :

1. Dans le menu principal, accédez à **Découverte et déploiement** → **Déploiement et attribution** → **Paquets d'installation**.

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

   L'Assistant de création du paquet d'installation se lance. Naviguez dans les fenêtres de l'Assistant à l'aide du bouton **Suivant**.

3. Sélectionnez l'option **Sélectionner l'application de la base de Kaspersky pour créer un paquet d'installation**.

   > Cette option est accessible uniquement en présence d'une licence pour le fonctionnement de Gestion des vulnérabilités et des correctifs.

   Accédez à l'étape suivante de l'Assistant.

4. Sélectionnez l'application pour laquelle vous souhaitez créer un paquet d'installation.

   Accédez à l'étape suivante de l'Assistant.

5. Sélectionnez la version linguistique appropriée dans la liste déroulante, puis cliquez sur Suivant.

> Cette étape ne s'affiche que si l'application propose un choix de plusieurs options de langue.

6. Si vous êtes invité(e) à accepter un Contrat de licence pour l'installation, à l'étape **Contrats de licence et Politiques de confidentialité** de l'assistant, procédez comme suit :

   a. Cliquez sur le lien **Afficher** pour lire le Contrat de licence sur le site Internet du fournisseur ou consulter les mises à jour de la licence.

   b. Cochez la case **Je confirme que j'ai entièrement lu, que je comprends et que j'accepte les termes et les conditions de ce Contrat de licence utilisateur final**.

   c. Cliquez sur le bouton **Accepter tout** pour accepter tous les contrats de licence et toutes les politiques de confidentialité qui figurent dans la liste.

7. À l'étape **Nom du nouveau paquet d'installation** de l'assistant, dans le **Nom de l'archive**, entrez le nom du paquet d'installation, puis cliquez sur **Suivant**.

   Le paquet d'installation nouvellement créé est chargé sur le Serveur d'administration. L'Assistant de création du paquet d'installation affiche un message vous informant de la création du paquet d'installation.

8. Cliquez sur le bouton **Terminer**.

Le paquet d'installation nouvellement créé s'affiche dans la liste des paquets d'installation. Vous pouvez sélectionner ce paquet lors de la création ou de la reconfiguration de la tâche Installation à distance d'une application.

> Vous pouvez créer et reconfigurer la tâche Installation à distance d'une application à l'aide d'un paquet d'installation d'une application tierce provenant de la base de données Kaspersky uniquement si vous disposez d'une licence pour la Gestion des vulnérabilités et des correctifs.

Affichage et modification des paramètres d'un paquet d'installation d'une application tierce à partir de la base de données de Kaspersky

Si vous avez précédemment créé des paquets d'installation d'applications tierces mentionnées dans la base de données de Kaspersky, vous pouvez afficher et modifier les paramètres de ces paquets.

> La modification des paramètres d'un paquet d'installation d'une application tierce à partir de la base de données de Kaspersky n'est proposée que sous la licence pour le fonctionnement de Gestion des vulnérabilités et des correctifs.

Pour afficher et modifier les paramètres d'un paquet d'installation d'une application tierce à partir de la base de données de Kaspersky :

1. Dans le menu principal, accédez à **Découverte et déploiement** → **Déploiement et attribution** → **Paquets d'installation**.
2. Dans la liste des paquets d'installation qui s'ouvre, cliquez sur le nom du paquet concerné.

   La fenêtre des propriétés s'ouvre.
3. Modifiez les paramètres si nécessaire.
4. Cliquez sur le bouton **Enregistrer**.

Les paramètres que vous avez modifiés sont enregistrés.

Paramètres d'un paquet d'installation d'une application tierce à partir de la base de données de Kaspersky

Les paramètres d'un paquet d'installation d'une application tierce sont regroupés dans les onglets suivants :

Tous les paramètres répertoriés ci-dessous ne s'affichent pas par défaut. Vous pouvez ajouter les colonnes dont vous avez besoin en cliquant sur le bouton **Filtre**, puis en sélectionnant les noms de colonnes pertinents dans la liste.

- Onglet **Général** :
  - Champ de saisie contenant le nom du paquet d'installation qui peut être modifié manuellement
  - **Application**

    Le nom de l'application tierce pour laquelle le paquet d'installation est créé.
  - **Version**

    Le numéro de version de l'application tierce pour laquelle le paquet d'installation est créé.
  - **Taille**

    La taille du paquet d'installation tiers (en kilo-octets).
  - **Créé**

    La date et l'heure de création du paquet d'installation tiers.
  - **Chemin**

    Le chemin d'accès au dossier réseau où est stocké le paquet d'installation tiers.

- Onglet **Séquence de l'installation** :
  - **Installer les modules système général requis**

    Si cette option est activée, l'application, avant d'installer une mise à jour, installe automatiquement tous les composants généraux système (prérequis) requis pour l'installation de la mise à jour. Par exemple, il peut s'agir des mises à jour du système d'exploitation.

    Si cette option est désactivée, vous devrez peut-être installer les prérequis manuellement.

    Cette option est Inactif par défaut.

  - Tableau affichant les propriétés de mise à jour et contenant les colonnes suivantes :
    - **Nom**

      Le nom de la mise à jour.

    - **Description**

      La description de la mise à jour.

    - **Source**

      La source de la mise à jour, c'est-à-dire si elle a été publiée par Microsoft ou par un autre développeur tiers.

    - **Type**

      Le type de mise à jour, c'est-à-dire si elle est destinée à un pilote ou à une application.

    - **Catégorie**

      La catégorie Windows Server Update Services (WSUS) affichée pour les mises à jour Microsoft (mises à jour critiques, mises à jour des définitions, pilotes, paquets des modules complémentaires, mises à jour de la protection, Service Packs, outils, paquets cumulatifs de mise à jour, mises à jour, mise à niveau).

    - **Niveau d'importance selon MSRC**

      Le niveau d'importance de la mise à jour défini par Microsoft Security Response Center (MSRC).

    - **Niveau d'importance**

      Le niveau d'importance de la mise à jour défini par Kaspersky.

    - **Niveau d'importance du correctif**

      Le niveau d'importance du correctif s'il est destiné à une application Kaspersky.

- **Article**

  L'identifiant (ID) de l'article dans la Base de connaissances décrivant la mise à jour.

- **Bulletin**

  L'identifiant du bulletin de sécurité décrivant la mise à jour.

- **Non désignée pour l'installation (nouvelle version)**

  Indique si la mise à jour présente l'état Non désigné pour l'installation.

- **À installer**

  Indique si la mise à jour présente l'état À installer.

- **Installation**

  Indique si la mise à jour présente l'état Installation.

- **Installée**

  Indique si la mise à jour présente l'état Installée.

- **Échec**

  Indique si la mise à jour présente l'état Échec.

- **Redémarrage requis**

  Indique si la mise à jour présente l'état Redémarrage requis.

- **Enregistrée**

  Affiche la date et l'heure d'enregistrement de la mise à jour.

- **Installation en mode non interactif**

  Indique si la mise à jour nécessite une action de l'utilisateur pendant de l'installation.

- **État d'approbation de la mise à jour**

  Indique si la mise à jour est approuvée pour l'installation.

- **Révision**

  Affiche le numéro de révision actuel de la mise à jour.

- **Identifiant de mise à jour**

  Affiche l'identifiant de la mise à jour.

- **Version de l'application**

  Affiche le numéro de version vers lequel l'application doit être mise à jour.

- **Remplacée**

  Affiche la ou les autres mises à jour qui peuvent remplacer la mise à jour.

- **Remplaçable**

  Affiche la ou les autres mises à jour qui peuvent être remplacées par la mise à jour.

- **Il faut accepter les conditions du Contrat de licence**

  Indique si la mise à jour nécessite l'acceptation des conditions d'un Contrat de licence utilisateur final (CLUF).

- **Descriptions URL**

  Affiche le nom du fournisseur de la mise à jour.

- **Famille d'application**

  Affiche le nom de la famille d'applications à laquelle appartient la mise à jour.

- **Application**

  Affiche le nom de l'application à laquelle appartient la mise à jour.

- **Langue de localisation**

  Affiche la langue de la localisation de la mise à jour.

- **Non désignée pour l'installation (nouvelle version)**

  Indique si la mise à jour présente l'état Non désignée pour l'installation (nouvelle version).

- **L'installation des préaccessoires est requise**

  Indique si la mise à jour présente l'état L'installation des préaccessoires est requise.

- **Mode de téléchargement**

  Affiche le mode de téléchargement de la mise à jour.

- **Est un correctif**

  Indique si la mise à jour est un correctif.

- **Non installée**

  Indique si la mise à jour présente l'état Non installée.

- **Créé**

- L'onglet **Paramètres** affichant les paramètres des paquets d'installation (avec leurs noms, leurs descriptions et leurs valeurs) utilisés comme paramètres de ligne de commande lors de l'installation. Si le paquet ne fournit pas de tels paramètres, le message correspondant s'affiche. Vous pouvez modifier les valeurs de ces paramètres.

- L'onglet **Historique des révisions** qui affiche les révisions du paquet d'installation et qui contient les colonnes suivantes :

  - **Révision** – le numéro de la révision des paquets d'installation.

  - **Heure** – la date et l'heure de modification des paramètres du paquet d'installation.

  - **Utilisateur** – le nom de l'utilisateur ayant modifié les paramètres du paquet d'installation.

  - **Adresse IP de l'appareil de l'utilisateur** – l'adresse IP de l'appareil à partir duquel lequel l'objet a été modifié.

  - **Adresse IP de la Web Console** – l'adresse IP de Kaspersky Security Center Web Console avec laquelle l'objet a été modifié.

  - **Action** – les actions effectuées sur le paquet d'installation dans la révision.

  - **Description** – la description de la révision de modification des paramètres du paquet d'installation.

    Par défaut, la description de la révision n'est pas remplie. Pour ajouter une description de la révision, choisissez la révision requise, puis cliquez sur le bouton **Modifier la description**. Dans la fenêtre qui s'ouvre, saisissez un texte correspondant à la description de la révision.

Correction des vulnérabilités dans un réseau isolé

Cette section décrit les étapes que vous pouvez suivre pour corriger les vulnérabilités des logiciels tiers sur les appareils administrés connectés à des Serveurs d'administration sans accès à Internet.

