kaspersky

Kaspersky Security Center Cloud Console

© 2025 AO Kaspersky Lab

Contenu

Aide de Kaspersky Security Center Cloud Console
Nouveautés
Kaspersky Security Center Cloud Console
- À propos de Kaspersky Security Center Cloud Console
- Configurations matérielle et logicielle requises pour Kaspersky Security Center Cloud Console
- Compatible avec les applications et les solutions de Kaspersky
- Localisation de Kaspersky Security Center Cloud Console
- Comparaison de Kaspersky Security Center et de Kaspersky Security Center Cloud Console

Architecture et concepts de base
- Architecture
- Ports utilisés par Kaspersky Security Center Cloud Console
- Notions principales
  - Agent d'administration
  - Groupes d'administration
  - Hiérarchie des Serveurs d'administration
  - Serveur d'administration virtuel
  - Point de distribution
  - Plug-in Web d'administration
  - Stratégies
  - Profils de stratégie
  - Corrélation de la stratégie et des paramètres locaux de l'application

Licence de l'application
- Licence de Kaspersky Security Center Cloud Console
- À propos du mode d'évaluation de Kaspersky Security Center Cloud Console
- Utilisation de la place de marché de Kaspersky pour choisir les solutions d'entreprise de Kaspersky
- Licences et nombre minimum d'appareils pour chaque licence
- Événements de dépassement de la restriction de licence
- Méthodes de distribution des codes d'activation aux appareils administrés
- Ajout de la clé de licence du Serveur d'administration
- Ajout de la clé de licence dans le stockage du Serveur d'administration
- Déploiement d'une clé de licence sur les appareils clients
- Diffusion automatique de la clé de licence
- Affichage des informations sur les clés de licence utilisées dans le stockage du Serveur d'administration
- Affichage des informations sur les clés de licence utilisées pour une application Kaspersky particulière
- Suppression de la clé de licence du Serveur d'administration
- Suppression d'une clé de licence du stockage
- Affichage de la liste des appareils sur lesquels aucune application Kaspersky n'est activée
- Révocation d'un Contrat de licence utilisateur final
- Renouvellement des licences des applications Kaspersky
- Utilisation de Kaspersky Security Center Cloud Console après expiration de la licence
- Définitions des licences
  - À propos de la licence
  - À propos du certificat de licence
  - À propos de la clé de licence
  - À propos du code d'activation
  - À propos de l'abonnement

À propos des données
Données envoyées aux serveurs Kaspersky
Données nécessaires au fonctionnement de l'espace de travail
Données nécessaires au fonctionnement des applications administrées
Données de l'utilisateur traitées localement
À propos des documents juridiques de Kaspersky Security Center Cloud Console
Guide de renforcement
Planification de l'architecture Kaspersky Security Center Cloud Console
Comptes et authentification
Gestion de la protection des appareils clients
Configuration de la protection des applications administrées
Transfert d'événements vers des systèmes tiers
Interface de Kaspersky Security Center Cloud Console
Modification de la langue de l'interface de Kaspersky Security Center Cloud Console
Modification de la page d'accueil de Kaspersky Security Center Cloud Console
Ajout et suppression de signets
Configuration initiale de Kaspersky Security Center Cloud Console
Gestion de l'espace de travail
À propos de l'administration de l'espace de travail dans Kaspersky Security Center Cloud Console
Prise en main de Kaspersky Security Center Cloud Console
Création d'un compte
Enregistrement d'une entreprise et création d'un espace de travail
Protection de plus de 10 000 appareils
Ouverture de l'espace de travail de Kaspersky Security Center Cloud Console
Retour à la liste des espaces de travail
Déconnexion de Kaspersky Security Center Cloud Console
Gestion de l'entreprise et la liste des espaces de travail
Modification d'informations sur une entreprise et un espace de travail
Suppression d'un espace de travail et d'une entreprise
Annulation de la suppression de l'espace de travail
Gestion de l'accès à l'entreprise et à ses espaces de travail
Octroi de l'accès à votre entreprise et à ses espaces de travail
Révocation de l'accès à votre entreprise et à ses espaces de travail
Réinitialisation de votre mot de passe
Modification des paramètres du compte sur Kaspersky Security Center Cloud Console
Modification d'une adresse email
Modification d'un mot de passe
Utilisation de la vérification en deux étapes
À propos de la vérification en deux étapes
Scénario : Configuration de la vérification en deux étapes
Configuration de la vérification en deux étapes par SMS
Configuration de la vérification en deux étapes à l'aide d'une application d'authentification
Modification de votre numéro de téléphone mobile
Désactivation de la vérification en deux étapes
Suppression d'un compte sur Kaspersky Security Center Cloud Console
A propos du choix des centres de données pour la conservation des informations de Kaspersky Security Center Cloud Console
Accès aux serveurs DNS publics

Scénario : création d'une hiérarchie de Serveurs d'administration administrés par Kaspersky Security Center Cloud Console
Migration vers Kaspersky Security Center Cloud Console
À propos de la migration depuis Kaspersky Security Center Web Console
Méthodes de migration vers Kaspersky Security Center Cloud Console
Scénario : migration sans hiérarchie de Serveurs d'administration
Assistant de migration
Étape 1. Exportation d'appareils administrés, d'objets et de paramètres à partir de Kaspersky Security Center Web Console
Étape 2. Importation du fichier d'exportation Kaspersky Security Center Cloud Console
Étape 3. Réinstallez l'Agent d'administration sur les appareils administrés par Kaspersky Security Center Cloud Console
Migration avec une hiérarchie de Serveurs d'administration
Scénario : migration d'appareils exécutant des systèmes d'exploitation Linux ou macOS
Scénario : migration inverse de Kaspersky Security Center Cloud Console vers Kaspersky Security Center
Migration avec des Serveurs d'administration virtuels
Scénario : migration avec des Serveurs d'administration virtuels en déplaçant des appareils
Scénario : migration manuelle avec des Serveurs d'administration virtuels
Scénario : déplacement d'appareils à partir de groupes d'administration sous la gestion de Serveurs virtuels
À propos de la migration depuis Kaspersky Endpoint Security Cloud
Assistant de démarrage rapide de l'application
À propos de l'assistant de démarrage rapide de l'application
Lancement de l'assistant de démarrage rapide de l'application
Étape 1. Sélection des paquets d'installation à télécharger
Étape 2. Configuration des paramètres du serveur proxy
Étape 3. Configuration de Kaspersky Security Network
Étape 4. Configuration des paramètres d'administration des mises à jour tierces
Étape 5. Création de la configuration de base de la protection d'un réseau
Étape 6. Fin de l'assistant de démarrage rapide de l'application
Déploiement initial des applications Kaspersky
Scénario : Déploiement initial des applications Kaspersky
Création de paquets d'installation pour les applications Kaspersky
Propagation des paquets d'installation sur les Serveurs d'administration secondaires
Création des paquets d'installation autonome pour l'Agent d'administration
Affichage de la liste des paquets d'installation autonomes
Génération des paquets d'installation personnalisés
Exigences d'un point de distribution
Paramètres du paquet d'installation de l'Agent d'administration
Infrastructure virtuelle
Recommandations sur la réduction de la charge sur les machines virtuelles
Prise en charge des machines virtuelles dynamiques
Prise en charge de la copie des machines virtuelles
Utilisation de l'Agent d'administration pour Windows, Linux et macOS : comparaison
Spécification des paramètres pour l'installation à distance sur les appareils Unix
Remplacement d'application de sécurité d'éditeurs tiers
Possibilités d'installation manuelle des applications
Déploiement forcé à l'aide d'une tâche d'installation à distance des applications de Kaspersky Security Center Cloud Console
Assistant de déploiement de la protection
Étape 1. Démarrage de l'assistant de déploiement de la protection
Étape 1. Sélection du paquet d'installation

Étape 2. Sélection de la version de l'Agent d'administration
Étape 3. Sélection des appareils
Étape 4. Indiquez les paramètres de la tâche d'installation à distance
Étape 5. Administration du redémarrage
Étape 6. Suppression des applications incompatibles avant l'installation
Étape 7. Déplacement des appareils vers Appareils administrés
Étape 8. Sélection des comptes pour accéder aux appareils
Étape 9. Démarrage de l'installation
Paramètres réseau pour l'interaction avec des services externes
Préparation d'un appareil exécutant Astra Linux dans l'environnement logiciel fermé mode pour l'installation de l'Agent d'administration
Préparation d'un appareil Linux et installation de l'Agent d'administration sur un appareil Linux à distance
Installation des applications à l'aide de la tâche d'installation à distance
Installation d'une application à distance
Installation des applications sur les Serveurs d'administration secondaires
Lancement et arrêt des applications Kaspersky.
Administration des appareils mobiles
Capacités de Detection and Response
À propos des capacités de Detection and Response
Modifications d'interface après intégration des fonctionnalités de Detection and Response
Découverte des appareils en réseau et création de groupes d'administration
Scénario de recherche d'appareils en réseau
Sondage réseau
Sondage du réseau Windows
Sondage du contrôleur de domaine
Sondage des plages IP
Configuration d'un contrôleur de domaine Samba
Ajout et modification d'une plage IP
Réglage des points de distribution et des passerelles de connexion
Calcul de la quantité et de la configuration des points de distribution
Configuration typique des points de distribution : un bureau simple
Configuration typique des points de distribution : plusieurs petits bureaux isolés
Assignation manuelle des points de distribution
Modifier la liste des points de distribution pour un groupe d'administration
Utilisation d'un point de distribution en tant que serveur push
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
Création des groupes d'administration
Création des règles de déplacement des appareils
Copie des règles de déplacement des appareils
Conditions d'une règle de déplacement de l'appareil
Ajout manuel d'appareils à un groupe d'administration
Déplacement manuel des appareils ou des clusters à un groupe d'administration
Configuration des règles de rétention pour les appareils non définis
Configuration de la protection réseau
Scénario : Configuration de la protection réseau
À propos des méthodes d'administration de la sécurité centrées sur l'appareil et l'utilisateur
Configuration et diffusion des stratégies : approche centrée sur l'appareil
Configuration et diffusion des stratégies : approche centrée sur l'utilisateur

Paramètres de la stratégie de l'Agent d'administration
Comparaison des paramètres de stratégie de l'Agent d'administration par système d'exploitation
Configuration manuelle d'une stratégie de Kaspersky Endpoint Security
Configuration de Kaspersky Security Network
Consultation de la liste des réseaux protégés par le Pare-feu
Exclusion des détails du logiciel de la mémoire du Serveur d'administration
Configuration de l'enregistrement d'événements de stratégie importants dans la base de données du Serveur d'administration
Configuration manuelle d'une tâche de groupe de mise à jour de Kaspersky Endpoint Security
Tâches
À propos des tâches
À propos de la zone d'action des tâches
Création d'une tâche
Affichage de la liste des tâches
Lancer une tâche manuellement
Lancement d'une tâche pour les appareils sélectionnés
Paramètres et propriétés de la tâche générale
Exportation d'une tâche
Importation d'une tâche
Affichage de l'historique des tâches entreposé sur le Serveur d'administration
Administration des appareils clients
Paramètres de l'appareil administré
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
Consultation et configuration des actions quand les appareils sont inactifs
À propos des états des appareils
Configuration de la permutation des états des appareils
Modification du Serveur d'administration pour les appareils clients
Évitement des conflits entre plusieurs Serveurs d'administration
Création de profils de connexion au Serveur d'administration
À propos des clusters et des groupes des serveurs
Propriétés d'un cluster ou d'un groupe de serveurs
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
Marquage manuel des appareils
Suppression de tags attribués des appareils
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
Quarantaine et sauvegarde
Téléchargement d'un fichier à partir de stockages
Suppression des fichiers depuis les stockages
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
Exécution du diagnostic à distance d'une application et téléchargement des résultats
Exécution d'une application sur un appareil client
Génération d'un fichier dump pour une application
Connexion à distance au bureau de l'appareil client
Connexion aux appareils à l'aide du Partage du bureau Windows
Déclenchement des règles en mode Apprentissage intelligent
Consultation de la liste des détections réalisées à l'aide des règles du contrôle évolutif des anomalies
Ajout d'exclusions au départ des règles du contrôle évolutif des anomalies
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
Stratégies et profils de stratégie
À propos des stratégies
À propos du cadenas et des paramètres verrouillés
Héritage des stratégies, utilisation des profils des stratégies
Hiérarchie des stratégies
Profils de stratégie dans une hiérarchie de stratégies
Comment les paramètres sont mis en œuvre sur un appareil administré
Administration des stratégies
Affichage de la liste des stratégies
Création d'une stratégie
Modification d'une stratégie
Paramètres généraux de la stratégie
Activation et désactivation d'une option d'héritage de stratégie
Copie d'une stratégie
Déplacement d'une stratégie
Exportation d'une stratégie
Importation d'une stratégie
Affichage du graphique de l'état de la distribution des stratégies
Activation automatique d'une stratégie lors d'un événement " Propagation de virus "
Synchronisation forcée
Suppression d'une stratégie
Administration des profils de stratégies

Consultation des profils d'une stratégie
Modification de la priorité d'un profil de stratégie
Création d'un profil de stratégie
Modification du profil de stratégie
Copie d'un profil de stratégie
Création d'une règle d'activation du profil de stratégie
Suppression d'un profil de stratégie
Chiffrement et protection des données
Consultation de la liste des disques chiffrés
Formation et consultation des rapports sur le chiffrement
Accorder l'accès à un disque chiffré en mode déconnecté
Utilisateurs et rôles d'utilisateurs
À propos des comptes utilisateurs
Ajout d'un compte d'un utilisateur interne
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
Attribution d'un rôle à un utilisateur ou à un groupe de sécurité
Création d'un rôle d'utilisateur
Modification d'un rôle d'utilisateur
Modification de la zone d'action d'un rôle d'utilisateur
Suppression d'un rôle d'utilisateur
Association des profils des stratégies aux rôles
Création d'un groupe de sécurité
Modification d'un groupe de sécurité
Ajout de comptes utilisateurs à un groupe interne
Suppression d'un groupe de sécurité
Configuration de l'intégration ADFS
Configuration de l'intégration avec Microsoft Entra ID
Activation du sondage Microsoft Entra ID
Ajout de Kaspersky Security Center Cloud Console à la liste des applications
Désignation d'un utilisateur en tant que propriétaire de l'appareil
Désignation d'un utilisateur en tant que propriétaire de l'appareil Linux après l'installation de l'Agent d'administration
Utilisation des révisions des objets
Restauration des modifications
Ajout d'une description de la révision
Affichage et enregistrement d'une révision de la stratégie
Kaspersky Security Network (KSN)
À propos de KSN
Activation et désactivation 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
Suppression d'objets
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
Création de la tâche de téléchargement des mises à jour dans les stockages des points de distribution
Configuration des appareils administrés pour recevoir les mises à jour uniquement à partir de points de distribution
Activation et désactivation de l'installation automatique des mises à jour et des correctifs pour les composants de Kaspersky Security Center Cloud Console
Installation automatique des mises à jour pour Kaspersky Endpoint Security for Windows
À propos des statuts de mise à jour
Approbation et refus des mises à jour du logiciel
Utilisation de fichiers diff pour la mise à jour des bases de données et des modules logiciels Kaspersky
Mise à jour des bases de données et des modules logiciels de Kaspersky sur des appareils déconnectés
Mise à jour des bases de données de Kaspersky Security for Windows Server
Gestion des applications tierces sur les appareils client
Limitations de la fonctionnalité Gestion des vulnérabilités et des correctifs
Disponibilité des fonctionnalités de la gestion des vulnérabilités et des correctifs en mode d'essai et commercial et sous diverses options de licence
À propos des applications tierces
Mises à jour du logiciel tiers
Scénario : mise à jour des logiciels tiers
Installation des mises à jour du logiciel tiers
Création de la tâche Recherche de vulnérabilités et des mises à jour requises
La tâche Recherche de vulnérabilités et de mises à jour requises est créée
Création de la tâche Installer les mises à jour requises et corriger les vulnérabilités
Ajout de règles pour l'installation de la mise à jour
Création de la tâche Installation des mises à jour Windows Update
Consultation des informations sur les mises à jour du logiciel tiers disponibles
Exportation de la liste des mises à jour du logiciel disponibles vers un fichier
Approuver et refuser les mises à jour du logiciel tiers
Mise à jour automatique des applications tierces
Recherche et correction des vulnérabilités dans les applications
Correction des vulnérabilités dans les applications
Création de la tâche Correction des vulnérabilités
Création de la tâche Installer les mises à jour requises et corriger les vulnérabilités
Ajout de règles pour l'installation de la mise à jour
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
Scénario : rechercher et corriger les vulnérabilités dans les applications
Définition de la durée maximale de stockage des informations sur les vulnérabilités corrigées
Gestion des applications exécutées sur les appareils client
Utilisation du Contrôle des applications pour gérer les fichiers exécutables
Modes et catégories du Contrôle des applications
Obtention et consultation d'une liste des applications installées sur les appareils client
Obtention et consultation d'une liste des fichiers exécutables installés 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
Affichage de la liste des catégories d'applications

Configuration du Contrôle des applications dans la stratégie Kaspersky Endpoint Security for Windows
Ajout de fichiers exécutables liés par un événement à la catégorie d'applications
Création d'un paquet d'installation d'une application tierce à partir de la base de données Kaspersky
Affichage et modification des paramètres d'un paquet d'installation d'une application tierce à partir de la base de données de Kaspersky
Paramètres d'un paquet d'installation d'une application tierce à partir de la base de données de Kaspersky
Tags de l'application
Création d'un tag de l'application
Renommage d'un tag de l'application
Attribution de tags à une application
Suppression de tags attribués à un appareil
Suppression d'un tag de l'application
Configuration du Serveur d'administration
Création d'une hiérarchie des Serveurs d'administration : ajout d'un Serveur d'administration secondaire
Configuration de la durée de stockage des événements concernant les appareils supprimés
Agrégation de courriels sur les événements
Limitations de l'administration des Serveurs d'administration secondaires fonctionnant sur site via Kaspersky Security Center Cloud Console
Affichage de la liste des Serveurs d'administration secondaires
Suppression d'une hiérarchie des Serveurs d'administration
Configuration de l'interface
Administration des Serveurs d'administration virtuels
Création d'un Serveur d'administration virtuel
Activation et désactivation d'un Serveur d'administration virtuel
Désignation d'un administrateur pour un Serveur d'administration virtuel
Suppression d'un Serveur d'administration virtuel
Surveillance et rapports
Scénario : Surveillance et rapports
À propos des types de surveillance et de rapport
Tableau de bord et widgets
À propos du tableau de bord
Ajout de widgets au tableau de bord
Dissimulation d'un widget dans le tableau de bord
Déplacement d'un widget sur le tableau de bord
Modification de la taille et de l'apparence du widget
Modification des réglages d'un widget
À propos le mode Tableau de bord uniquement
Configuration du mode Tableau de bord uniquement
Rapports
Utilisation des rapports
Créer le nouveau rapport
Consultation et modification des propriétés du modèle de rapport
Exportation d'un rapport dans un fichier
Génération et affichage d'un rapport
Création d'une tâche d'envoi du rapport
Suppression des modèles de rapport
Événements et sélections d'événements
À propos des événements dans Kaspersky Security Center Cloud Console
Événements des modules de Kaspersky Security Center Cloud Console

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 détails d'un événement
Exportation des événements dans un fichier
Voir un historique d'objet à partir d'un événement
Enregistrement des événements sur les tâches et les stratégies
Supprimer des événements
Suppression de sélections d'événements
Notifications et états de l'appareil
Présentation des notifications
Configuration de la permutation des états des appareils
Configuration des paramètres d'envoi des notifications
Annonces de Kaspersky
À propos des annonces de Kaspersky
Désactivation des annonces de Kaspersky
Réception d'un avertissement d'expiration de licence
Cloud Discovery
Activation de Cloud Discovery à l'aide du widget
Ajout du widget Cloud Discovery au tableau de bord
Affichage des informations sur l'utilisation des services cloud
Niveau de risque d'un service cloud
Bloquer l'accès aux services cloud indésirables
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
Exécution du diagnostic à distance d'une application et téléchargement des résultats
Exécution d'une application sur un appareil client
Génération d'un fichier dump pour une application

Exécution de diagnostics à distance sur un appareil client basé sur Linux
Exportation des événements dans les systèmes SIEM
Configuration de l'export d'événements vers des systèmes SIEM
Conditions préalables
À propos de l'exportation des événements
Configuration de l'export d'événements dans le système SIEM
Marquage des événements pour l'export vers les systèmes SIEM au format Syslog
Marquage des événements d'une application Kaspersky pour l'exportation au format Syslog
Marquage d'événements généraux pour l'exportation au format Syslog
À propos de l'exportation des événements via le format Syslog
Configuration de Kaspersky Security Center Cloud Console pour l'exportation des événements vers le système SIEM
Consultation des résultats de l'exportation
Guide de démarrage rapide pour les fournisseurs de services gérés (MSP)
À propos de Kaspersky Security Center Cloud Console
Fonctionnalités principales de Kaspersky Security Center Cloud Console
À propos des licences de Kaspersky Security Center Cloud Console pour MSP
À propos des capacités de Detection and Response pour MSPs
Prise en main de Kaspersky Security Center Cloud Console
Recommandations pour la gestion des appareils de vos clients
Schéma de déploiement typique pour les MSP
Scénario : déploiement de la protection (gestion des locataires via des serveurs d'administration virtuels)
Scénario : déploiement de la protection (gestion des locataires via des groupes d'administration)
Utilisation conjointe de Kaspersky Security Center fonctionnant sur site et de Kaspersky Security Center Cloud Console
Licences des applications Kaspersky pour les MSP
Capacités de surveillance et de reporting pour les MSP
Utilisation de Kaspersky Security Center Cloud Console dans l'environnement cloud
Options de licence pour l'environnement cloud
Préparation au travail dans l'environnement cloud via Kaspersky Security Center Cloud Console
Utilisation de l'environnement cloud Amazon Web Services
À propos de l'utilisation de l'environnement cloud d'Amazon Web Services
Création de comptes utilisateurs IAM pour les instances d'Amazon EC2
Garantie des privilèges pour le fonctionnement de Kaspersky Security Center Cloud Console avec AWS
Création d'un compte utilisateur IAM pour utiliser la Kaspersky Security Center Cloud Console
Manipulation dans l'environnement cloud Microsoft Azure
À propos de l'utilisation de Microsoft Azure
Création d'un abonnement, d'un identifiant de l'application et d'un mot de passe
Attribution d'un rôle à un identifiant de l'application Azure
Travailler dans Google Cloud
Assistant de configuration pour une utilisation dans le Cloud dans Kaspersky Security Center Cloud Console
Étape 1. Vérification des plug-ins et des paquets d'installation requis
Étape 2. Sélection de la méthode d'activation de l'application
Étape 3. Sélection de l'environnement cloud et de l'autorisation
Étape 4. Sondage par segment et configuration de la synchronisation avec le Cloud
Étape 5. Sélection de l'application pour laquelle créer une stratégie et des tâches
Étape 6. Configuration de Kaspersky Security Network pour Kaspersky Security Center Cloud Console
Étape 7. Création d'une configuration initiale de protection
Sondage de segments du réseau via Kaspersky Security Center Cloud Console
Ajout de connexions pour le sondage des segments dans le Cloud via Kaspersky Security Center Cloud Console