Scénario : Correction des vulnérabilités des logiciels tiers dans un réseau isolé

Vous pouvez installer des mises à jour et corriger les vulnérabilités des logiciels tiers installés sur les appareils administrés dans un réseau isolé. De tels réseaux incluent les Serveurs d'administration et les appareils administrés qui y sont connectés et qui n'ont pas accès à Internet. Pour corriger les vulnérabilités d'un tel réseau, vous avez besoin d'un Serveur d'administration connecté à Internet. En utilisant le Serveur d'administration avec accès à Internet, vous pourrez télécharger les correctifs (mises à jour requises), puis les transmettre aux Serveurs d'administration isolés.

> Vous pouvez télécharger les mises à jour logicielles tierces émises par les éditeurs de logiciels, mais vous ne pouvez pas télécharger les mises à jour des logiciels Microsoft sur les Serveurs d'administration isolés à l'aide de Kaspersky Security Center.

Pour en savoir plus sur le processus de correction des vulnérabilités dans un réseau isolé, consultez la description et le schéma de ce processus.

Prérequis

Avant de commencer, procédez comme suit :

1. Attribuez un appareil pour la connexion à Internet et le téléchargement des correctifs. Cet appareil sera considéré comme le Serveur d'administration avec accès à Internet.
2. Installez Kaspersky Security Center Linux, au plus tôt de version 15.1, sur les appareils suivants :
   - Appareil alloué, qui agira comme Serveur d'administration avec accès à Internet
   - Appareils isolés, qui agiront comme Serveurs d'administration isolés d'Internet (ci-après dénommés Serveurs d'administration isolés)
3. Assurez-vous que chaque Serveur d'administration dispose suffisamment d'espace disque pour télécharger et stocker les mises à jour et les correctifs.

Étapes

L'installation des mises à jour et la correction des vulnérabilités des logiciels tiers sur les appareils administrés des Serveurs d'administration isolés comprennent les étapes suivantes :

1. **Configuration du Serveur d'administration avec accès à Internet**

   Préparez votre Serveur d'administration avec un accès à Internet pour administrer les demandes de mises à jour logicielles tierces requises et pour télécharger les correctifs.

2. **Configuration des Serveurs d'administration isolés**

   Préparez vos Serveurs d'administration isolés afin qu'ils puissent former régulièrement des listes de mises à jour requises et administrer les correctifs téléchargés par le Serveur d'administration avec accès à Internet. Après la configuration, les Serveurs d'administration isolés n'essayent plus de télécharger les correctifs depuis Internet. Au lieu de cela, ils obtiennent des mises à jour via des correctifs.

3. **Transmission des correctifs et installation des mises à jour sur des Serveurs d'administration isolés**

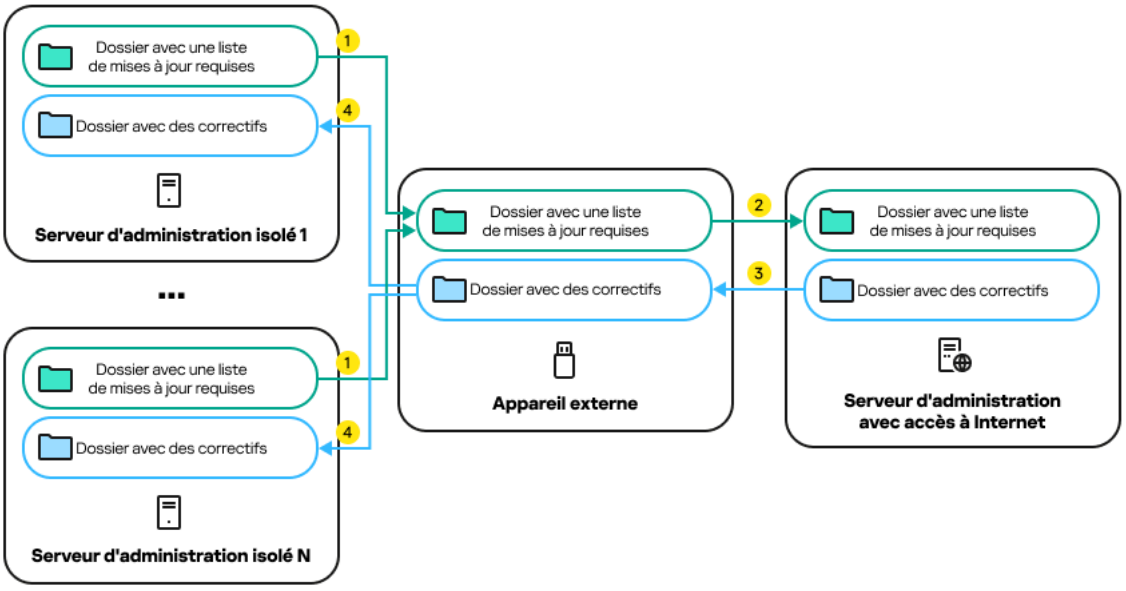
   Une fois la configuration des Serveurs d'administration terminée, vous pouvez transmettre les listes de mises à jour et les correctifs requis à partir du Serveur d'administration avec accès à Internet vers les Serveurs d'administration isolés. Ensuite, les mises à jour des correctifs seront installées sur les appareils administrés à l'aide de la tâche *Installation des mises à jour requises et correction des vulnérabilités*.

Résultats

Ainsi, les mises à jour des logiciels tiers sont transmises aux Serveurs d'administration isolés et installées sur les appareils administrés connectés à l'aide de Kaspersky Security Center Linux. Il suffit de configurer les Serveurs d'administration une fois, et après cela, vous pouvez obtenir des mises à jour aussi souvent que nécessaire, par exemple une ou plusieurs fois par jour.

À propos de la correction des vulnérabilités des logiciels tiers dans un réseau isolé

Le processus de correction des vulnérabilités des logiciels tiers dans un réseau isolé est illustré dans la figure ci-dessous. Vous pouvez répéter ce processus périodiquement.



Le processus de transmission des correctifs et la liste des mises à jour nécessaires entre le Serveur d'administration avec accès à Internet et les Serveurs d'administration isolés

Chaque Serveur d'administration isolé d'Internet (ci-après dénommé Serveur d'administration isolé) génère une liste des mises à jour qui doivent être installées sur les appareils administrés connectés à ce Serveur d'administration. La liste des mises à jour est stockée dans un dossier particulier sous la forme d'un ensemble de fichiers binaires, chacun portant l'identifiant du correctif contenant la mise à jour nécessaire. Par conséquent, chaque fichier de la liste correspond à un correctif particulier.

La liste des mises à jour requises est transférée du Serveur d'administration isolé vers le Serveur d'administration désigné avec accès à Internet à l'aide d'un appareil externe. Ensuite, le Serveur d'administration désigné télécharge les correctifs depuis Internet et les place dans le dossier prévu à cet effet.

Une fois que tous les correctifs sont téléchargés et placés dans le dossier désigné, ils sont retransférés vers chaque Serveur d'administration isolé à partir duquel la liste des mises à jour requises a été obtenue. Les correctifs sont enregistrés dans un dossier créé spécialement pour eux sur chaque Serveur d'administration isolé.

Par conséquent, la tâche *Installation des mises à jour requises et correction des vulnérabilités* exécute les correctifs et installe les mises à jour sur les appareils administrés des Serveurs d'administration isolés.

Configuration du Serveur d'administration avec accès à Internet pour corriger les vulnérabilités dans un réseau isolé

Pour préparer la correction des vulnérabilités et la transmission des correctifs dans un réseau isolé, il convient d'abord de configurer le Serveur d'administration avec un accès à Internet, puis de configurer des Serveurs d'administration isolés.

Pour configurer le Serveur d'administration avec accès à Internet :

1. Créez deux dossiers sur le disque où le Serveur d'administration est installé :

   - Dossier pour la liste des mises à jour requises
   - Dossier pour les correctifs

   Vous pouvez donner à ces dossiers le nom que vous voulez.

2. Accordez le droit **Modifier** au groupe KLAdmins dans les dossiers créés, en utilisant les outils d'administration standard du système d'exploitation.

3. Utilisez l'utilitaire klscflag pour préciser les chemins d'accès aux dossiers dans les propriétés du Serveur d'administration.

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

4. Exécutez les commandes suivantes dans la ligne de commande :

   - Pour définir le chemin d'accès au dossier des correctifs :
     `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v "<chemin d'accès au dossier>"`

   - Pour définir le chemin d'accès au dossier pour la liste des mises à jour requises :
     `klscflag -fset -pv klserver -n VAPM_REQ_IMPORT_PATH -t s -v "<chemin d'accès au dossier>"`

   Exemple : `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v "/FolderForPatches"`

5. Si nécessaire, utilisez l'utilitaire klscflag pour spécifier la fréquence à laquelle le Serveur d'administration doit vérifier les nouvelles demandes de correctif :

```
klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PERIOD_SEC -t d -v <valeur en secondes>
```

Le paramètre par défaut est de 120 secondes.

Exemple : `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PERIOD_SEC -t d -v 120`

6. Créez la tâche *Recherche de vulnérabilités et de mises à jour requises* pour obtenir des informations sur les correctifs des logiciels tiers installés sur les appareils administrés, puis définissez la planification de la tâche.

7. Créez la tâche *Corriger les vulnérabilités* pour spécifier les correctifs pour les logiciels tiers utilisés pour corriger les vulnérabilités, puis définissez la planification de la tâche.

   Démarrez les tâches manuellement si vous souhaitez qu'elles s'exécutent plus tôt qu'il n'est spécifié dans la planification. L'ordre de lancement des tâches est important. La tâche *Corriger les vulnérabilités* doit être lancée après la tâche *Recherche de vulnérabilités et de mises à jour requises*.

8. Relancez le service du Serveur d'administration.

Le Serveur d'administration avec accès à Internet est prêt à télécharger et à transmettre les mises à jour aux Serveurs d'administration isolés. Avant de commencer à corriger les vulnérabilités, configurez des Serveurs d'administration isolés.

Configuration des Serveurs d'administration isolés pour corriger les vulnérabilités d'un réseau isolé

Après avoir configuré le Serveur d'administration avec accès à Internet, préparez chaque Serveur d'administration isolé de votre réseau afin de corriger les vulnérabilités et d'installer les mises à jour sur les appareils administrés connectés à ces Serveurs d'administration isolés.

Pour configurer des Serveurs d'administration isolés, suivez les étapes ci-dessous pour chaque Serveur d'administration :

1. Activez une clé de licence pour la fonction Gestion des vulnérabilités et des correctifs (VAPM).

2. Créez deux dossiers sur le disque où le Serveur d'administration est installé :

   - Dossier pour la liste des mises à jour requises

   - Dossier pour les correctifs

   Vous pouvez donner à ces dossiers le nom que vous voulez.

3. Accordez le droit **Modifier** au groupe KLAdmins dans les dossiers créés, en utilisant les outils d'administration standard du système d'exploitation.

4. Utilisez l'utilitaire klscflag pour préciser les chemins d'accès aux dossiers dans les propriétés du Serveur d'administration.

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

5. Exécutez les commandes suivantes dans la ligne de commande :

   - Pour définir le chemin d'accès au dossier des correctifs :
     ```
     klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v "<chemin d'accès au dossier>"
     ```

   - Pour définir le chemin d'accès au dossier pour la liste des mises à jour requises :
     ```
     klscflag -fset -pv klserver -n VAPM_REQ_EXPORT_PATH -t s -v "<chemin d'accès au dossier>"
     ```

   Exemple : `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v "/FolderForPatches"`

6. Si nécessaire, utilisez l'utilitaire klscflag pour spécifier la fréquence à laquelle le Serveur d'administration isolé doit rechercher de nouveaux correctifs :
   ```
   klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PERIOD_SEC -t d -v <valeur en secondes>
   ```

   Le paramètre par défaut est de 120 secondes.

   Exemple : `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PERIOD_SEC -t d -v 120`

7. Si nécessaire, utilisez l'utilitaire klscflag pour calculer les hachages SHA256 des correctifs :
   ```
   klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_VERIFY_HASH -t d -v 1
   ```

   Si vous exécutez cette commande, vous pouvez vous assurer que les correctifs n'ont pas été modifiés lors de leur transfert sur le Serveur d'administration isolé et que vous avez reçu les bons correctifs contenant les mises à jour requises.

   Par défaut, Kaspersky Security Center Linux ne calcule pas les hachages SHA256 des correctifs. Si vous activez cette option, après la réception des correctifs par le Serveur d'administration isolé, Kaspersky Security Center Linux calcule leurs hachages et compare les valeurs acquises avec les hachages stockés dans la base de données du Serveur d'administration. Si le hachage calculé ne correspond pas au hachage de la base de données, l'erreur se produit et vous devez remplacer les mauvais correctifs.

8. Créez la tâche *Recherche de vulnérabilités et de mises à jour requises* pour obtenir des informations sur les correctifs des logiciels tiers installés sur les appareils administrés, puis définissez la planification de la tâche.

9. Créez la tâche *Corriger les vulnérabilités* pour spécifier les correctifs pour les logiciels tiers utilisés pour corriger les vulnérabilités, puis définissez la planification de la tâche.

   Démarrez les tâches manuellement si vous souhaitez qu'elles s'exécutent plus tôt qu'il n'est spécifié dans la planification. L'ordre de lancement des tâches est important. La tâche *Corriger les vulnérabilités* doit être lancée après la tâche *Recherche de vulnérabilités et de mises à jour requises*.

10. Relancez le service du Serveur d'administration.

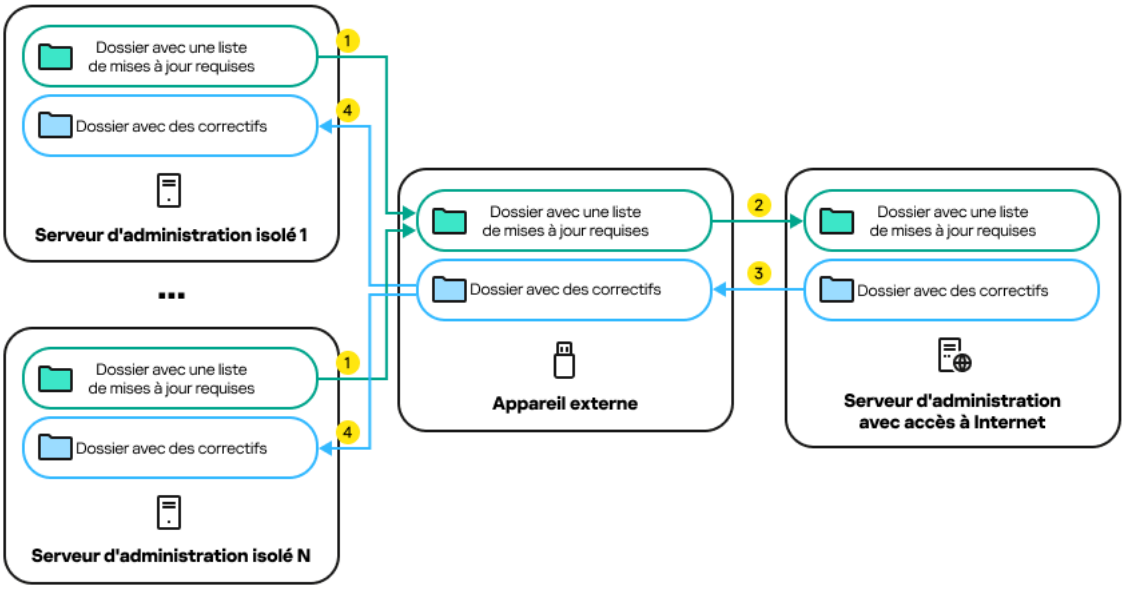
Après avoir configuré tous les Serveurs d'administration, vous pouvez transmettre les correctifs et les listes de mises à jour requises et corriger les vulnérabilités des logiciels tiers sur les appareils administrés dans le réseau isolé.

Transmission des correctifs et installation des mises à jour dans un réseau isolé

Après avoir terminé la configuration des Serveurs d'administration, vous pouvez transférer des correctifs contenant les mises à jour nécessaires du Serveur d'administration avec accès à Internet vers des Serveurs d'administration isolés. Vous pouvez transmettre et installer des mises à jour aussi souvent que nécessaire, par exemple, une ou plusieurs fois par jour.

> Vous avez besoin d'un appareil externe, tel qu'un lecteur amovible, pour transférer les correctifs et la liste des mises à jour nécessaires entre les Serveurs d'administration. Par conséquent, assurez-vous que l'appareil externe a suffisamment d'espace disque pour télécharger et stocker les correctifs.

Le processus de transmission des correctifs et la liste des mises à jour requises sont illustrés dans la figure ci-dessous :



Le processus de transmission des correctifs et la liste des mises à jour nécessaires entre le Serveur d'administration avec accès à Internet et les Serveurs d'administration isolés

Pour installer les mises à jour et corriger les vulnérabilités sur les appareils administrés connectés aux Serveurs d'administration isolés :

1. Lancez la tâche *Installation des mises à jour requises et correction des vulnérabilités* si elle n'est pas encore en cours d'exécution.

2. Connectez un appareil externe à n'importe quel Serveur d'administration isolé.

3. Créez deux dossiers sur l'appareil externe : un pour la liste des mises à jour requises et un pour les correctifs. Vous pouvez donner à ces dossiers le nom que vous voulez.

   Si vous avez créé ces dossiers précédemment, effacez-les.

4. Copiez la liste des mises à jour requises de chaque Serveur d'administration isolé et collez cette liste dans le dossier de la liste des mises à jour requises sur l'appareil externe.

   Ainsi, vous réunissez toutes les listes acquises de tous les Serveurs d'administration isolés dans un seul dossier. Par conséquent, ce dossier doit contenir des fichiers binaires avec les identifiants des correctifs requis pour tous les Serveurs d'administration isolés.

5. Connectez l'appareil externe au Serveur d'administration avec accès à Internet.

6. Copiez la liste des mises à jour requises à partir de l'appareil externe et collez cette liste dans le dossier de la liste des mises à jour requises sur le Serveur d'administration avec accès Internet.

   Tous les correctifs requis sont automatiquement téléchargés depuis Internet dans le dossier des correctifs sur le Serveur d'administration. Cela peut prendre plusieurs heures.

7. Assurez-vous que tous les correctifs requis sont téléchargés. Pour ce faire, vous pouvez effectuer une des actions suivantes :

   - Vérifiez le dossier des correctifs sur le Serveur d'administration avec accès à Internet. Tous les correctifs spécifiés dans la liste des mises à jour requises doivent être téléchargés dans un dossier nécessaire. Ceci est plus pratique si un petit nombre de correctifs est requis.

   - Préparez un script spécial, par exemple un script shell. Si vous obtenez un grand nombre de correctifs, il sera difficile de vérifier par vous-même que tous les correctifs ont été téléchargés. Dans de tels cas, il est préférable d'automatiser le contrôle.

8. Copiez les correctifs depuis le Serveur d'administration avec accès Internet et collez-les dans le dossier correspondant sur votre appareil externe.

9. Transférez les correctifs sur chaque Serveur d'administration isolé. Mettez les correctifs dans un dossier spécifique pour eux.

Par conséquent, chaque Serveur d'administration isolé crée une liste réelle des mises à jour qui sont nécessaires pour les appareils administrés connectés au Serveur d'administration actuel. Une fois que le Serveur d'administration avec accès à Internet a reçu la liste des mises à jour requises, le Serveur d'administration télécharge les correctifs depuis Internet. Lorsque ces correctifs apparaissent sur des Serveurs d'administration isolés, la tâche *Installation des mises à jour requises et correction des vulnérabilités* gère les correctifs. Ainsi, les mises à jour sont installées sur les appareils administrés et les vulnérabilités des logiciels tiers sont corrigées.

Lorsque la tâche *Installation des mises à jour requises et correction des vulnérabilités* est en cours d'exécution, ne redémarrez pas l'appareil du Serveur d'administration et n'exécutez pas la tâche *Sauvegarde des données du Serveur d'administration* (cela entraînera également un redémarrage). Par conséquent, la tâche *Installation des mises à jour requises et correction des vulnérabilités* est interrompue et les mises à jour ne sont pas installées. Dans ce cas, vous devez redémarrer cette tâche manuellement ou attendre que la tâche démarre selon la planification configurée.