Suppression d'une connexion pour le sondage des segments dans le Cloud
Configuration de la programmation du sondage via Kaspersky Security Center Cloud Console
Affichage des résultats du sondage des segments dans le Cloud via Kaspersky Security Center Cloud Console
Affichage des propriétés des appareils du Cloud via Kaspersky Security Center Cloud Console
Synchronisation avec le Cloud : Configuration de la règle de déplacement
Installation à distance d'applications sur les machines virtuelles Azure
Contacter le Support Technique
Façons de profiter du support technique
Support technique via le Kaspersky CompanyAccount
Informations requises pour les spécialistes du Support Technique de Kaspersky
Sources d'informations sur l'application
Problèmes connus
Glossaire
Administrateur de Kaspersky Security Center Cloud Console
Agent d'administration
Agent d'authentification
Appareil administré
Appareil protégé au niveau UEFI
Application incompatible
AWS Application Program Interface (AWS API)
Base antivirus
Clé active
Clé d'accès AWS IAM
Clé de licence complémentaire (ou de réserve)
Cloud Discovery
Compte utilisateur sur Kaspersky Security Center Cloud Console
Console de gestion AWS
Domaine multidiffusion
Durée de validité de la licence
Espace de travail
État de la protection
État de la protection du réseau
Fichier clé
Gestion centralisée des applications
Gestion des identités et des accès (IAM)
Gestion directe des applications
Gravité de l'événement
Groupe d'administration
HTTPS
Image machine Amazon (AMI)
Installation à distance
Installation forcée
Installation locale
Instance d'Amazon EC2
JavaScript
Kaspersky Next Expert View
Kaspersky Private Security Network (KPSN)
Kaspersky Security Network (KSN)

Lightweight Nagent (LWNGT)
Mise à jour
Mise à jour disponible
Network Location Awareness (NLA)
Niveau d'importance du correctif
Opérateur de Kaspersky Security Center Cloud Console
Paquet d'installation
Paramètres de l'application
Paramètres de la tâche
Passerelle des connexions
Plug-in Web d'administration
Point de distribution
Profil de la stratégie
Propagation de virus
Propriétaire de l'appareil
Protection antivirus du réseau
Quarantaine
Restauration
Rôle IAM
Serveur d'administration
Serveur d'administration domestique
Serveur d'administration virtuel
Serveurs de mise à jour de Kaspersky
Seuil d'activité de virus
SSL
Stockage d'événements
Stratégie
Tâche
Tâche de groupe
Tâche locale
Tâches pour l'ensemble d'appareils
Tag de l'appareil
Tag de l'application
Utilisateur IAM
Vulnérabilité
Zone démilitarisée (DMZ)
Informations sur le code tiers
Avis de marques déposées

Aide de Kaspersky Security Center Cloud Console

	Nouveautés Découvrez les nouveautés de la version la plus récente d'application.		**Configuration de la protection réseau** Gérez la sécurité d'une organisation en configurant les stratégies et les tâches de l'application Kaspersky conformément aux exigences de l'organisation.
	Configurations logicielle et matérielle Découvrez quels sont les systèmes d'exploitation et les versions de l'application prises en charge.		**Applications Kaspersky : mise à jour régulière des bases de données et des modules logiciels** Maintenir la fiabilité du système de protection.
	Licence de Kaspersky Security Center Cloud Console À propos de Kaspersky Security Center Cloud Console en mode d'essai et en mode commercial.		**Surveillance et rapports** Affichez votre infrastructure, les états de la protection des appareils en réseau et les statistiques pour administrer l'état de la protection actuel de votre organisation. Vous pouvez également utiliser des rapports.
	Configuration initiale Commencez à travailler avec votre espace de travail, configurez Kaspersky Security Center Cloud Console en fonction de vos besoins.		**Gestion des vulnérabilités et des correctifs** Recherchez et corrigez les vulnérabilités dans les logiciels tiers.
	Migration vers Kaspersky Security Center Cloud Console Migrez vos groupes d'administration existants et les objets associés de Kaspersky Security Center sur site vers Kaspersky Security Center Cloud Console.		**Exportation des événements dans les systèmes SIEM** Configurez l'exportation des événements dans les systèmes SIEM Via le protocole Syslog.
	Recherche d'appareils en réseau Découvrez les appareils nouveaux et existants sur le réseau de votre organisation.		**Fonctionnement dans un environnement cloud** Protégez les machines virtuelles dans l'environnement cloud : Amazon Web Services™, Microsoft Azure™, Google™ Cloud Platform.
	Réglage des points de distribution et/ou des passerelles de connexion Configurer les points de distribution.		**Guide de démarrage rapide pour les prestataires de services gérés (MSP)** Découvrez comment utiliser Kaspersky Security Center Cloud Console si vous êtes administrateur de MSP.
	Applications Kaspersky : déploiement centralisé Déploiement d'applications Kaspersky.		

Nouveautés

Mise à jour avril 2025

Cette mise à jour de Kaspersky Security Center Cloud Console introduit les améliorations suivantes :

- Kaspersky Security Center Cloud Console prend désormais en charge les applications Kaspersky suivantes :
  - Kaspersky Embedded Systems Security 3.4 for Linux
  - Kaspersky Endpoint Security 12.2 for Linux
  - Kaspersky Endpoint Security 12.8 for Windows
- Téléchargez et exécutez une application (ou un script) pour les diagnostics sur un appareil administré. Vous pouvez maintenant télécharger soit le dossier 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.
- Les informations sur les utilisateurs actuellement connectés à l'appareil administré sont désormais affichées dans la section **Général** → **Sessions** de la fenêtre des propriétés de l'appareil.
- Nouvelles langues prises en charge : l'infrastructure Kaspersky Security Center Cloud Console est disponible en chinois simplifié.
- Améliorations de l'expérience utilisateur :
  - Les paquets d'installation disponibles sont affichés sur un seul onglet.
  - Vous pouvez modifier les paramètres de la page d'accueil via la nouvelle section **Liens rapides**. Par défaut, l'onglet **Paramètres de page d'accueil** de la section **Liens rapides** est définie comme page d'accueil.
  - La navigation dans les groupes d'administration est mise à jour : vous pouvez accéder au sous-groupe souhaité en cliquant sur le lien portant son nom dans le chemin d'accès au groupe d'administration.
  - La section **Épinglé** du menu principal s'appelle désormais **Signets**. Vous pouvez ajouter des sections de Kaspersky Security Center Cloud Console à vos signets pour y accéder rapidement.

Mise à jour de février 2025

Cette mise à jour de Kaspersky Security Center Cloud Console améliore les performances lors de l'ouverture et de la navigation dans Web Console.

Mise à jour, Octobre 2024

Cette mise à jour de Kaspersky Security Center Cloud Console introduit les améliorations suivantes :

- Nous avons amélioré l'intégration avec Microsoft Entra ID. Désormais, lorsqu'un utilisateur se déconnecte du compte Microsoft Entra ID utilisé pour l'authentification dans Kaspersky Security Center Cloud Console, la session se termine également pour Kaspersky Security Center Cloud Console et l'utilisateur est automatiquement déconnecté de la console.

- Vous pouvez désormais consulter et télécharger les révisions des stratégies. Kaspersky Security Center Cloud Console vous permet de consulter un rapport au format HTML ou d'enregistrer la révision dans un fichier JSON.
- Kaspersky Security Center Cloud Console affiche désormais le dernier état de la tâche connu du Serveur d'administration.
- Le **Rapport d'attaques réseau** inclut désormais l'adresse MAC et le port de la machine attaquante.
- Vous pouvez maintenant fermer le panneau de droite en cliquant n'importe où en dehors du panneau. Si vous apportez des modifications au panneau et que vous essayez ensuite de le fermer en cliquant à l'extérieur du panneau, une fenêtre de confirmation s'affiche.
- L'en-tête du tableau reste désormais épinglé en haut lorsque vous faites défiler le tableau.

Mise à jour septembre 2024

Cette mise à jour de Kaspersky Security Center Cloud Console introduit les améliorations suivantes :

- Kaspersky Endpoint Agent 4.0 est pris en charge.
- Un certain nombre d'anciennes versions de navigateurs ne sont plus prises en charge (Chrome avant la version 128, Edge avant la version 128, Firefox ESR avant la version 115, Safari avant la version 17.6).

Mise à jour avril 2024

Cette mise à jour de Kaspersky Security Center Cloud Console introduit les nouvelles fonctionnalités et améliorations suivantes :

- Une nouvelle fonctionnalité Cloud Discovery. Cette 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. La fonctionnalité Cloud Discovery suit les tentatives des utilisateurs d'accéder à ces services via les navigateurs et les applications de bureau.
- L'intégration avec Microsoft Entra ID pour permettre aux utilisateurs de votre organisation de se connecter à Kaspersky Security Center Cloud Console à l'aide des identifiants de leur compte Microsoft Entra ID. Attention, cette fonctionnalité n'est pas disponible dans la Fédération de Russie.
- Désormais, vous pouvez créer des profils de connexion pour connecter l'Agent d'administration au Serveur d'administration. Les profils de connexion permettent aux utilisateurs itinérants avec des ordinateurs portables de modifier le 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.
- Vous pouvez désormais ouvrir la liste de vos espaces de travail directement depuis le menu principal de l'application.
- Deux nouvelles langues de localisation ont été ajoutées : le chinois traditionnel et le chinois simplifié.
- Le paramètre de stockage des événements par défaut dans les paramètres de la tâche est passé de **Sauvegarder tous les événements** à **Sauvegarder uniquement le résultat de la tâche**. Cette option permet de réduire la quantité d'espace occupé dans la base de données de l'espace de travail. Cette modification ne concerne que les tâches créées pour Kaspersky Security Center. Ce paramètre reste inchangé dans les tâches des applications de sécurité Kaspersky.
- Kaspersky Security Center Cloud Console vous avertit également de la suppression prévue de votre espace de travail 7 et 30 jours après la suppression ou l'expiration de la dernière clé de licence de l'espace de travail. Vous

disposerez ainsi de plus de temps pour acheter une autre licence et ajouter sa clé de licence à l'espace de travail.

- Les infrastructures Kaspersky Business Hub et Kaspersky Security Center Cloud Console prennent désormais en charge les licences Kaspersky Next. Le logo de l'application change automatiquement, en fonction de la licence que vous utilisez.
- Kaspersky Security Center Cloud Console prend désormais en charge les applications Kaspersky suivantes :
  - Kaspersky Endpoint Security for Windows version 12.4
  - Kaspersky Endpoint Security 12.0 for Mac Correctif A
- Lorsque vous passez d'une application de sécurité de Kaspersky à une autre et que l'application actuelle est protégée par mot de passe, vous pouvez indiquer le mot de passe de désinstallation directement dans les propriétés de la tâche d'installation à distance.
- Vous pouvez désormais personnaliser le menu principal de l'application en épinglant ou en désépinglant vos sections de menu favorites. Les sections épinglées sont ajoutées à la zone **Épinglé** pour y faciliter l'accès.
- Interface de l'application et expérience utilisateur optimisées lorsque vous sélectionnez l'option **À la fin d'une autre tâche** lors de la planification d'une tâche.
- Le rapport sur le matériel peut désormais inclure des informations sur les appareils macOS.
- Désormais, vous pouvez sélectionner un ou plusieurs appareils clients dans la liste des appareils clients, puis lancer une tâche créée précédemment pour eux.

Mise à jour de février 2024

Cette mise à jour de Kaspersky Security Center Cloud Console introduit les nouvelles fonctionnalités et améliorations suivantes :

- Depuis la liste des appareils administrés, vous pouvez désormais sélectionner un ou plusieurs appareils, puis assigner une tâche existante à exécuter sur les appareils sélectionnés. La zone actuelle des appareils de la tâche sera remplacée par les appareils que vous avez sélectionnés.
- Vous pouvez désormais attribuer des tags à plusieurs appareils ou supprimer des tags d'appareil sur plusieurs appareils à la fois. Dans la liste des appareils administrés, sélectionnez les appareils, puis indiquez les tags que vous souhaitez attribuer ou supprimer des appareils sélectionnés.
- Apparence et expérience utilisateur optimisées pour la liste des appareils administrés. Ajout d'une nouvelle colonne **Tags** et de la possibilité de filtrer les appareils par tags d'appareil.

Mise à jour janvier 2024

Kaspersky Security Center Cloud Console prend désormais en charge Kaspersky Endpoint Security 12.4 for Windows.