Désactivation de la transmission des correctifs et de l'installation des mises à jour dans un réseau isolé

Vous pouvez désactiver la transmission des correctifs sur des Serveurs d'administration isolés, par exemple, si vous décidez de retirer un ou plusieurs Serveurs d'administration d'un réseau isolé. Ainsi, vous pouvez réduire le nombre de correctifs et le temps nécessaire pour les télécharger.

Pour désactiver la transmission des correctifs aux Serveurs d'administration isolés, procédez comme suit :

1. Si vous souhaitez retirer tous les Serveurs d'administration de l'isolement, supprimez, dans les propriétés du Serveur d'administration avec accès à Internet, les chemins d'accès aux dossiers destinés aux correctifs et la liste des mises à jour requises. Si vous souhaitez conserver certains Serveurs d'administration dans un réseau isolé, ignorez cette étape.

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

   Exécutez les commandes suivantes dans la ligne de commande :

   - Pour supprimer le chemin d'accès au dossier des correctifs :
     ```
     klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v ""
     ```
   - Pour supprimer le chemin d'accès au dossier pour une liste des mises à jour requises :
     ```
     klscflag -fset -pv klserver -n VAPM_REQ_IMPORT_PATH -t s -v ""
     ```

2. Redémarrez le service sur le Serveur d'administration avec accès à Internet si vous avez supprimé les chemins d'accès aux dossiers.

3. Dans les propriétés de chaque Serveur d'administration isolé que vous souhaitez retirer du réseau isolé, supprimez les chemins d'accès aux dossiers des correctifs et la liste des mises à jour requises.

   Sous un compte avec des privilèges root, exécutez les commandes suivantes dans la ligne de commande :

   - Pour supprimer le chemin d'accès au dossier des correctifs :
     ```
     klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v ""
     ```
   - Pour supprimer le chemin d'accès au dossier pour une liste des mises à jour requises :
     ```
     klscflag -fset -pv klserver -n VAPM_REQ_EXPORT_PATH -t s -v ""
     ```

4. Redémarrez le service de chaque Serveur d'administration sur lequel vous avez supprimé les chemins d'accès aux dossiers.

Si vous avez reconfiguré le Serveur d'administration avec accès à Internet, les correctifs ne seront plus transmis via Kaspersky Security Center Linux.

Si vous n'avez reconfiguré que des Serveurs d'administration particuliers et que vous les avez supprimés du réseau isolé, ils ne recevront plus les correctifs via Kaspersky Security Center Linux. Seuls les Serveurs d'administration qui restent dans le réseau isolé continueront à recevoir les correctifs.

Si vous souhaitez commencer à corriger les vulnérabilités sur les Serveurs d'administration isolés désactivés à l'avenir, vous devez configurer ces Serveurs d'administration et le Serveur d'administration avec accès à internet encore une fois.

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,

Installez le paquet KlAkOAPI depuis l'archive KlAkOAPI.tar.gz sur l'appareil sur lequel le Serveur d'administration est installé.

Le paquet KlAkOAPI comprend un ensemble d'échantillons qui effectuent des opérations typiques. 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. L'archive KlAkOAPI.tar.gz qui contient ce paquet se trouve dans le dossier d'installation de Kaspersky Security Center Linux.

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

Exemple	Objectif de l'exemple	Scénario
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 d'administration sur les Serveurs d'administration secondaires	Vous pouvez vous connecter au Serveur d'administration primaire, télécharger une clé de licence requise à partir de celui-ci et transmettre cette clé à tous les Serveurs d'administration secondaires inclus dans une hiérarchie.	Licence des applications administrées
Créer un rapport des droits d'utilisateur effectifs	Vous pouvez créer les rapports différents . Par exemple, vous pouvez générer le rapport des droits d'utilisateur effectifs en utilisant cet exemple. Ce rapport décrit les droits dont dispose un utilisateur, en fonction de son groupe et de son rôle. Vous pouvez télécharger le rapport au format HTML, PDF ou Excel.	Génération et affichage d'un rapport
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
Créer des utilisateurs internes, créer et envoyer par email un paquet d'installation Android	Vous pouvez créer des utilisateurs internes à l'aide de la classe SecurityPolicy , créer un paquet d'installation Android et l'envoyer aux utilisateurs par email.	Ajout d'un compte d'un utilisateur interne

Applications interagissant avec Kaspersky Security Center Linux via OpenAPI

Certaines applications interagissent avec Kaspersky Security Center Linux via OpenAPI. Ces 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 pouvez développer à l'aide 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 comme à partir des serveurs de mise à jour de Kaspersky. Dans ce cas, il faut créer la tâche *Télécharger les mises à jour sur les stockages des points de distribution* pour l'appareil qui fait office de point de distribution.
  - 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.

La hiérarchie des Serveurs d'administration prend en charge le mode multilocation. Ce mode permet à un administrateur principal de gérer indépendamment plusieurs clients de manière centralisée. Chaque entreprise cliente ou bureau client est isolé des autres et est appelé locataire. Vous pouvez allouer plusieurs appareils administrés ainsi que leurs données, paramètres, stratégies et tâches associés à un locataire, et configurer les droits des utilisateurs par locataire.

Un Serveur d'administration principal, installé dans l'infrastructure principale de l'entreprise, fait office de locataire principal. Le Serveur d'administration principal permet aux Serveurs d'administration secondaires ou virtuels (ses locataires isolés) de recevoir et de traiter indépendamment leurs propres événements et de fonctionner avec leurs propres ressources, services et configurations.

Un fournisseur de services qui compte plusieurs entreprises clientes peut proposer les fonctionnalités de Kaspersky Security Center Linux, y compris l'agrégation des alertes et les actions de réponse, à chaque entreprise cliente de manière indépendante. Pour ce faire, le fournisseur de services connecte des Serveurs d'administration secondaires ou virtuels en tant que locataires pour chaque entreprise cliente. Le fournisseur de services dispense ses services au moyen de son propre personnel et de ses propres ressources.

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.
Tantor (voir versions prises en charge)	Utilisez ce SGBD si vous prévoyez d'utiliser un seul Serveur d'administration pour moins de 50 000 appareils. Le SGBD Tantor est pris en charge uniquement sur Astra Linux Special Edition RUSB.10015-01 (mise à jour opérationnelle 1.8).

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.

Maintien des connexions inactives

Pour améliorer la stabilité de la connexion, nous vous recommandons de configurer les paramètres keepalive suivants sur les appareils de passerelle de connexion :

- `net.ipv4.tcp_keepalive_intvl` indique la fréquence d'envoi des messages keepalive après le premier. Définissez ce paramètre sur `1`.
- `net.ipv4.tcp_keepalive_probes` indique combien de messages keepalive peuvent être envoyés sans réponse avant que la connexion ne soit considérée comme interrompue. Définissez ce paramètre sur `10`.
- `net.ipv4.tcp_keepalive_time` indique le délai d'attente après le dernier paquet de données avant l'envoi du premier message keepalive. Définissez ce paramètre sur `900`.

Pour configurer les paramètres keepalive :

1. Ouvrez le fichier /etc/sysctl.conf.
2. Ajoutez les valeurs de paramètre suivantes :

```
net.ipv4.tcp_keepalive_intvl = 1
net.ipv4.tcp_keepalive_probes = 10
net.ipv4.tcp_keepalive_time = 900
```

3. Exécutez la commande suivante pour mettre à jour les paramètres keepalive :

```
sudo sysctl -p /etc/sysctl.conf
```

4. Exécutez les commandes suivantes pour vous assurer que les valeurs des paramètres ont bien été appliquées :

```
sudo sysctl net.ipv4.tcp_keepalive_intvl
sudo sysctl net.ipv4.tcp_keepalive_probes
sudo sysctl net.ipv4.tcp_keepalive_time
```

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.

Pour plus d'informations sur la protection des appareils mobiles, reportez-vous à la section Gestion des appareils mobiles.

Sous Microsoft Windows XP, un Agent d'administration peut ne pas effectuer correctement les opérations suivantes : télécharger les mises à jour directement à partir des serveurs de Kaspersky (comme point de distribution) ; fonctionner comme proxy KSN (comme point de distribution) et détecter les vulnérabilités tierces (si la gestion des vulnérabilités et des correctifs est utilisée).

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. Vous pouvez tracer l'itinéraire vers un point de distribution à l'aide de l'utilitaire tracert ou traceroute.

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).

Le groupe Appareils administrés comprend les groupes contenant des Serveurs d'administration, ainsi que les groupes Bureau 1 et Bureau 2.

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. 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 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. La modification 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 :

- 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 **Gestion des ressources** → **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 démarrage rapide crée une tâche de sauvegarde des paramètres du Serveur d'administration qui démarre chaque jour à 4 h 00. Les copies de sauvegarde sont enregistrées par défaut dans le dossier /var/opt/kaspersky/KSC_Backups*.

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 :

- Le nouveau Serveur d'administration doit se voir attribuer le même nom DNS.

  Si une adresse IP statique a été définie dans le paquet d'installation de l'Agent d'administration lors du déploiement des Agents d'administration, vous devez également attribuer la même adresse IP au nouveau Serveur 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).

- Dans le fichier de configuration IAM `var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml` , pour le `server_iam.ksc_address`, définissez exactement la même adresse du Serveur d'administration que celle indiquée dans le nom alternatif du sujet (SAN) du certificat du Serveur d'administration précédemment appliqué. Pour en savoir plus, consultez l'article suivant : Ajout de l'adresse du Serveur d'administration à la configuration du serveur IAM.

- 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. Réinstallez Web Console une fois la restauration terminée.

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.

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.

À propos du transfert de l'Agent d'administration à d'autres Serveurs d'administration

L'application Kaspersky Security Center Linux prévoit la possibilité de transférer l'Agent d'administration sur un appareil client vers d'autres Serveurs d'administration en cas de modification des caractéristiques du réseau suivantes :

- **Condition de l'adresse du serveur DHCP** : modification de l'adresse IP du serveur DHCP (Dynamic Host Configuration Protocol) dans le réseau.

  Le paramètre **Condition de l'adresse du serveur DHCP** n'est actuellement pas disponible.

- **Condition de l'adresse de la passerelle de connexion par défaut** : modification de la passerelle principale du réseau.
- **Condition du domaine DNS** : modification du suffixe DNS du sous-réseau.
- **Condition de l'adresse du serveur DNS** : l'adresse IP du serveur DNS dans le réseau a été modifiée.
- **Condition de l'adresse du serveur WINS** : modification de l'adresse IP du serveur WINS dans le réseau. Ce paramètre est disponible uniquement pour les appareils exécutant Windows.
- **Condition de la résolution des noms** : le nom DNS ou NetBIOS de l'appareil client a changé.
- **Condition du sous-réseau** : modifie l'adresse et le masque du sous-réseau.

- **Condition de l'accessibilité du domaine Windows** : modification de l'état du domaine Windows auquel l'appareil client est connecté. Ce paramètre est disponible uniquement pour les appareils exécutant Windows.

- **Condition de l'accessibilité de l'adresse de connexion SSL** : l'appareil client peut ou ne peut pas (selon l'option sélectionnée) établir une connexion SSL avec un serveur défini (nom:port). Vous devez utiliser un serveur dédié équipé d'un logiciel capable de gérer une charge élevée et des demandes fréquentes de connexion de l'Agent d'administration. N'indiquez pas le port du Serveur d'administration. Pour chaque serveur, vous pouvez également définir un certificat SSL. Dans ce cas, l'Agent d'administration vérifie le certificat du serveur en plus de vérifier la capacité d'une connexion SSL. Si le certificat ne correspond pas, la connexion échoue.

Paramètres de connexion d'origine de l'Agent d'administration au Serveur d'administration lors de l'installation de l'Agent d'administration. Par la suite, quand des règles de permutation de l'Agent d'administration sur d'autres Serveurs d'administration sont rédigées, l'Agent d'administration réagit aux modifications des caractéristiques du réseau de la manière suivante :

- Si les caractéristiques du réseau correspondent à une des règles formées, l'Agent d'administration se connecte au Serveur d'administration indiqué dans cette règle. Si la règle le prévoit, les applications installées sur les appareils clients adopteront les stratégies pour les utilisateurs autonomes.

- Si une des règles n'est pas exécutée, l'Agent d'administration revient aux paramètres d'origine de connexion au Serveur d'administration définis lors de l'installation. Les applications installées sur les appareils clients reviennent aux stratégies actives.

- Si le Serveur d'administration est inaccessible, l'Agent d'administration utilise les stratégies pour les utilisateurs autonomes.

L'Agent d'administration bascule vers la stratégie pour les utilisateurs autonomes uniquement si l'option **Activer le mode de l'utilisateur autonome quand le Serveur d'administration n'est pas disponible** est activée dans les paramètres de la stratégie de l'Agent d'administration.

Les paramètres de connexion de l'Agent d'administration au Serveur d'administration sont préservés dans le profil de connexion. Le profil de connexion permet de créer des règles de permutation des appareils clients vers les stratégies pour les utilisateurs autonomes, ainsi que de configurer le profil de sorte qu'il soit uniquement utilisé pour le téléchargement des mises à jour.

Création d'un profil de connexion pour les utilisateurs itinérants

Pour créer le profil de connexion de l'Agent d'administration au Serveur d'administration pour les utilisateurs itinérants, procédez comme suit :

1. Si vous souhaitez créer un profil de connexion pour un groupe d'appareils administrés, ouvrez la stratégie de l'Agent d'administration de ce groupe. Pour ce faire, procédez comme suit :

   a. Dans le menu principal, accédez à **Gestion des ressources** → **Stratégies**.

   b. Sélectionnez le groupe d'administration pour lequel le profil de connexion doit être créé :

      - Pour le groupe racine, vous pouvez passer à l'étape suivante.

      - Pour un sous-groupe, cliquez sur le bouton **Afficher la hiérarchie** en haut de la page, puis dans la fenêtre qui s'ouvre, cliquez sur le nom du sous-groupe requis.

Le chemin vers le groupe sélectionné est affiché en haut de la page. Si nécessaire, vous pouvez cliquer sur un lien avec le nom du groupe d'administration pour accéder au groupe. Par défaut, le dernier lien du chemin est inactif. Vous pouvez également fermer la fenêtre de la hiérarchie en cliquant sur le bouton **Masquer la hiérarchie**.

c. Ajoutez la stratégie de l'Agent d'administration pour le groupe d'appareils administrés. Si vous l'avez déjà créé, cliquez sur le nom de la stratégie de l'Agent d'administration pour ouvrir les propriétés de la stratégie.

2. Si vous souhaitez créer un profil de connexion pour un appareil administré spécifique, procédez comme suit :

   a. Dans le menu principal, accédez à **Gestion des ressources** → **Ressources (Appareils)**.

   b. Cliquez sur le nom de l'appareil administré.

   c. Dans la fenêtre des propriétés de l'appareil administré qui s'ouvre, accédez à l'onglet **Applications**.

   d. Cliquez sur le nom de la stratégie de l'Agent d'administration à laquelle seul l'appareil administré sélectionné s'applique.

3. Dans la fenêtre des propriétés qui s'ouvre, accédez à **Paramètres de l'application** → **Connectivité** → **Profils de connexion.**

4. Dans la section **Profils de connexion au Serveur d'administration**, cliquez sur le bouton **Ajouter**.

   Par défaut, la liste des profils de connexion contient les profils <Offline mode> et <Home Administration Server>. Les profils ne peuvent être modifiés ou supprimés.

   Le profil <Offline mode> ne définit aucun serveur pour la connexion. Par conséquent, l'Agent d'administration, une fois transféré vers ce profil, ne tente aucune connexion à un Serveur d'administration quelconque tant que les applications installées sur les appareils clients utilisent les stratégies pour les utilisateurs itinérants. Le profil <Offline mode> est invoqué quand les appareils sont déconnectés du réseau.

   Le profil <Home Administration Server> spécifie la connexion pour le Serveur d'administration qui a été sélectionnée lors de l'installation de l'Agent d'administration. Le profil <Home Administration Server> est invoqué quand un appareil qui fonctionnait dans un autre réseau se connecte à nouveau au Serveur d'administration domestique.

5. Dans la fenêtre **Configurer le profil** qui s'ouvre, configurez les paramètres du profil de connexion :

   - **Nom du profil**

     Le champ de saisie permet de consulter ou de modifier le nom du profil de connexion.

   - **Adresse du Serveur d'administration**

     Adresse du Serveur d'administration auquel l'appareil client doit se connecter lors de l'activation du profil.

   - **Numéro de port**

     Numéro du port utilisé pour la connexion.

- **Port SSL**

  Numéro de port utilisé pour la connexion par protocole SSL.

- **Utiliser une connexion SSL**

  Si l'option est activée, la connexion aura lieu via un port sécurisé à l'aide du protocole SSL.

  Cette option est activée par défaut. Nous vous recommandons de ne pas désactiver cette option afin que votre connexion reste sécurisée.

- Sélectionnez l'option **Utiliser un serveur proxy** si vous souhaitez utiliser un serveur proxy pour vous connecter à Internet. Si cette option est sélectionnée, les champs sont disponibles pour saisir les paramètres. Configurez les paramètres suivants de connexion au serveur proxy :

  - **Adresse**

    Adresse du serveur proxy pour la connexion de Kaspersky Security Center Linux à Internet.

  - **Numéro de port**

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

  - **Authentification du serveur proxy**

    Si la case est cochée, les champs de saisie permettent d'indiquer les identifiants pour l'authentification sur le serveur proxy.

  - **Nom d'utilisateur**

    Compte utilisateur sous lequel la connexion au serveur proxy est établie (ce champ est disponible si la case **Authentification du serveur proxy** est cochée).

  - **Mot de passe**

    Mot de passe défini par l'utilisateur sous le compte duquel la connexion au serveur proxy est établie (ce champ est disponible si la case **Authentification du serveur proxy** est cochée).

    Pour voir le mot de passe saisi, cliquez sur le bouton **Afficher** et maintenez-le enfoncé aussi longtemps que vous en avez besoin.

- **Adresse de la passerelle de connexion**

  Adresse de la passerelle via laquelle la connexion entre les appareils clients et le Serveur d'administration s'opère.

- **Activer le mode de l'utilisateur autonome quand le Serveur d'administration n'est pas disponible**

  Cochez cette case afin que lors de la connexion, les applications installées sur un appareil client utilisent les profils de stratégie pour les appareils en mode de l'utilisateur autonome et les stratégies pour les utilisateurs itinérants si le Serveur d'administration est inaccessible. Si aucune stratégie pour les utilisateurs autonomes n'est définie pour l'application, c'est la stratégie active qui sera utilisée.

  Si l'option est activée, les applications utiliseront les stratégies actives.

  Celle-ci est décochée par défaut.

- **Utiliser uniquement pour récupérer les mises à jour**

  Si l'option est désactivée, le profil sera utilisé uniquement lors du téléchargement des mises à jour par les applications installées sur l'appareil client. Pour les autres opérations, la connexion au Serveur d'administration sera réalisée selon les paramètres de connexion d'origine définis lors de l'installation de l'Agent d'administration.

  Cette option est activée par défaut.

- **&Synchroniser les paramètres de connexion aux paramètres du Serveur d'administration indiqués dans ce profil**

  Si l'option est activée, l'Agent d'administration se connecte au Serveur d'administration en utilisant les paramètres utilisés dans les propriétés du profil.

  Si l'option est désactivée, l'Agent d'administration se connecte au Serveur d'administration en utilisant les paramètres d'origine définis lors de l'installation.

  Cette option n'est accessible que si l'option **Utiliser uniquement pour récupérer les mises à jour** est désactivée.

  Cette option est Inactif par défaut.

Finalement, le profil de connexion de l'Agent d'administration au Serveur d'administration pour les utilisateurs itinérants sera créé. Lors de la connexion de l'Agent d'administration au Serveur d'administration via ce profil de l'application, les applications installées sur l'appareil client utiliseront les stratégies pour les appareils en mode de l'utilisateur autonome et les stratégies pour les utilisateurs autonomes.

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 **Gestion des ressources** → **Ressources (Appareils)**.

   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

Restrictions de Kaspersky Security Center Linux

Le tableau ci-après reprend les restrictions de la version actuelle de Kaspersky Security Center Linux.