Mise à jour, décembre 2023

Cette mise à jour de Kaspersky Security Center Cloud Console introduit les nouvelles fonctionnalités et améliorations suivantes :

- Vous pouvez maintenant vérifier la connexion à un système SIEM.
- Kaspersky Security Center Cloud Console prend désormais en charge le sondage d'un contrôleur de domaine Microsoft Active Directory et d'un contrôleur de domaine Samba via un point de distribution Linux.
- Diagnostics à distance des appareils administrés basés sur Linux.
- Kaspersky Security Center Cloud Console prend désormais en charge les applications Kaspersky suivantes :
  - Kaspersky Endpoint Security for Windows version 12.3 Correctif A
  - Kaspersky Endpoint Security 12.0 for Linux
  - Kaspersky Endpoint Security 12.0 for Mac
  - Kaspersky Endpoint Agent 3.16
  - Kaspersky Embedded Systems Security 3.3 for Windows
- Dans le menu principal, deux sections de l'interface étaient masquées, car elles étaient hors du champ de fonctionnalité de l'application :
  - Événements du chiffrement (**Opérations** → **Chiffrement et protection des données** → **Événements du chiffrement**)
  - Plages IP (**Découverte et déploiement** → **Découverte** → **Plages IP**)
- Nous avons mis à jour le texte du Contrat de traitement des données de Kaspersky Security Center Cloud Console.
- Un certain nombre d'anciennes versions du navigateur ne sont plus prises en charge (Firefox ESR antérieure à la version 102).

Mise à jour septembre 2023

Cette mise à jour de Kaspersky Security Center Cloud Console introduit les nouvelles fonctionnalités et améliorations suivantes :

- Kaspersky Security Center Cloud Console prend désormais en charge Kaspersky Embedded Systems Security 3.3 for Linux.
- Kaspersky Security Center Cloud Console prend désormais en charge Kaspersky Endpoint Security 12.2 for Windows.
- Optimisation de l'interface utilisateur lors de l'utilisation de la liste des utilisateurs dans la section **Ressources (Appareils)**.

Mise à jour juin 2023

Cette mise à jour de Kaspersky Security Center Cloud Console introduit les nouvelles fonctionnalités et améliorations suivantes :

- Un nouveau guide renforcement a été publié. Nous vous recommandons vivement de lire attentivement le guide et de suivre les recommandations de sécurité pour configurer Kaspersky Security Center Cloud Console et

votre infrastructure réseau.

- Kaspersky Security Center Cloud Console prend désormais en charge Kaspersky Endpoint Security 11.3 for Mac.
- Kaspersky Security Center Cloud Console prend désormais en charge Kaspersky Endpoint Security 11.4 for Linux.
- Vous pouvez utiliser Kaspersky Security Center Cloud Console pour exporter des sélections d'événements dans un fichier, puis importer les sélections d'événements dans Kaspersky Security Center Windows ou Kaspersky Security Center Linux.
- Vous pouvez désormais utiliser un point de distribution comme serveur push pour les appareils administrés par l'Agent d'administration. Cette fonction vous permet de vous garantir qu'une connectivité continue entre un appareil administré et le Serveur d'administration est établie.
- Réorganisation de la section avec des paramètres pour intégrer Kaspersky Security Center Cloud Console avec d'autres applications Kaspersky.
- Réorganisation de l'interface utilisateur de la section **Diagnostic à distance**.
- Vous pouvez désormais enregistrer des informations sur tous les appareils inclus dans une sélection d'appareils dans un fichier CSV.
- Un certain nombre d'améliorations dans l'interface utilisateur et la convivialité, y compris la possibilité de sélectionner tous les éléments dans un tableau.

Mise à jour, mars 2023

Cette mise à jour de Kaspersky Security Center Cloud Console introduit les nouvelles fonctionnalités et améliorations suivantes :

- Kaspersky Security Center Cloud Console prend désormais en charge les clusters et les baies de serveurs en tant qu'appareils administrés. Si une application Kaspersky est installée sur un nœud du cluster, l'Agent d'administration envoie ces informations au Serveur d'administration. Dans Web Console, les clusters et les baies de serveurs sont répertoriés séparément des autres appareils administrés. Vous administrez chaque cluster ou groupe de serveurs comme un objet individuel et indissociable.
- Kaspersky Security Center Cloud Console prend désormais en charge Kaspersky Endpoint Security 12.0 for Windows.
- Le nombre maximal d'entrées qu'un rapport peut inclure a été augmenté jusqu'à 2500 pour un rapport dans Web Console et jusqu'à 10 000 pour un rapport que vous exportez dans un fichier.
- Vous pouvez maintenant choisir d'inclure ou non les appareils administrés avec l'état OK dans le rapport État de la protection.
- Vous pouvez désormais activer Kaspersky Security Center Cloud Console en utilisant l'une des licences suivantes ou ajouter les clés de licence des licences répertoriées à un espace de travail existant :
  - Kaspersky Symphony Security
  - Kaspersky Symphony EDR
  - Kaspersky Symphony MDR

- Kaspersky Symphony XDR

- Une édition spéciale de l'Agent d'administration pour Windows XP est sortie.

- L'Agent d'administration mis à jour pour Linux prend en charge le service KSN Proxy. Outre les points de distribution Windows, vous pouvez désormais utiliser les points de distribution Linux pour transférer les requêtes Kaspersky Security Network (KSN) des appareils administrés. Cette fonction vous permet de rediffuser et optimiser le trafic sur le réseau.

- L'Agent d'administration mis à jour pour Linux prend en charge la fonction Registre des applications. L'Agent d'administration peut compiler une liste des applications installées sur un appareil administré basé sur Linux, puis transmettre cette liste au Serveur d'administration.

- Vous pouvez utiliser Kaspersky Security Center Cloud 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.

Mise à jour, Novembre 2022

Cette mise à jour de Kaspersky Security Center Cloud Console introduit les nouvelles fonctionnalités et améliorations suivantes :

- Kaspersky Security Center Cloud Console prend désormais en charge Kaspersky Endpoint Security 11.3 for Linux.

- Kaspersky Security Center Cloud Console prend désormais en charge Kaspersky Managed Detection and Response 2.1.18.

- Kaspersky Security Center Cloud Console prend désormais en charge les versions mises à jour de Kaspersky Endpoint Security for Mac 11.2 et 11.2.1 pour prendre en charge macOS 13.

- Les vidéos de la section **Introduction et tutoriels** ont été mises à jour.

Mise à jour, Octobre 2022

Cette mise à jour de Kaspersky Security Center Cloud Console introduit les nouvelles fonctionnalités et améliorations suivantes :

- Nous avons mis à jour le texte du Contrat de traitement des données de Kaspersky Security Center Cloud Console.

- L'infrastructure de Kaspersky Security Center Cloud Console vous signale désormais un espace de travail qui n'a pas de clé de licence active et qui peut être supprimé si vous n'ajoutez pas de nouvelle clé de licence.

- Kaspersky Security Center Cloud Console prend désormais en charge Kaspersky Endpoint Security 11.11.0 for Windows.

- Kaspersky Security Center Cloud Console prend désormais en charge Kaspersky Endpoint Detection and Response Optimum 2.3.

- Kaspersky Embedded Systems Security 3.2 for Windows est pris en charge.

Mise à jour septembre 2022

Cette mise à jour de Kaspersky Security Center Cloud Console introduit les nouvelles fonctionnalités et améliorations suivantes :

- Vous pouvez désormais désigner des administrateurs dédiés pour les Serveurs d'administration virtuels. Vous créez un compte utilisateur pour un administrateur, puis vous accordez à l'administrateur les droits d'accès à un Serveur d'administration virtuel. L'administrateur désigné a accès uniquement au Serveur d'administration virtuel sélectionné et ne peut pas se connecter au Serveur d'administration principal ou à d'autres Serveurs d'administration secondaires, physiques ou virtuels.

- Expérience utilisateur optimisée lors de la suppression d'une clé de licence pour Kaspersky Security Center Cloud Console. Le nouveau mécanisme vous évite de supprimer votre dernière clé de licence active par accident.

- Vous pouvez désormais utiliser les points de distribution Linux pour télécharger les bases antivirus pour les applications de sécurité Kaspersky à l'aide de la tâche Téléchargement des mises à jour sur les stockages des points de distribution.

- L'Agent d'administration est désormais disponible en version japonaise.

- Dans l'interface de Kaspersky Security Center Cloud Console, le style entièrement majuscule des noms de section a été remplacé par une majuscule de style phrase.

Mise à jour août 2022

Nouvelles langues prises en charge : Kaspersky Security Center Cloud Console est entièrement disponible en japonais.

Mise à jour en juillet 2022

Cette mise à jour de Kaspersky Security Center Cloud Console introduit les nouvelles fonctionnalités et améliorations suivantes :

- Nouvelles versions des applications Kaspersky prises en charge :
  - Kaspersky Endpoint Agent 3.13
  - Kaspersky Endpoint Security 11.2.1 for Mac
  - Kaspersky Security for iOS 1.0.0
  - Kaspersky Endpoint Security 11.10.0 for Windows
- Nous avons mis à jour le texte du Contrat et du Contrat de traitement des données de Kaspersky Security Center Cloud Console.
- Nouvelle langue proposée : l'infrastructure Kaspersky Security Center Cloud Console est désormais disponible en japonais également. La prise en charge du japonais dans les espaces de travail de Kaspersky Security Center Cloud Console arrive bientôt.

Mise à jour avril 2022

Cette mise à jour de Kaspersky Security Center Cloud Console introduit les nouvelles fonctionnalités et améliorations suivantes :

- Kaspersky Security Center Cloud Console prend désormais en charge Kaspersky Endpoint Security 11.9.0 for Windows.
- Kaspersky Security Center Cloud Console prend désormais en charge la localisation japonaise de Kaspersky Embedded Systems Security.

Mise à jour le 09 mars 2022

Cette mise à jour de Kaspersky Security Center Cloud Console introduit les nouvelles fonctionnalités et améliorations suivantes :

- L'intégration avec Kaspersky Endpoint Detection and Response Expert est implémentée.
- La plateforme de réponse aux incidents (IRP) est implémentée. Vous pouvez désormais gérer les incidents de sécurité via Kaspersky Security Center Cloud Console.
- Kaspersky Security Center Cloud Console accepte désormais les clés de licence pour Kaspersky Endpoint Detection and Response Expert. Le nombre minimum d'appareils pour la licence est de 50.

Mise à jour le 11 février 2022

Cette mise à jour de Kaspersky Security Center Cloud Console introduit les nouvelles fonctionnalités et améliorations suivantes :

- Les licences de Kaspersky Embedded Systems Security pour Windows sont désormais prises en charge.
- Kaspersky Endpoint Security 11.8.0 for Windows est pris en charge.
- Vous pouvez installer Kaspersky Endpoint Security 11.8.0 for Windows à l'aide d'un paquet de distribution en japonais.
- Kaspersky Endpoint Agent 3.12 est pris en charge.

Mise à jour le 10 décembre 2021

Cette mise à jour de Kaspersky Security Center Cloud Console introduit les nouvelles fonctionnalités et améliorations suivantes :

- Le travail avec les utilisateurs internes a été amélioré :
  - Vous pouvez maintenant ajouter de nouveaux utilisateurs internes sur le portail.
  - L'application vous empêche maintenant de diminuer vos propres droits.

Mise à jour le 18 octobre 2021

Cette mise à jour de Kaspersky Security Center Cloud Console introduit les nouvelles fonctionnalités et améliorations suivantes :

- Kaspersky Security Center Cloud Console prend désormais en charge Kaspersky Endpoint Detection and Response Optimum 2.0.

- Vous pouvez maintenant administrer des appareils exécutant Android à l'aide de Kaspersky Security Center Cloud Console.

- La place de marché de Kaspersky est disponible en tant que nouvelle section de menu : vous pouvez désormais rechercher l'application Kaspersky à l'aide de Kaspersky Security Center Cloud Console.

- Une nouvelle section du menu, les annonces de Kaspersky, est disponible. Les annonces Kaspersky vous tiennent informé en fournissant des informations relatives aux applications Kaspersky installées sur les appareils administrés. Kaspersky Security Center Cloud Console met périodiquement à jour les informations figurant dans cette section.

- Vous pouvez désormais administrer les Serveurs d'administration secondaires fonctionnant sous les systèmes d'exploitation Linux via Kaspersky Security Center Cloud Console.

Mise à jour le 7 septembre 2021

Cette mise à jour de Kaspersky Security Center Cloud Console introduit les nouvelles fonctionnalités et améliorations suivantes :

- Vous pouvez désormais utiliser Active Directory Federation Services (AD FS) pour vous connecter à Kaspersky Security Center Cloud Console à l'aide de votre compte Active Directory, sans créer de nouveau compte utilisateur.

- Kaspersky Security Center Cloud Console fonctionne désormais avec les environnements Cloud suivants : Amazon Web Services, Microsoft Azure et Google Cloud. Pour protéger les machines virtuelles (ou instances) dans un environnement cloud, vous avez besoin de l'une des Licences Kaspersky Hybrid Cloud Security. L'Assistant de configuration pour une utilisation dans le Cloud est disponible.

- Le nombre maximum d'appareils par espace de travail est désormais de 25 000.

- L'intégration avec les systèmes SIEM est désormais disponible dans Kaspersky Security Center Cloud Console. Vous pouvez exporter des événements vers des systèmes SIEM en utilisant le protocole Syslog.

- Vous pouvez désormais créer des Serveurs d'administration virtuels. Chaque Serveur d'administration virtuel peut avoir sa propre structure de groupes d'administration, de stratégies, de tâches, de rapports et d'événements. Vous pouvez utiliser des Serveurs d'administration virtuels pour la gestion des entreprises clientes avec des workflows complexes au sein de votre espace de travail. Cependant, vous ne pouvez pas migrer les Serveurs d'administration virtuels de Kaspersky Security Center fonctionnant sur site vers Kaspersky Security Center Cloud Console.

- Vous pouvez désormais ajuster la largeur des colonnes dans les tableaux, trier et rechercher des données.

- Nous avons amélioré la stabilité et la disponibilité de Kaspersky Business Hub et de Kaspersky Security Center Cloud Console.

Mise à jour le 27 octobre 2020

Cette mise à jour de Kaspersky Security Center Cloud Console introduit les nouvelles fonctionnalités et améliorations suivantes :

- Kaspersky Security Center Cloud Console prend désormais en charge Kaspersky Endpoint Security 11.6.0 for Windows, Kaspersky Endpoint Security 11.1 for Mac Correctif A et Kaspersky Endpoint Agent 3.10 (comme partie intégrante de Kaspersky Endpoint Detection and Response Optimum).

- Vous pouvez maintenant utiliser les licences suivantes :

    - Kaspersky Endpoint Detection and Response Optimum
    - Kaspersky Endpoint Security for Business Advanced
    - Kaspersky Total Security for Business
- Les fonctionnalités suivantes sont mises en œuvre :
    - Gestion des vulnérabilités et des correctifs
    - Gestion du chiffrement
    - Contrôle des applications
    - Contrôle évolutif des anomalies
    - Sessions RDP, y compris le partage du bureau Windows
- Le menu de navigation est désormais vertical et ressemble à l'interface basée sur la Console de gestion (MMC) de Kaspersky Security Center.
- Des vidéos de formation technique sont maintenant disponibles ; elles vous aideront à apprendre comment fonctionne l'application.

Mise à jour le 30 juin 2020

Cette mise à jour de Kaspersky Security Center Cloud Console introduit les nouvelles fonctionnalités et améliorations suivantes :

- Kaspersky Security Center Cloud Console prend désormais en charge Kaspersky Security 11 for Windows Server (à partir du septembre 2020).
- Kaspersky Security Center Cloud Console prend désormais en charge Kaspersky Endpoint Agent 3.9 et Kaspersky Endpoint Security 11.4.0 for Windows.
- L'Assistant de démarrage rapide de l'application a été amélioré : certaines étapes ont été supprimées, la séquence des étapes a été légèrement modifiée et certains textes ont été modifiés pour plus de convivialité.
- Kaspersky Security Center Cloud Console est désormais disponible en italien.
- Vous pouvez désormais révoquer le Contrat de licence utilisateur final (CLUF) pour toute application Kaspersky administrée via l'interface de Kaspersky Security Center Cloud Console. Vous devez désinstaller l'application sélectionnée avant de révoquer son CLUF.
- Vous pouvez désormais supprimer des espaces de travail. Si vous marquez un espace de travail pour suppression, il est par défaut supprimé automatiquement au bout de sept jours. Cependant, vous pouvez forcer la suppression de l'espace de travail de manière à ce qu'il soit supprimé immédiatement.
- La vérification en deux étapes pour la connexion à la console est implémentée.

Kaspersky Security Center Cloud Console

Cette section reprend les informations sur la désignation, les fonctions clés et la composition de l'application Kaspersky Security Center Cloud Console.

Kaspersky Security Center Cloud Console est une application hébergée et maintenue par Kaspersky. Vous n'avez pas besoin d'installer Kaspersky Security Center Cloud Console sur votre ordinateur ou votre serveur. Kaspersky Security Center Cloud Console permet à l'administrateur d'installer des applications de sécurité 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. L'administrateur peut 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.

À propos de Kaspersky Security Center Cloud Console

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

Kaspersky Security Center Cloud Console vous permet d'effectuer les opérations suivantes :

- Installer des applications de Kaspersky sur les appareils de votre réseau et administrer les applications installées.
- Former une hiérarchie des groupes d'administration pour administrer les appareils (les appareils clients et les machines virtuelles) comme un ensemble.
- Créez des serveurs d'administration virtuels et organisez-les dans une hiérarchie.
- Protégez vos appareils réseau, y compris les postes de travail et les serveurs :
  - Administrer le système de protection anti-malware fondé sur les applications de Kaspersky.
  - Utilisez les fonctionnalités de détection et de réponse (EDR et MDR) (une licence pour Kaspersky Endpoint Detection and Response et/ou pour Kaspersky Managed Detection and Response est requise), notamment :
    - Enquêter sur les incidents et les analyser
    - Visualisation des incidents par la création d'un graphique de la chaîne de développement des menaces
    - Accepter ou rejeter les réponses manuellement ou configurer l'acceptation automatique de toutes les réponses
- Utiliser Kaspersky Security Center Cloud Console comme application multi-locataire.
- Administrer à distance les applications de Kaspersky installées sur les appareils clients.
- Effectuer un déploiement centralisé des clés de licence pour les applications Kaspersky sur les appareils client.
- Créer et gérer des stratégies de sécurité pour les appareils de votre réseau.
- Créer et gérer des comptes utilisateurs.
- Créer et gérer des rôles d'utilisateur (RBAC).

- Créer et administrer les tâches pour les applications installées sur vos appareils dans le réseau.
- Affichez les rapports sur l'état du système de sécurité pour chaque entreprise cliente individuellement.

Vous gérez Kaspersky Security Center Cloud Console à l'aide d'une Console d'administration basée sur le cloud qui garantit l'interaction entre votre appareil et le Serveur d'administration via un navigateur. Le Serveur d'administration est une application qui sert à administrer les applications de Kaspersky installées sur les appareils de votre réseau. Lorsque vous vous connectez à Kaspersky Security Center Cloud Console à l'aide de votre navigateur, celui-ci établit une connexion avec le serveur de la console Kaspersky Security Center sur le Cloud.

Le Serveur d'administration et le système de gestion de base de données (SGBD) connecté sont déployés dans un environnement sur le cloud et vous sont fournis en tant que service. La maintenance du Serveur d'administration et du SGBD est incluse dans le service. Tous les composants logiciels de Kaspersky Security Center Cloud Console sont mis à jour. Le Serveur d'administration et les objets créés (tels que les stratégies et les tâches) sont sauvegardés régulièrement pour assurer leur sécurité.

Kaspersky Security Center Cloud Console est une application multilingue. Vous pouvez modifier la langue de l'interface à tout moment, sans rouvrir l'application.

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.

Configurations matérielle et logicielle requises pour Kaspersky Security Center Cloud Console

Console d'administration

Pour un client, l'utilisation de Kaspersky Security Center Cloud Console nécessite uniquement un navigateur.

Vous ne pouvez utiliser qu'une seule fenêtre ou un seul onglet de navigateur pour travailler avec Kaspersky Security Center Cloud Console.

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 Cloud Console.

Navigateur :

- Google Chrome 133.0.6943.53 ou version ultérieure
- Microsoft Edge 134.0.3124.66 ou version ultérieure
- Safari 17.6 sur macOS
- Yandex Browser 25.2.3.809 ou version ultérieure
- Mozilla Firefox Extended Support Release 128.8.0 ou version ultérieure

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 matérielle minimum requise pour Gestion des vulnérabilités et des correctifs :

- Processeur cadencé à 1,4 GHz ou plus. Un système d'exploitation 64 bits est requis.
- Mémoire vive : 8 Go.
- Espace disque disponible : 1 Go.

Systèmes d'exploitation pris en charge par l'Agent d'administration

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 pour Stations de travail/Entreprise/Éducation 32 bits/64 bits Microsoft Windows 10 TH2 (novembre 2015) Famille/Pro pour Stations de travail/Entreprise/Éducation 32 bits/64 bits Microsoft Windows 10 RS1 (août 2016) Famille/Pro pour Stations de travail/Entreprise/Éducation 32 bits/64 bits Microsoft Windows 10 RS2 (avril 2017) Familiale/Pro pour Stations de travail/Entreprise/Éducation 32 bits/64 bits Microsoft Windows 10 RS3 (Fall Creators Update, v1709) Famille/Pro pour Stations de travail/Entreprise/Éducation 32 bits/64 bits Microsoft Windows 10 RS4 (mise à jour d'avril 2018, v17134) Famille/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 32 bits/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 pour Stations de travail/Entreprise/Éducation 32 bits/64 bits Microsoft Windows 10 20H2 (mise à jour d'octobre 2020) Famille/Pro pour Stations de travail/Entreprise/Éducation 32 bits/64 bits Microsoft Windows 10 21H1 (mise à jour de mai 2021) Famille/Pro pour Stations de travail/Entreprise/Éducation 32 bits/64 bits

	Microsoft Windows 10 21H2 (mise à jour d'octobre 2021) Famille/Pro pour Stations de travail/Entreprise/Éducation 32 bits/64 bits Microsoft Windows 10 22H2 (mise à jour d'octobre 2023) Famille/Pro pour Stations de travail/Entreprise/Éducation 32 bits/64 bits Microsoft Windows 11 Famille/Pro pour Stations de travail/Entreprise/Éducation 64 bits Microsoft Windows 11 22H2 Famille/Pro pour Stations de travail/Entreprise/Éducation 64 bits Microsoft Windows 11 23H2 Famille/Pro pour Stations de travail/Entreprise/Éducation 64 bits Microsoft Windows 11 24H2 Famille/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 avec Service Pack 3 et versions ultérieures 32 bits (pris en charge par l'Agent d'administration version 14.0.0.20023) Microsoft Windows XP Professional for Embedded Systems avec Service Pack 3 32 bits (pris en charge par l'Agent d'administration version 14.0.0.20023)
Systèmes d'exploitation. Serveurs Microsoft Windows	Microsoft Windows MultiPoint Server 2011 Standard/Premium 64 bits Microsoft Windows Server 2008 Standard/Enterprise/Datacenter/Foundation avec Service Pack 2 32 bits / 64 bits Microsoft Windows Server 2008 R2 Standard/Datacenter/Enterprise/Foundation avec Service Pack 1 et versions ultérieures 64 bits 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 Server Core/Datacenter/Essentials/Standard (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 2022 21H2 Standard/Datacenter 64 bits Microsoft Windows Server 2025 Standard/Datacenter/Core 64 bits Windows Small Business Server 2011 Standard/Essentials/Premium Add-on 64 bits
Systèmes d'exploitation. Linux	Debian GNU/Linux 12 (Bookworm) 32 bits / 64 bits Debian GNU/Linux 11.x (Bullseye) 32 bits / 64 bits Ubuntu Server 16.04 LTS (Xenial Xerus) 32 bits / 64 bits Ubuntu Server 24.04 LTS 64 bits Ubuntu Server 22.04 LTS 64 bits Ubuntu Server 20.04 LTS (Focal Fossa) 64 bits CentOS 7.x 64 bits CentOS Stream 8 64 bits CentOS Stream 9 64 bits Red Hat Enterprise Linux Server 9.x 64 bits Red Hat Enterprise Linux Server 8.x 64 bits Red Hat Enterprise Linux Server 7.x 64 bits openSUSE Leap 15 64 bits SUSE Linux Enterprise Server 15 (Tous Service Packs) 64 bits SUSE Linux Enterprise Server 12 (Tous Service Packs) 64 bits Oracle Linux 7 64 bits Oracle Linux 8 64 bits Oracle Linux 9 64 bits Linux Mint 20.x 64 bits Linux Mint 21.x 64 bits Linux Mint 22.x 64 bits Alma Linux 8.x 64 bits Alma Linux 9.x 64 bits Rocky Linux 8.x 64 bits Rocky Linux 9.x 64 bits Amazon Linux 2 64 bits