Restrictions de Kaspersky Security Center Linux

Type de restriction	Valeur
Nombre maximal d'appareils administrés par un Serveur d'administration	50 000
Nombre maximum d'appareils pour lesquels l'option **Maintenir la connexion au Serveur d'administration** est sélectionnée	300
Nombre maximum des groupes d'administration	10 000
Nombre maximum d'événements enregistrés	45 000 000
Nombre maximum de stratégies	2000
Nombre maximum de tâches	2000
Nombre maximum de profils dans une stratégie	100
Nombre maximum de Serveurs d'administration secondaires pour un Serveur d'administration principal	500
Nombre maximum de Serveurs d'administration virtuels	500
Nombre maximum d'appareils qu'un point de distribution peut desservir	10 000
Nombre maximum d'appareils qui peuvent utiliser une passerelle de connexion unique	10 000, y compris des appareils mobiles
Nombre maximal d'appareils mobiles sur un Serveur d'administration	100 000, moins le nombre d'appareils administrés fixes

Calculs pour les Serveurs d'administration

Cette section donne les exigences logicielles et matérielles applicables aux appareils utilisés comme Serveurs d'administration, Elle fournit également des recommandations sur le calcul du nombre de serveurs d'administration et de leur hiérarchie en fonction de la configuration du réseau de l'organisation.

Calcul des ressources matérielles pour le Serveur d'administration

Cette section donne les calculs servant à guider la planification des ressources matérielles pour le Serveur d'administration.

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.

Vous devez activer le fichier d'échange sur l'appareil sur lequel le Serveur d'administration est installé. La taille minimale du fichier d'échange doit être 1.5 fois supérieure au volume de la mémoire RAM.

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 des nœuds pour un cluster de basculement

Matériel	Valeur
Processeur	16 noyaux, 2500 MHz
Mémoire vive	32 Go
Espace disque	500 Go, 300 IOPS ou plus
Contrôleur d'interface réseau	1 Gbit/s

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	22 Go
Espace disque	250 Go, 150 IOPS ou plus

Configuration des nœuds pour un cluster de basculement

Matériel	Valeur
Processeur	16 noyaux, 2500 MHz
Mémoire vive	32 Go
Espace disque	500 Go, 300 IOPS ou plus
Contrôleur d'interface réseau	1 Gbit/s

Configuration de l'appareil sur lequel le Serveur d'administration et le SGBD PostgreSQL sont installés

Matériel	Valeur
Processeur	16 cœurs (20 cœurs recommandés), 2 500 MHz
Mémoire vive	34 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	6 noyaux, 2 500 MHz
Mémoire vive	10 Go
Espace disque	200 Go, 150 IOPS ou plus

Configuration des nœuds pour un cluster de basculement

Matériel	Valeur
Processeur	16 noyaux, 2500 MHz
Mémoire vive	32 Go
Espace disque	500 Go, 300 IOPS ou plus
Contrôleur d'interface réseau	1 Gbit/s

Configuration de l'appareil sur lequel le Serveur d'administration et le SGBD PostgreSQL sont installés

Matériel	Valeur
Processeur	8 cœurs (14 cœurs recommandés), 2 500 MHz
Mémoire vive	18 Go
Espace disque	300 Go, 300 IOPS ou plus

Le réseau comporte 1 000 appareils

Configuration de l'appareil avec le Serveur d'administration

Matériel	Valeur
Processeur	2 noyaux, 2 500 MHz
Mémoire vive	6 Go
Espace disque	10 Go, 150 IOPS ou plus

Configuration de l'appareil sur lequel le SGBD PostgreSQL est installé

Matériel	Valeur
Processeur	2 noyaux, 2 500 MHz
Mémoire vive	4 Go
Espace disque	20 Go, 150 IOPS ou plus

Configuration des nœuds pour un cluster de basculement

Matériel	Valeur
Processeur	16 noyaux, 2500 MHz
Mémoire vive	32 Go
Espace disque	500 Go, 300 IOPS ou plus
Contrôleur d'interface réseau	1 Gbit/s

Configuration de l'appareil sur lequel le Serveur d'administration et le SGBD PostgreSQL sont installés

Matériel	Valeur
Processeur	4 noyaux, 2500 MHz
Mémoire vive	10 Go
Espace disque	30 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.

  > Si les appareils administrés comprennent des machines virtuelles dynamiques, C représente la somme du nombre d'appareils administrés non dynamiques et du nombre de machines virtuelles dynamiques dotées de l'Agent d'administration créées entre deux exécutions consécutives de la tâche **Maintenance du Serveur d'administration**.

- " 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.

  Si les appareils administrés comprennent des machines virtuelles dynamiques, C représente la somme du nombre d'appareils administrés non dynamiques et du nombre de machines virtuelles dynamiques dotées de l'Agent d'administration créées entre deux exécutions consécutives de la tâche **Maintenance du Serveur d'administration**.

- " 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 dédiés dans un réseau comprenant un seul segment de réseau, en fonction du nombre d'appareils du réseau

Nombre d'appareils clients par segment de 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 dédiés dans un réseau comprenant plusieurs segments de réseau, en fonction du nombre d'appareils du réseau

Nombre d'appareils clients dans chaque 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 par segment de 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 dans chaque 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.

Enregistrement des événements sur 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 ce cas, il est recommandé de sélectionner une des deux options dans les paramètres de la tâche :

- **Sauvegarder les événements relatifs au déroulement des tâches**. 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 l'article suivant : 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 le paramètre **Sauvegarder les événements relatifs au déroulement des tâches** dans les propriétés des tâches générales, telles que les tâches de mise à jour. Pour en savoir plus, consultez l'article suivant : Conservation des événements pour les tâches et les stratégies.

Optimisez les paramètres de la tâche d'inventaire. Pour en savoir plus, consultez l'article suivant : 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 :

- Copie de 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 d'administration vers chaque appareil administré	Trafic de chaque appareil 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

Scénario	Trafic du Serveur d'administration vers chaque appareil administré	Trafic de chaque appareil administré vers le Serveur d'administration
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.

Problèmes connus et restrictions

Kaspersky Security Center Linux présente les restrictions suivantes, qui n'ont pas une incidence critique sur le fonctionnement de l'application :

- 9959974 : la fenêtre des propriétés de l'appareil sous l'onglet **Événements** inclut l'option **Tout sélectionner** pour supprimer les événements. L'utilisation de cette option peut entraîner la suppression de tous les événements de la base de données du Serveur d'administration, y compris ceux provenant d'autres appareils et ceux du Serveur d'administration lui-même.

- 10532098 : lors de la création de paquets d'installation pour installer l'application sur des appareils Windows, si vous recevez le message **Une erreur s'est produite. Veuillez réessayer le téléchargement**. Dans ce cas, suivez les étapes supplémentaires pour télécharger les dépendances nécessaires à la création de paquets d'installation.

- 9392997 : Après avoir sondé un contrôleur de domaine ALD Pro ou FreeIPA, un message d'erreur est ajouté au journal des événements. Cette erreur se produit lorsque le compte utilisé pour interroger le domaine ne dispose pas des autorisations nécessaires pour lire les attributs **ipaUniqueID** et **nsUniqueId**. Pour résoudre le problème, ajoutez le compte utilisé pour le sondage du domaine aux groupes d'administrateurs **admins** et **ald trust** dans le domaine ALD Pro ou FreeIPA.

- 10302954 : lors de la définition des conditions d'une règle de déplacement d'appareils, si vous activez, sous l'onglet **Réseau**, le paramètre **L'appareil se trouve dans un sous-groupe du groupe Domaines**, la liste déroulante des sous-groupes est vide.

- 9302142 : l'option **Utiliser l'Agent d'administration en tant que passerelle de connexion en DMZ** n'est pas prise en charge sous Microsoft Windows sur l'architecture ARM.

- 9504495 : Lors de l'attribution d'un utilisateur en tant que propriétaire d'un appareil à l'aide des paramètres du paquet d'installation de l'Agent d'administration, l'attribution peut être incorrecte. Pour éviter ce problème, ajoutez l'utilisateur à la liste d'exclusion de l'authentification à deux facteurs avant l'installation.

- 9316206 : Lors de l'ouverture de l'onglet **Authentification à deux facteurs** des propriétés du Serveur d'Administration et de l'actualisation du navigateur, les boutons de contrôle peuvent disparaître de tous les tableaux de cet onglet. Ce problème ne se produit que si l'assistant de démarrage rapide n'a pas été exécuté jusqu'au bout. Pour afficher les boutons du tableau, retournez dans les propriétés du Serveur d'administration, puis accédez à l'onglet **Authentification à deux facteurs**. Pour résoudre complètement ce problème, suivez toutes les étapes de l'assistant de démarrage rapide.

- 9065814 : Une erreur peut se produire lors d'une tentative d'authentification de domaine à partir d'un appareil Windows dans un domaine Samba 4.

- 9335676 : Après avoir changé le nœud principal d'un cluster de SGBD à haute disponibilité, l'accès à Kaspersky Security Center Web Console peut être indisponible ou subir des retards importants. Si Kaspersky Security Center Web Console reste inaccessible pendant plus de 10 minutes, redémarrez le service IAM à l'aide de la commande suivante :

  ```
  systemctl restart kliam_srv.service
  ```

- 9157005, 9157085 : Lors de l'exécution de la tâche *Installation des mises à jour requises et correction des vulnérabilités* sur un appareil administré sous Windows avec l'option **Commencer l'installation au moment du redémarrage ou de l'arrêt de l'appareil** activée, la tâche peut échouer et afficher une erreur. Ce problème peut se produire lorsqu'un grand nombre de mises à jour doivent être installées. Pour résoudre le problème, exécutez la tâche sans activer l'option **Commencer l'installation au moment du redémarrage ou de l'arrêt de l'appareil**.

- 9272534 : Si le tableau des utilisateurs contient plus de 50 000 utilisateurs, seuls les 50 000 premiers utilisateurs sont affichés, et les autres utilisateurs ne sont pas affichés.

- 9291235 : Après la restauration d'une sauvegarde sur le Serveur d'administration version 16.1, Kaspersky Security Center Web Console affiche la page de connexion. Une fois l'authentification réussie, un code de sécurité à usage unique pour l'authentification à deux facteurs est demandé. Lorsqu'un code de sécurité à usage unique valide est saisi, un message d'erreur s'affiche, indiquant que le code de sécurité à usage unique est incorrect. Dans ce cas, attendez quelques minutes, puis actualisez manuellement la page pour réessayer de vous connecter à Kaspersky Security Center Web Console. Une fois le processus de restauration de la sauvegarde terminé, l'authentification aboutira lors de la tentative suivante.