	Kylin 10 64 bits
Systèmes d'exploitation. macOS	macOS Monterey (12.x) macOS Ventura (13.x) macOS Sonoma (14.x) macOS Sequoia (15.x)

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

Plateformes de virtualisation prises en charge :

- VMware vSphere 6.7
- VMware vSphere 7.0
- Citrix XenServer 7.1 LTSR
- Citrix XenServer 8.x
- Parallels Desktop 18
- Oracle VM VirtualBox 7.x
- Microsoft Hyper-V Server 2019 64 bits
- Microsoft Hyper-V Server 2022 64 bits
- Machine virtuelle basée sur le noyau (tous les systèmes d'exploitation Linux pris en charge par l'Agent d'administration)

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

Compatible avec les applications et les solutions de Kaspersky

Les licences relatives à différents produits confèrent divers ensembles d'applications et de solutions Kaspersky.

Vous pouvez déployer et gérer les applications et les solutions Kaspersky suivantes via Kaspersky Security Center Cloud Console :

- Kaspersky Security for Windows Server 11.0.1
- Kaspersky Endpoint Security 12.9 for Windows (seul le chiffrement simplifié (AES56) est pris en charge)
- Kaspersky Endpoint Security 12.2 for Linux
- Kaspersky Endpoint Security 12.1 for Mac
- Kaspersky Embedded Systems Security 3.4 for Windows
- Kaspersky Embedded Systems Security 3.4 for Linux
- Kaspersky Endpoint Agent 4.0

- Kaspersky Endpoint Security for Android
- Kaspersky Security for iOS

Vous pouvez intégrer les solutions suivantes pour afficher et traiter les incidents de sécurité :

- Kaspersky Managed Detection and Response
- Kaspersky Endpoint Detection and Response Optimum
- Kaspersky Endpoint Detection and Response Expert

Si vous installez une nouvelle version de l'application sur un appareil administré, tout en faisant appel à une stratégie obsolète pour la nouvelle version de l'application au lieu de mettre à jour la stratégie, l'application fournit toujours des données à Kaspersky Security Center Cloud Console, mais Kaspersky Security Center Cloud Console ne peut pas traiter ces données, comme décrit dans la section Données traitées des applications administrées de la documentation. Pour que Kaspersky Security Center Cloud Console traite ces données, vous devez créer une nouvelle stratégie pour la nouvelle version de l'application.

Localisation de Kaspersky Security Center Cloud Console

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

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

Comparaison de Kaspersky Security Center et de Kaspersky Security Center Cloud Console

Vous pouvez utiliser Kaspersky Security Center de l'une des manières suivantes :

- En tant que solution cloud

  Kaspersky Security Center est installé pour vous dans l'environnement cloud et Kaspersky vous fournit un accès au Serveur d'administration en tant que service. Vous administrez le système de sécurité réseau via la Console d'administration dans le cloud nommée Kaspersky Security Center Cloud Console. Cette console dispose d'une interface semblable à l'interface de Kaspersky Security Center Web Console.

- En tant que solution sur site (Windows ou Linux)

  Vous installez Kaspersky Security Center sur un appareil local et vous gérez le système de sécurité du réseau via une Console d'administration basée sur Microsoft Management Console ou Kaspersky Security Center Web Console.

  En plus de l'application Windows, Kaspersky Security Center Linux est également disponible. Kaspersky Security Center Linux est conçu pour déployer et gérer la protection des appareils Linux en utilisant un serveur d'administration basé sur Linux pour répondre aux exigences des environnements Linux purs. Kaspersky Security Center et Kaspersky Security Center Linux basés sur Windows ont différents ensembles de fonctionnalités.

Le tableau ci-dessous vous permet de comparer les principales fonctionnalités de Kaspersky Security Center et de Kaspersky Security Center Cloud Console.

Comparaison des fonctionnalités de Kaspersky Security Center fonctionnant sur site et en tant que solution cloud

Fonctionnalité ou propriété	Kaspersky Security Center exécuté sur site	Kaspersky Security Center Cloud Console
Emplacement du Serveur d'administration	Sur site	Dans le Cloud
Emplacement du système de gestion de base de données (SGBD)	Sur site	Dans le Cloud
Console d'administration Internet	✓	✓
Maintenance du Serveur d'administration et du SGBD	Administré par le client	Administré par Kaspersky
Hiérarchie des Serveurs d'administration	✓	✓ (le Serveur d'administration de Kaspersky Security Center Cloud Console ne peut agir qu'en tant que Serveur d'administration principal dans la hiérarchie et ne peut être utilisé que pour la surveillance des stratégies et des tâches)
Hiérarchie du groupe d'administration	✓	✓
Migration des appareils administrés et des objets associés de Kaspersky Security Center sur site vers Kaspersky Security Center Cloud Console	✓	✓
Sondage réseau	✓	✓ (par points de distribution uniquement)
Nombre maximum d'appareils administrés	100 000	25 000
Protection des appareils administrés Windows, Linux et macOS	✓	✓
Protection des appareils mobiles	✓	✓ (seuls Kaspersky Endpoint Security for Android et Kaspersky Security for iOS sont pris en charge)
Protection de l'infrastructure Cloud publique	✓	✓
Administration de la sécurité centrée sur l'appareil	✓	✓
Stratégies d'application	✓	✓
Tâches pour les applications Kaspersky	✓	✓

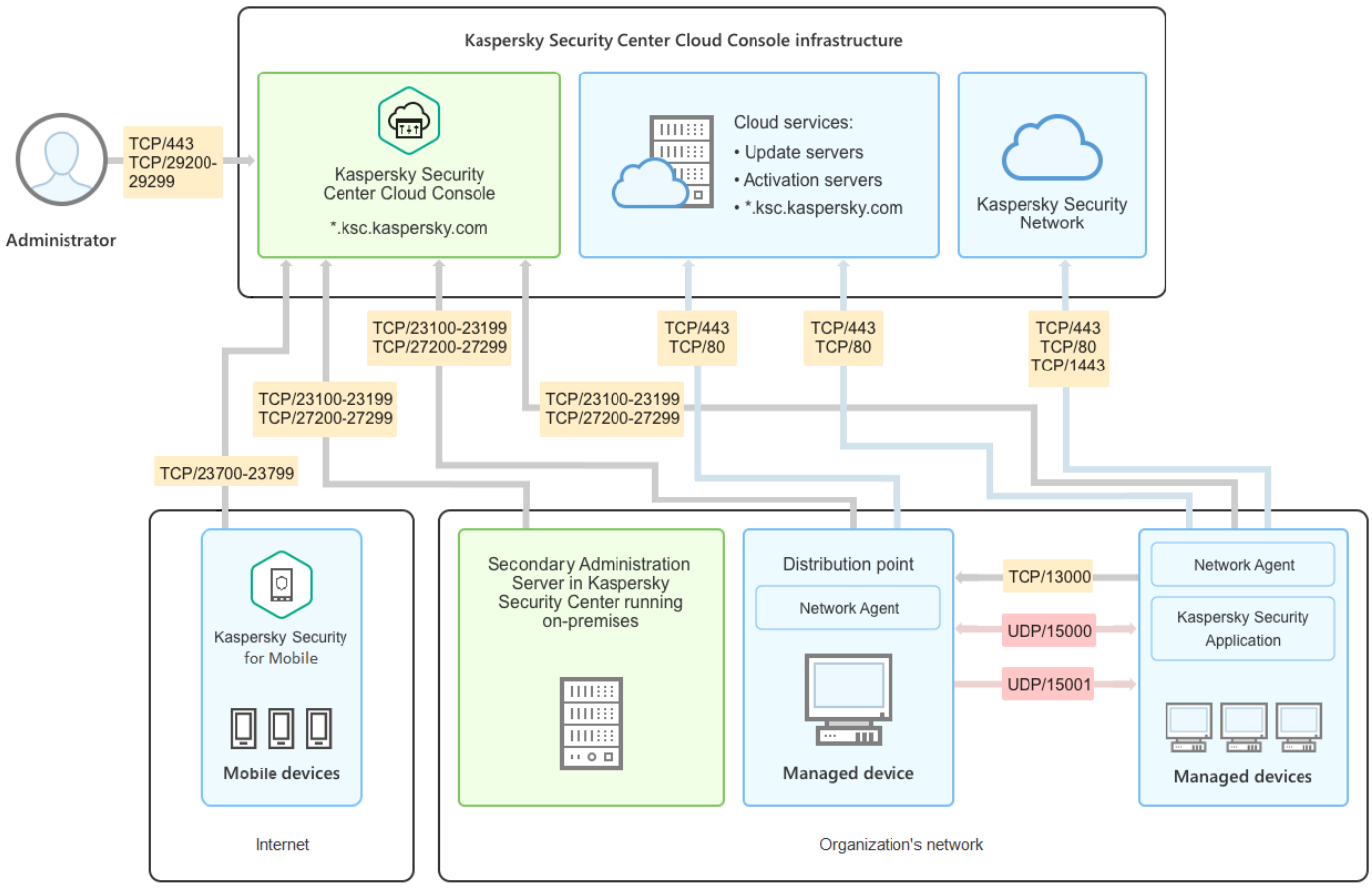
Kaspersky Security Network	✓	✓
Serveur proxy KSN	✓	✓ (sur les points de distribution uniquement)
Kaspersky Private Security Network	✓	—
Déploiement centralisé des clés de licence pour les applications Kaspersky	✓	✓
Transfert des Appareils administrés vers un autre Serveur d'administration	✓	— (vous devez réinstaller les Agents d'administration sur les appareils administrés pour les transférer vers un autre Serveur d'administration)
Prise en charge des Serveurs d'administration virtuels	✓	✓
Installation des mises à jour du logiciel tiers et correction des vulnérabilités dans les applications tierces	✓	✓ (pour corriger les vulnérabilités dans les applications tierces, seuls les correctifs recommandés peuvent être installés)
Notifications sur les événements survenus sur les appareils administrés	✓	✓
Création et gestion des comptes utilisateurs	✓	✓
Nombre maximal d'événements stockés dans la base de données	400 000 (peut être augmenté jusqu'à 45 000 000)	400 000 (dépend du nombre d'appareils administrés)
Intégration avec les systèmes SIEM	✓	✓ (en utilisant uniquement le format Syslog et le protocole TLS par TCP)
Utilisation du Serveur d'administration comme serveur WSUS	✓	—
Surveillance de l'état des stratégies et des tâches	✓	✓
Prise en charge des clusters et des matrices de serveurs dans les groupes d'administration	✓	✓
Installation à distance des systèmes d'exploitation	✓	—
Prise en charge SNMP	✓	—
Nombre maximum de Serveurs virtuels	500	200
Clonage du disque dur d'un appareil	✓	—

Architecture et concepts de base

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

Architecture

Cette section décrit les composants de Kaspersky Security Center Cloud Console et leur interaction.