- 7939561 : Lors d'une tentative de modification d'un compte utilisateur protégé, le fait de cliquer sur le bouton **Annuler** dans la fenêtre de saisie des informations d'identification pour **Protection du compte** entraîne une erreur.

- 8562938 : L'ouverture du port pour les appareils mobiles dans les propriétés de la stratégie du Serveur d'administration n'active pas la fonctionnalité Administration des appareils mobiles et ne déclenche pas la génération d'un certificat mobile. Pour activer la fonctionnalité Administration des appareils mobiles, le port pour les appareils mobiles doit être ouvert dans les propriétés du Serveur d'administration.

- 8732282 : Pour un utilisateur qui dispose de l'option **L'utilisateur ne peut pas modifier le mot de passe** dans les propriétés du compte au sein d'Active Directory, l'action de réponse **Réinitialiser le mot de passe** dans Active Directory ne sera pas exécutée. L'administrateur du contrôleur de domaine doit désactiver l'option **L'utilisateur ne peut pas modifier le mot de passe** pour cet utilisateur ou réinitialiser le mot de passe manuellement. Ce problème survient si vous possédez la licence Kaspersky Next XDR Optimum, si l'intégration à Active Directory est activée et si l'utilisateur fait partie d'un groupe de sécurité Active Directory.

- 8688182 : Si l'option **Le mot de passe n'expire jamais** de l'utilisateur est activée dans les propriétés du compte d'Active Directory, après l'exécution de l'action de réponse **Réinitialiser le mot de passe**, l'option **Le mot de passe n'expire jamais** est désactivée, et l'utilisateur devra modifier son mot de passe de domaine lors de la prochaine connexion. Ce problème survient si vous possédez la licence Kaspersky Next XDR Optimum, si l'intégration à Active Directory est activée et si l'utilisateur fait partie d'un groupe de sécurité Active Directory.

- 8703857 : La connexion au serveur proxy pour Kaspersky Security Center Web Console et les plug-ins Internet d'administration est établie uniquement si le serveur proxy prend en charge l'authentification de base.

- 7939561 : Une erreur se produit lorsque vous cliquez sur le bouton **Annuler** dans la fenêtre **Protection du compte**.

- 7911778 : Lorsque vous exécutez la tâche **Désinstallation à distance d'une application** pour désinstaller l'Agent d'administration d'un appareil qui exécute un système d'exploitation avec l'architecture Arm et qui présente également une heure non synchronisée avec le Serveur d'administration, l'état de la tâche ne passe pas de **En cours d'exécution** à **Terminée**, même après l'Agent d'administration a été désinstallé de l'appareil. Pour résoudre ce problème, synchronisez l'heure de l'appareil sur lequel est installé l'Agent d'administration et l'heure de l'appareil où se trouve le Serveur d'administration avant de lancer **Désinstallation à distance d'une application**.

- 6896585 : Un appareil administré ne peut pas se connecter à KSN via le service KSN Proxy si Kaspersky Security Center Linux est installé sur un appareil dont le nom comporte des caractères cyrilliques.

- 7523299 : L'Agent d'administration ne redémarre pas après avoir arrêté son processus sur un appareil administré fonctionnant sous CentOS 6.6.

- 7835858 : Si vous créez une tâche avec les **paramètres de planification Tous les N jours** et Selon les jours de la semaine dans Kaspersky Security Center Web Console version 15.2 ou ultérieure, et que vous ouvrez ensuite la tâche dans des versions antérieures de Kaspersky Security Center Web Console ou dans la Console d'administration (par exemple, lorsque la tâche est également appliquée sur les Serveurs d'administration secondaires qui peuvent être basés à la fois sur Linux et sur Windows), les paramètres de planification peuvent être affichés de manière incorrecte ou une erreur peut se produire.

- 7555541 : Si vous créez la tâche *Modifier le mot de passe du compte (Linux uniquement)* pour un utilisateur et activez l'option **Définir comme mot de passe à usage unique (l'utilisateur doit modifier le mot de passe après la première connexion)**, l'utilisateur ne peut pas se connecter à Kaspersky Security Center Web Console après avoir modifié le mot de passe à usage unique.

- 7208621 : 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.

- 6511063 : 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.

- 5915107 : Dans les rapports au format lettre, un saut de page peut couper une ligne de texte horizontalement.

- 5556109 : 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.

- 7069744 : Vous ne pouvez pas modifier le compte qui lui est attribué lorsque la tâche *Exécuter des scripts à distance* démarre. Pour modifier le compte utilisateur auquel la tâche est attribuée, il faut arrêter la tâche dans les paramètres de la tâche et la créer de nouveau avec les bons détails du compte.

- 7555788 : La tâche *Modifier le mot de passe du compte* peut ne pas fonctionner correctement si SELinux est activé sur l'appareil de l'utilisateur. Pour en savoir plus sur la désactivation de SELinux, consultez le guide de l'utilisateur pour votre système d'exploitation.

- 9093038 : Si le Serveur d'administration de Kaspersky Security Center Linux ne démarre pas après l'installation et que le journal du système d'exploitation contient l'erreur 213/SECUREBITS liée à kladminserver_srv.service, exécutez les commandes suivantes en tant que superutilisateur :

  ```
  mkdir -p /etc/systemd/system/kladminserver_srv.service.d
  echo "[Service]" > /etc/systemd/system/kladminserver_srv.service.d/override.conf
  echo "AmbientCapabilities=CAP_IPC_LOCK" >> /etc/systemd/system/kladminserver_srv.service.d/override.conf
  mkdir -p /etc/systemd/system/klwebsrv_srv.service.d
  echo "[Service]" > /etc/systemd/system/klwebsrv_srv.service.d/override.conf
  echo "AmbientCapabilities=CAP_IPC_LOCK" >> /etc/systemd/system/klwebsrv_srv.service.d/override.conf
  ```

  Si Kaspersky Security Center Web Console ne démarre pas après l'installation et que le journal du système d'exploitation contient l'erreur 213/SECUREBITS liée à KSCWebConsole.service, exécutez les commandes suivantes en tant que superutilisateur :

  ```
  mkdir -p /etc/systemd/system/KSCSvcWebConsole.service.d
  echo "[Service]" > /etc/systemd/system/KSCSvcWebConsole.service.d/override.conf
  echo "AmbientCapabilities=CAP_IPC_LOCK" >> /etc/systemd/system/KSCSvcWebConsole.service.d/override.conf
  mkdir -p /etc/systemd/system/KSCWebConsoleManagement.service.d
  echo "[Service]" > /etc/systemd/system/KSCWebConsoleManagement.service.d/override.conf
  echo "AmbientCapabilities=CAP_IPC_LOCK" >> /etc/systemd/system/KSCWebConsoleManagement.service.d/override.conf
  mkdir -p /etc/systemd/system/KSCWebConsoleNATS.service.d
  echo "[Service]" > /etc/systemd/system/KSCWebConsoleNATS.service.d/override.conf
  echo "AmbientCapabilities=CAP_IPC_LOCK" >> /etc/systemd/system/KSCWebConsoleNATS.service.d/override.conf
  mkdir -p /etc/systemd/system/KSCWebConsolePlugin.service.d
  echo "[Service]" > /etc/systemd/system/KSCWebConsolePlugin.service.d/override.conf
  echo "AmbientCapabilities=CAP_IPC_LOCK" >> /etc/systemd/system/KSCWebConsolePlugin.service.d/override.conf
  mkdir -p /etc/systemd/system/KSCWebConsole.service.d
  echo "[Service]" > /etc/systemd/system/KSCWebConsole.service.d/override.conf
  echo "AmbientCapabilities=CAP_IPC_LOCK" >> /etc/systemd/system/KSCWebConsole.service.d/override.conf
  ```

  Si le service kliam_srv ne démarre pas après l'installation et que le journal du système d'exploitation contient l'erreur 213/SECUREBITS liée au service, exécutez les commandes suivantes en tant que superutilisateur :

  ```
  mkdir -p /etc/systemd/system/kliam_srv.service.d
  echo "[Service]" > /etc/systemd/system/kliam_srv.service.d/override.conf
  echo "AmbientCapabilities=CAP_IPC_LOCK" >> /etc/systemd/system/kliam_srv.service.d/override.conf
  ```

- 9165434 : L'authentification NTLM ne fonctionne pas pour les comptes utilisateurs appartenant au groupe Utilisateurs protégés.

Contacter le Support Technique

Cette section décrit comment profiter du support technique et les conditions d'accès à celui-ci.

Façons de profiter du support technique

Si vous n'avez pas trouvé de solution à votre problème dans la documentation ou dans d'autres sources d'information sur Kaspersky Security Center Linux, nous vous recommandons de contacter le Support technique. Les experts du support technique répondront à toutes vos questions concernant l'installation et l'utilisation de Kaspersky Security Center.

Kaspersky apporte un soutien en relation avec Kaspersky Security Center pendant son cycle de vie (voir la page du cycle de vie du support de l'application). Avant de contacter le Support Technique, il est recommandé de lire les règles d'octroi du support technique.

Vous pouvez contacter les experts du Support Technique d'une des manières suivantes :

- En vous rendant sur le site Internet du Support Technique
- En envoyant une demande au Support technique de Kaspersky 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 de vos requêtes en ligne pendant leur traitement par les Experts Kaspersky et en conserver l'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 tombe en panne, vous pouvez contacter le Support technique de Kaspersky. Le Support technique peut vous demander d'envoyer les fichiers de vidage du Serveur d'administration pour une analyse plus approfondie chez Kaspersky.

Les fichiers de vidage peuvent contenir des données personnelles. Il est recommandé de protéger vos informations contre tout accès non autorisé avant de les envoyer à Kaspersky.

Sources d'informations sur l'application

Page Kaspersky Security Center 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.

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

Un employé de l'entreprise cliente chargé de surveiller l'état de la sécurité antivirus.

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 Windows. Il existe des versions distinctes de l'Agent d'administration pour les applications Kaspersky sous Novell®, Unix™ et Mac.

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.

Agent de mise à jour

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.

Appareil MDM iOS

Appareil mobile qui se connecte au Serveur MDM iOS via le protocole MDM iOS. Le protocole MDM iOS permet de connecter et d'administrer les appareils ayant un système d'exploitation iOS.

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.

Bases 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 du Serveur d'administration permet d'authentifier ce dernier lorsque la Console d'administration s'y connecte et lors des communications avec les appareils clients. Le certificat du Serveur d'administration est créé lors de l'installation du module Serveur d'administration et conservé dans le dossier %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert 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 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)

Un appareil, un serveur ou un poste de travail sur lequel l'Agent d'administration et les applications Kaspersky administrées sont installés et fonctionnent.

Cloud Discovery

Cloud Discovery gère l'accès des utilisateurs aux services cloud. Microsoft Teams, Salesforce et Microsoft Office 365 sont des exemples de services cloud. Les services cloud sont regroupés en catégories, par exemple *Partage de fichiers*, *Messagerie instantanée* et *Email*.

Console d'administration

Le composant de Kaspersky Security Center Linux qui fournit l'interface utilisateur des services d'administration du Serveur d'administration et de l'Agent d'administration.

Copie de 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 :

- La base de connaissances 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)
- Le certificat du Serveur d'administration.

Domaine multidiffusion

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

La période pendant laquelle vous êtes autorisé à utiliser les fonctionnalités 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 reflète le niveau de protection de l'appareil.

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 tient compte de facteurs tels que les applications de protection installées, l'utilisation des clés, ainsi que le nombre et les types de 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. Vous ne pouvez utiliser l'application que si vous disposez d'un fichier clé.

FileTransferBridge

Un composant interne de Kaspersky Security Center Linux qui assure la distribution locale des mises à jour des applications Kaspersky. FileTransferBridge est intégré à l'Agent d'administration (klnagent) et s'exécute localement sur chaque appareil administré.

Lorsque les applications Kaspersky reçoivent des mises à jour de Kaspersky Security Center Linux, l'Agent d'administration télécharge les fichiers de mise à jour depuis le Serveur d'administration ou un point de distribution. FileTransferBridge transfère ensuite les fichiers localement aux applications Kaspersky installées, assurant une distribution fiable des mises à jour des bases de données et des correctifs logiciels.

FileTransferBridge utilise les ports TCP 30522 et 30523. Les ports sont à l'écoute uniquement sur l'interface localhost (127.0.0.1) et n'acceptent pas les connexions entrantes provenant de réseaux externes.

Gestion directe des applications

Gestion des applications par l'interface locale.

Gestionnaire des identités et des accès (IAM)

Composant du Serveur d'administration qui vous permet d'utiliser l'authentification de domaine (authentification unique). La fonctionnalité d'authentification unique permet à un utilisateur d'activer l'authentification sécurisée dans Kaspersky Security Center Web Console sans avoir à saisir à nouveau le mot de passe sur le réseau d'entreprise.

Gravité de l'événement

Caractéristique de l'événement consigné dans le fonctionnement de l'application de Kaspersky. Il existe quatre niveaux de gravité :

- 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.

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.

Installation à distance

Installation des applications de Kaspersky à l'aide des outils offerts par l'application Kaspersky Security Center Linux.

Installation locale

Installation d'une application de protection sur un appareil du réseau de l'entreprise qui implique le lancement manuel de l'installation à partir du paquet de distribution de l'application de protection ou l'exécution manuelle d'un paquet d'installation publié préalablement téléchargé sur l'appareil.

Installation manuelle

Installation d'une application de protection sur un appareil du réseau de l'organisation à partir d'un 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 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 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.

Mises à jour

Procédure de remplacement ou d'ajout de nouveaux fichiers (bases ou modules logiciels) récupérés sur les serveurs de mise à jour de Kaspersky.

Nagent léger (LWNGT)

Protocole d'interaction avec Kaspersky Endpoint Security sur les appareils mobiles. Le LWNGT (également appelé protocole mobile) fonctionne comme un Agent d'administration sans installer d'Agent d'administration sur les appareils mobiles.

Niveau d'importance du correctif

Attribut du correctif. Il existe cinq niveaux d'importance pour les correctifs de Microsoft et les correctifs d'éditeurs tiers :

- Critique
- Élevé.
- Normal.
- Faible.
- Inconnu.

Le niveau d'importance du correctif d'un éditeur étranger ou de Microsoft est défini par le niveau de gravité le plus défavorable de la vulnérabilité corrigé par le correctif.

Paquet d'installation

L'ensemble de fichiers pour l'installation à distance de l'application Kaspersky à l'aide du système d'administration à distance Kaspersky Security Center. Le paquet d'installation contient un ensemble de paramètres nécessaires pour installer une application et assurer son efficacité immédiatement après l'installation. Les valeurs des paramètres correspondent aux valeurs des paramètres de l'application par défaut. Le paquet d'installation est créé sur la base de fichiers aux extensions .kpd et .kud inclus dans la distribution de l'application.

Paramètres de l'application

Paramètres des applications, communs à tous les types de tâches et servant au fonctionnement de l'application dans son ensemble, par exemple : paramètres de performances de l'application, paramètres de gestion des rapports, paramètres de la Sauvegarde.

Paramètres de la tâche

Paramètres de l'application propres à 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.

Poste de travail de l'administrateur

L'appareil sur lequel la Console d'administration est installée fait office de composant fournissant l'interface d'administration de Kaspersky Security Center Linux.

Depuis le poste de travail de l'administrateur, l'administrateur gère la partie serveur de Kaspersky Security Center en créant et en contrôlant le système de protection centralisée du réseau de l'organisation fondé sur les applications 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.

Propagation de virus

Tentatives multiples d'infection d'un appareil par un virus.

Propriétaire de l'appareil

Le propriétaire de l'appareil est un utilisateur que l'administrateur peut contacter lorsqu'il faut exécuter certaines opérations sur un appareil.

Protection antivirus du réseau

L'ensemble de mesures techniques et d'organisation qui diminuent la possibilité d'intrusion des virus et du spam sur les appareils de réseau de l'entreprise et qui empêchent les attaques de réseau, le phishing et les autres menaces. La protection antivirus du réseau est renforcée lorsque vous utilisez des applications et des services de sécurité, et que vous appliquez et respectez la stratégie de sécurité des données de l'entreprise.

Reconnaissance de l'emplacement réseau (NLA)

Service Windows qui aide le système d'exploitation à identifier le réseau actuel. La reconnaissance de l'emplacement réseau effectue la détection des modifications apportées au réseau et ajuste la configuration de sécurité de l'appareil.

Restauration

Le déplacement d'un objet original depuis le dossier de quarantaine ou de sauvegarde vers l'emplacement où il était avant sa mise en quarantaine, sa désinfection ou sa suppression ou vers un dossier spécifié par l'utilisateur.

Restauration des données du Serveur d'administration

Il s'agit de la restauration des données du Serveur d'administration à l'aide d'un utilitaire de sauvegarde sur la base des informations présentes dans le dossier de sauvegarde. L'utilitaire permet de restaurer :

- La base de connaissances 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)
- Le certificat du Serveur d'administration.

Serveur d'administration

Module de Kaspersky Security Center qui centralise les informations sur toutes les applications Kaspersky installées sur le réseau de l'entreprise et en assure le contrôle.

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 MDM iOS

Module Kaspersky Security Center installé sur l'appareil client et qui permet de connecter les appareils mobiles iOS au Serveur d'administration et de les administrer à l'aide du service Apple Push Notifications (APNs).

Serveur Web de Kaspersky Security Center Linux

Un module de Kaspersky Security Center Linux qui s'installe avec le Serveur d'administration. Le Serveur Web est conçu pour transférer via le 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 un nombre illimité de stratégies pour les applications installées sur les appareils de 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 seul appareil client.

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. L'administrateur peut utiliser un compte utilisateur interne pour lancer Kaspersky Security Center Web Console et consulter les informations sur l'état de la sécurité antivirus du réseau. Dans Kaspersky Security Center Linux, les utilisateurs internes disposent des droits 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.

Vulnérabilité

Un défaut au sein d'un système d'exploitation ou d'une application qui pourrait être exploité par des pirates informatiques afin de s'introduire dans le système d'exploitation ou l'application et d'en compromettre l'intégrité. Un système d'exploitation qui présente un gros volume de vulnérabilités n'est plus fiable, car les applications malveillantes qui y pénètrent peuvent provoquer des dysfonctionnements du système d'exploitation lui-même et des applications installées.

Zone démilitarisée (DMZ)

La zone démilitarisée est un segment du réseau local où se trouvent les serveurs qui répondent aux requêtes Internet. Afin de garantir la sécurité du réseau local, l'accès à celui-ci depuis la zone démilitarisée est limité et protégé par un pare-feu.

Informations sur le code tiers

Les informations sur le code tiers sont reprises dans le fichier legal_notices.txt situé dans le répertoire d'installation de l'application.

Avis de marques déposées

Les autres noms et marques déposés appartiennent à leurs propriétaires respectifs.

Adobe, Acrobat, Flash, PostScript et Shockwave 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 une marque déposée ou une marque d'Apache Software Foundation aux États-Unis et/ou dans d'autres pays.

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 et 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 aux États-Unis et dans certains autres 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.

La marque 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.

OpenVPN est une marque commerciale d'OpenVPN, Inc.

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.

La marque BlackBerry appartient à Research In Motion Limited et est déposée aux États-Unis ; elle peut être en cours de dépôt ou déjà déposée dans d'autres pays.

Rocky Linux est une marque déposée de The Rocky Enterprise Software Foundation.

Samsung est une marque de SAMSUNG aux Etats-Unis ou dans d'autres pays.

Debian une marque déposée de Software in the Public Interest, Inc.

Splunk, SPL sont des marques commerciales et des marques commerciales déposées de Splunk Inc. aux États-Unis et dans d'autres pays.

SUSE est une marque déposée de SUSE LLC aux États-Unis et dans d'autres pays.

La marque de commerce Symbian appartient à la Symbian Foundation Ltd.

OpenAPI est la marque de commerce de The Linux Foundation.

UNIX est une marque commerciale déposée aux États-Unis et dans d'autres pays, sous licence exclusive via X/Open Company Limited.

Zabbix est une marque déposée de Zabbix SIA.