Architecture Kaspersky Security Center Cloud Console

L'instance de Kaspersky Security Center Cloud Console administrée via la console dans le cloud comprend deux composants principaux : l'infrastructure de Kaspersky Security Center Cloud Console et l'infrastructure du client.

L'infrastructure de Kaspersky Security Center Cloud Console se compose des éléments suivants :

- **Console d'administration dans le cloud**. Ceci offre une interface Web pour créer et maintenir le système de protection du réseau d'une entreprise cliente administrée par Kaspersky Security Center Cloud Console.
- **Services cloud**. Comprend les serveurs de mises à jour et les serveurs d'activation.
- **Kaspersky Security Network (KSN)**. Serveurs contenant la base de données de Kaspersky, qui reçoit continuellement 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.

L'infrastructure du client peut comprendre les éléments suivants :

- **Point de distribution**. Ordinateur avec un Agent d'administration installé, utilisé pour la diffusion des mises à jour, le sondage du réseau, l'installation à distance des applications, la collecte d'informations sur les ordinateurs faisant partie du groupe d'administration et/ou d'un domaine multidiffusion. L'administrateur sélectionne les appareils appropriés et leur attribue manuellement des points de distribution.

- **Appareils administrés**. Ordinateurs du réseau du client protégés par Kaspersky Security Center Cloud Console. L'Agent d'administration et une application de sécurité Kaspersky doivent être installés sur chaque appareil administré.

- **Serveur d'administration secondaire fonctionnant sur site** (facultatif). Vous pouvez utiliser un Serveur d'administration fonctionnant sur site pour créer une hiérarchie de Serveurs d'administration.

Ports utilisés par Kaspersky Security Center Cloud Console

Pour utiliser Kaspersky Security Center Cloud Console, qui fait partie de l'infrastructure Kaspersky, vous devez ouvrir les ports suivants sur les appareils clients pour permettre la connexion Internet (voir le tableau ci-dessous) :

Ports qui doivent être ouverts sur les appareils clients pour permettre la connexion Internet

Port (ou plage de ports)	Protocole	But du port (ou plage de ports)
23100-23199	TCP/TLS	Réception des connexions des Agents d'administration et des Serveurs d'administration secondaires sur le Serveur d'administration de Kaspersky Security Center Cloud Console à l'adresse *.ksc.kaspersky.com. L'infrastructure Kaspersky peut se servir de n'importe quel port dans cette plage et de n'importe quelle adresse Web dans ce masque. Le port et l'adresse Internet peuvent changer de temps en temps.
23700-23799 (uniquement si vous administrez des appareils mobiles)	TCP/TLS	Réception des connexions des appareils mobiles. Connexion au Serveur d'administration de Kaspersky Security Center Cloud Console à l'adresse *.ksc.kaspersky.com. L'infrastructure Kaspersky peut se servir de n'importe quel port dans cette plage et de n'importe quelle adresse Web dans ce masque. Le port et l'adresse Internet peuvent changer de temps en temps.
27200-27299	TCP/TLS	Réception des connexions pour l'activation de l'application depuis les appareils administrés (sauf les appareils mobiles). Connexion au Serveur d'administration de Kaspersky Security Center Cloud Console à l'adresse *.ksc.kaspersky.com. L'infrastructure Kaspersky peut se servir de n'importe quel port dans cette plage et de n'importe quelle adresse Web dans ce masque. Le port et l'adresse Internet peuvent changer de temps en temps.
29200-29299	TCP/TLS	Établissement de connexions en tunnel aux appareils appareil administrés à l'aide de l'utilitaire klsctunnel via le serveur d'administration de Kaspersky Security Center Cloud Console à l'adresse *.ksc.kaspersky.com. L'infrastructure Kaspersky peut se servir de n'importe quel port dans cette plage et de n'importe quelle adresse Web dans ce masque. Le port et l'adresse Internet peuvent changer de temps en temps.
443	HTTPS	Connexion au service de découverte de Kaspersky Security Center Cloud Console à l'adresse *.ksc.kaspersky.com. L'infrastructure de Kaspersky peut utiliser n'importe quelle adresse Web dans ce masque.
1443	TCP	Connexion à Kaspersky Security Network
80	TCP	Connection permet de vérifier la validité des certificats de Kaspersky Security Center sur *.digicert.com. L'infrastructure de Kaspersky peut utiliser n'importe quelle adresse Web dans ce masque.

Le tableau ci-dessous indique les ports qui doivent être ouverts sur les appareils clients sur lesquels l'Agent d'administration est installé.

Ports qui doivent être ouverts sur les appareils clients

Numéro de port	Protocole	Destination du port	Zone de fonctionnement
15000	UDP	Réception de données à partir de passerelles de connexion (si elles sont utilisées)	Administration des appareils clients
15000	Diffusion UDP	Obtention de données sur d'autres Agents d'administration dans le même domaine de diffusion	Remise des mises à jour et des paquets d'installation
15001	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

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

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

Le tableau ci-dessous indique les ports supplémentaires qui doivent être ouverts sur les appareils client sur lesquels l'Agent d'administration est installé et agit en tant que point de distribution.

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

Numéro de port	Protocole	Destination du port	Zone de fonctionnement
13000	TCP/TLS	Réception des connexions des Agents d'administration	Administration des appareils clients, et remise des mises à jour et des paquets d'installation
13111 (uniquement si le service KSN proxy est exécuté sur l'appareil)	TCP	Réception des requêtes des appareils administrés au serveur proxy KSN	Serveur proxy KSN
13295 (uniquement si vous utilisez le point de distribution comme serveur push)	TCP/TLS	Envoi de notifications push aux appareils administrés	Point de distribution utilisé comme serveur push
15111 (uniquement si le service KSN proxy est exécuté sur l'appareil)	UDP	Réception des requêtes des appareils administrés au serveur proxy KSN	Serveur proxy KSN
17111 (uniquement si le service KSN proxy est exécuté sur l'appareil)	HTTPS	Réception des requêtes des appareils administrés au serveur proxy KSN	Serveur proxy KSN

Si vous avez un ou plusieurs Serveurs d'administration sur votre réseau et que vous les utilisez comme Serveurs d'administration secondaires lorsque le Serveur d'administration principal est situé dans l'infrastructure de Kaspersky, veuillez vous référer à la liste des ports utilisés par Kaspersky Security Center fonctionnant sur site. Utilisez ces ports pour l'interaction entre votre Serveur d'administration secondaire (ou les Serveurs d'administration secondaires) et les appareils clients.

Notions principales

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

Agent d'administration

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

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

- Sous le nom " Agent d'administration de Kaspersky Security Center "
- Avec lancement automatique lors du démarrage du système d'exploitation
- Utilisation du compte LocalSystem

Un appareil doté de l'Agent d'administration est un *appareil administré* ou un *appareil*. Vous pouvez installer l'Agent d'administration sur un appareil Windows, Linux ou Mac.

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

L'Agent d'administration synchronise l'appareil administré avec le serveur d'administration. Kaspersky Security Center Cloud Console synchronise automatiquement le Serveur d'administration avec les appareils administrés plusieurs fois par heure. Le Serveur d'administration définit l'intervalle de synchronisation (également appelé *pulsation*) en fonction du nombre d'appareils administrés.

Groupes d'administration

Un *groupe d'administration* (ci-après également appelé *groupe*) est un ensemble logique d'appareils administrés regroupés sur la base d'une caractéristique en vue de gérer les appareils groupés en tant qu'unité unique dans Kaspersky Security Center Cloud Console.

Pour tous les appareils administrés dans le groupe d'administration, 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'ordinateur de cet employé depuis le groupe d'administration Comptables vers le groupe d'administration Développeurs. L'ordinateur recevra automatiquement par la suite les paramètres des applications requis pour les développeurs.

Hiérarchie des Serveurs d'administration

Les Serveurs d'administration peuvent développer une hiérarchie du type " serveur primaire – serveur secondaire ". Chaque Serveur d'administration peut avoir plusieurs Serveurs d'administration secondaires aux différents niveaux hiérarchiques. Le niveau d'intégration des Serveurs d'administration 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.

Le Serveur d'administration de Kaspersky Security Center Cloud Console ne peut agir qu'en tant que Serveur d'administration principal et ne peut avoir comme serveurs secondaires que des Serveurs d'administration exécutés sur site.

Lors de la migration du serveur d'administration qui s'exécute sur site vers le Serveur d'administration de Kaspersky Security Center Cloud Console, vous pouvez organiser les Serveurs d'administration dans une hiérarchie. Ensuite, pour limiter la migration, vous ne pouvez déplacer qu'une partie de vos appareils administrés vers l'administration du Serveur d'administration de Kaspersky Security Center Cloud Console. Les autres appareils administrés restent sous l'administration du Serveur d'administration local. Cela vous permet de tester les fonctionnalités d'administration de Kaspersky Security Center Cloud Console sur un nombre limité d'appareils administrés. Dans le même temps, vous pouvez configurer des stratégies, des tâches, des rapports et d'autres objets pour tester l'administration et la surveillance de l'ensemble de votre réseau. Cela vous permet de revenir aux objets configurés sur le Serveur d'administration local si nécessaire.

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 d'administration différents.

Serveur d'administration virtuel

Serveur d'administration virtuel (ci-après *Serveur virtuel*) : le module de l'application Kaspersky Security Center Cloud Console conçu pour l'administration du système de protection antivirus du réseau de l'entreprise cliente. Chaque Serveur d'administration virtuel peut avoir sa propre structure de groupes d'administration et ses propres moyens de gestion et de surveillance, comme des stratégies, des tâches, des rapports et des événements. La zone de fonctionnement des Serveurs d'administration virtuels peut être utilisée par des organisations avec des workflows complexes.

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

- Les Serveurs d'administration virtuels ne sont pris en charge que dans le mode commercial de Kaspersky Security Center Cloud Console.
- La création des Serveurs d'administration secondaires (y compris les Serveurs virtuels) n'est pas prise en charge par le Serveur d'administration virtuel.
- Vous ne pouvez pas migrer les Serveurs d'administration virtuels de Kaspersky Security Center vers Kaspersky Security Center Cloud Console.
- Les Serveurs d'administration virtuels ne peuvent pas être administrés par des administrateurs dédiés. Par défaut, l'administrateur qui gère le Serveur d'administration principal gère également 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.
- Dans la fenêtre des propriétés du Serveur d'administration virtuel, l'ensemble de sections est limité.

Point de distribution

Le point de distribution 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 :

- Distribuez les mises à jour et les paquets d'installation sur les appareils clients du groupe (y compris la distribution par multidiffusion en utilisant UDP). Les mises à jour peuvent être reçues des serveurs de mises à jour de Kaspersky par le biais d'une tâche de mise à jour créée pour le point de distribution.

  Les appareils de points de distribution exécutant macOS ne peuvent pas télécharger les mises à jour à partir des serveurs de mises à jour de Kaspersky.

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

- Diffuser les stratégies et les tâches de groupe à l'aide d'une diffusion de type multidiffusion via le protocole UDP.
- Servir de passerelle pour la connexion au Serveur d'administration des appareils administrés, car une connexion directe ne peut pas être établie dans l'infrastructure cloud.
- Sonder le réseau dans le but de détecter de nouveaux appareils et de mettre à jour les informations sur les appareils détectés.
- Installer à distance les applications tierces comme les applications Kaspersky à l'aide de Microsoft Windows, y compris sur les appareils clients sans Agent d'administration installé.

  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.

  Cette fonctionnalité n'est pas prise en charge par les appareils de point de distribution exécutant Linux ou macOS.

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

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

Les appareils sur lesquels l'Agent d'administration est installé doivent se voir attribuer des points de distribution manuellement, en fonction des groupes 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. L'appareil qui fait office de point de distribution ne doit pas se trouver obligatoirement dans le groupe d'administration auquel il est attribué. Si la hiérarchie des groupes d'administration compte plusieurs points de distribution, l'Agent d'administration de l'appareil administré se connecte au point de distribution le plus proche dans la hiérarchie.

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

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

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

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

Un point de distribution nécessite au moins 4 Go d'espace libre sur le disque. Si l'espace libre disponible sur le disque du point de distribution est inférieur à 2 Go, Kaspersky Security Center Cloud Console crée un problème de sécurité avec le niveau d'importance *Avertissement*. Le problème de sécurité 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 de la vulnérabilité 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.

Plug-in Web d'administration

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

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 Cloud 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 Cloud Console fournit une stratégie propre à chaque application Kaspersky d'un groupe d'administration. La stratégie possède un des états suivants (voir le tableau ci-dessous) :

L'état de la stratégie

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

Le fonctionnement des stratégies obéit aux règles suivantes :

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

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

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

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

Les profils de stratégie fonctionnent conformément aux règles suivantes :

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

Profils de stratégie

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

Pour vous éviter la création de plusieurs instances d'une seule stratégie, Kaspersky Security Center Cloud Console 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.

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.

Licence de l'application

Cette section fournit des informations relatives à la licence de l'application.

Licence de Kaspersky Security Center Cloud Console

En suivant ce scénario, vous pouvez commencer à utiliser Kaspersky Security Center Cloud Console et les applications de sécurité administrées sous licence.

Kaspersky Security Center Cloud Console permet de diffuser de manière centralisée les clés de licence des applications de Kaspersky sur les appareils clients, suivre l'utilisation des clés et de prolonger la durée de validité des licences.

Si vous utilisez déjà Kaspersky Security Center Cloud Console, vous pouvez visiter la place de marché de Kaspersky pour afficher l'ensemble de la gamme de solutions d'entreprise de Kaspersky, sélectionner celles dont vous avez besoin et procéder à l'achat sur le site Internet de Kaspersky.

Vérification des fonctionnalités de Kaspersky Security Center Cloud Console en mode d'essai avant d'acheter une licence

Vous pouvez d'abord essayer gratuitement Kaspersky Security Center Cloud Console. Pour ce faire, créez un espace de travail d'essai qui se terminera dans 30 jours. Si vous souhaitez un espace de travail commercial que vous pouvez utiliser aussi longtemps que vous le souhaitez, vous devrez acheter une licence.

Le mode d'évaluation ne vous permet pas de passer au mode commercial. Tout espace de travail d'évaluation est automatiquement supprimé ainsi que tout son contenu lorsque la durée d'utilisation de 30 jours a expiré.

Étapes

Le scénario se déroule par étapes :

1. **Obtention d'un code d'activation pour la licence Kaspersky Security Center Cloud Console en mode commercial. Achat d'une licence (ou de licences)**

   Différentes licences permettent d'utiliser différentes applications et différents services Kaspersky, vous pouvez donc envisager d'acheter plus d'une licence.

   Découvrez les licences que vous pouvez acheter et le nombre minimum d'appareils pour chaque licence.

   Kaspersky Security Center Cloud Console fait partie de plusieurs solutions Kaspersky. Choisissez la solution que vous souhaitez utiliser et achetez une licence pour celle-ci. Vous devrez contacter Kaspersky ou l'un des partenaires de Kaspersky avec une demande spéciale si vous souhaitez acheter une licence couvrant 10 000 appareils ou plus.

   Utilisez le tableau pour vérifier les fonctionnalités de la gestion des vulnérabilités et des correctifs disponibles sous chaque licence.

   Si vous souhaitez utiliser Kaspersky Security Center Cloud Console dans un environnement cloud tel que Microsoft Azure, informez-vous sur les options de licence pour les environnements cloud.

   Si vous êtes un prestataire de services gérés (MSP), découvrez les licences de Kaspersky Security Center Cloud Console pour les MSP.

2. **Activation de Kaspersky Security Center Cloud Console lors de la création de l'espace de travail**

   Vous indiquez votre clé de licence pour activer Kaspersky Security Center Cloud Console lors de la création d'un espace de travail.

   Si vous disposez de plusieurs clés de licence, indiquez l'une d'entre elles. Vous devrez ensuite ajouter d'autres clés de licence dans Kaspersky Security Center Cloud Console pour activer les applications Kaspersky administrées.

3. **Ajout de clés de licence pour les applications administrées au stockage du Serveur d'administration**

   Avant le déploiement des clés de licence, vous devez ajouter ces clés de licence au stockage du Serveur d'administration.

   La clé de licence que vous avez indiquée lors de la création de l'espace de travail est automatiquement ajoutée au stockage du Serveur d'administration.

   Si vous avez plusieurs clés de licence, ajoutez vos clés de licence une par une au stockage du Serveur d'administration de Kaspersky Security Center Cloud Console.

4. **Déploiement de clés de licence pour les applications administrées**

   Choisissez une méthode de déploiement de la clé de licence (ou des clés de licence) sur tous les appareils que vous souhaitez protéger :

   - Déploiement automatique

     > Si vous utilisez différentes applications administrées et que vous devez absolument déployer un code d'activation déterminé pour les applications, sélectionnez une autre manière de déployer ce code d'activation.

     Kaspersky Security Center permet automatiquement de diffuser les clés de licence se trouvant sur les applications administrées. Par exemple, le stockage du Serveur d'administration contient trois clés de licence. Vous avez activé l'option **Distribuer automatiquement la clé de licence sur les appareils administrés** pour toutes les trois clés de licence. Sur les appareils de l'entreprise, l'application de sécurité de Kaspersky, par exemple, Kaspersky Endpoint Security for Windows est installée. Une nouvelle application administrée sur un appareil a été détectée pour laquelle il faut diffuser une clé de licence. Par exemple, deux des clés de licence du stockage peuvent être déployées pour l'application administrée sur l'appareil : la clé de licence dénommée *Clé_1* et la clé de licence dénommée *Clé_2*. Une de ces clés de licence est déployée pour l'application administrée. 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, car le déploiement automatique des clés de licence ne prévoit pas l'intervention de l'administrateur.

     Lors du déploiement d'une clé de licence, le nombre d'installations est recalculé pour cette clé. Vous devez vous assurer que le nombre d'applications pour lesquelles la clé de licence a été diffusée ne dépasse pas la restriction de licence. Si le nombre d'installations dépasse la restriction de licence, l'état *Critique* est attribué à tous les appareils non couverts par la licence.

     Instructions pour :

     - Ajout de la clé de licence dans le stockage du Serveur d'administration
     - Diffusion automatique de la clé de licence

   - 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.

     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.

5. **Vérification des appareils sur lesquels les applications Kaspersky administrées sont activées**

   Pour vous assurer que les clés de licence sont correctement déployées, affichez la liste des clés de licence utilisées pour une application.

6. **Configuration des événements liés à l'expiration de la licence**

   Configurez les événements de manière à ce que vous soyez averti lorsque vos clés de licence sont épuisées ou sur le point d'expirer :

   - 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

À propos du mode d'évaluation de Kaspersky Security Center Cloud Console

Le *Mode d'évaluation* est un mode spécial de Kaspersky Security Center Cloud Console destiné à familiariser l'utilisateur avec Kaspersky Security Center Cloud Console. Dans ce mode, vous pouvez effectuer vos activités dans un espace de travail dont la durée d'utilisation est limitée à 30 jours. Le mode d'évaluation est activé automatiquement dès que vous créez un espace de travail d'évaluation. L'ensemble des fonctionnalités disponibles en mode d'évaluation est identique à celui de la licence standard pour Kaspersky Endpoint Security for Business Advanced.

Dans Kaspersky Security Center Cloud Console, vous ne devez pas concéder une licence au Serveur d'administration, car les fonctionnalités qui nécessitent une licence spéciale ne sont pas prises en charge. Si vous souhaitez utiliser Kaspersky Security Center Cloud Console en mode d'évaluation, vous obtenez automatiquement une licence d'évaluation lorsque vous créez votre premier espace de travail.

Le mode d'évaluation ne vous permet pas de passer au mode commercial. Tout espace de travail d'évaluation est automatiquement supprimé ainsi que tout son contenu lorsque la durée d'utilisation de 30 jours a expiré.

L'utilisation des fonctionnalités de Kaspersky Security Center Cloud Console en mode d'évaluation est soumise aux restrictions suivantes :

- Vous ne pouvez pas créer de hiérarchie des Serveurs d'administration. Aucun Serveur d'administration virtuel ne peut être créé.
- La section **Licence** est disponible en lecture seule. Toutes les opérations sont interdites dans cette section, y compris l'ajout et la suppression des clés de licence.
- Vous ne pouvez pas créer de paquets d'installation personnalisés.

- Vous ne pouvez pas créer de rôles personnalisés pour les utilisateurs.
- La fonction Propagation de virus n'est pas disponible. Les événements Propagation de virus ne sont pas stockés et aucune notification n'est envoyée.
- Le stockage des **Objets supprimés** n'est pas disponible.
- Vous ne pouvez pas activer l'ajout d'événements par lots (publiés en grandes quantités) à la base de données.
- La migration des Serveurs d'administration du mode Sur site vers le mode Cloud Console n'est pas prise en charge.
- Les informations sur les statistiques de KSN des composants du Serveur d'administration, comme le Serveur d'administration ou l'Agent d'administration, ne sont pas envoyées à Kaspersky.

Certaines limites sont également imposées à la création de certains objets de l'application (cf. tableau ci-après). Si une de ces limites est dépassée quand une tentative de création d'un tel objet est effectuée, la création de l'objet sera bloquée et un message d'erreur indiquant la limite s'affichera.

Limitations sur la création d'objets Kaspersky Security Center Cloud Console en mode d'évaluation

Type de restriction	Valeur
Stratégies	8
Tâches	17
Clés de licence	1
Paquets d'installation	5
Sélections d'appareils (instances préréglées non incluses)	5
Sélections d'événements (instances préréglées non incluses)	5
Règles de déplacement des appareils	3
Modèles de rapports du même type	10
Groupes de sécurité internes	20
Appareils administrés	20

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 Cloud Console 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.

Licences et nombre minimum d'appareils pour chaque licence

Si vous souhaitez utiliser Kaspersky Security Center Cloud Console en mode commercial, vous devez acheter une licence avant de créer votre premier espace de travail. Le tableau ci-dessous indique les licences que vous pouvez acheter et un nombre minimum d'appareils pour chaque licence (même si vous souhaitez protéger moins d'appareils) :

Licences qui autorisent l'utilisation de Kaspersky Security Center Cloud Console

Licence	Nombre minimum d'appareils (même si vous souhaitez protéger un nombre inférieur)
Kaspersky Endpoint Security for Business Select	Pour les licences commerciales : 300 Pour les licences commerciales (abonnement) : 100
Kaspersky Endpoint Security for Business Advanced	Pour les licences commerciales : 300 Pour les licences commerciales (abonnement) : 100
Kaspersky Total Security for Business	300
Kaspersky Endpoint Detection and Response Optimum	Pour les licences commerciales : 300 Pour les licences commerciales (abonnement) : 100
Kaspersky Endpoint Detection and Response Expert	50
Kaspersky Hybrid Cloud Security, Desktop	Pour les licences commerciales : 300 Pour les licences commerciales (abonnement) : 100
Kaspersky Hybrid Cloud Security, Serveur	50
Kaspersky Hybrid Cloud Security, Noyau	20
Kaspersky Hybrid Cloud Security, Processeur	20
Kaspersky Hybrid Cloud Security Enterprise, Desktop	Pour les licences commerciales : 300 Pour les licences commerciales (abonnement) : 100
Kaspersky Hybrid Cloud Security Enterprise, Serveur	50
Kaspersky Hybrid Cloud Security Enterprise, Processeur	20
Kaspersky Embedded Systems Security	300
Kaspersky Embedded Systems Security Compliance Edition	300
Kaspersky Symphony (actuellement disponible uniquement en Russie)	300
Kaspersky Next EDR Foundations	Pour les licences commerciales : 300 utilisateurs Pour les licences commerciales (abonnement) : 100 utilisateurs Chaque licence utilisateur peut être appliquée à 1 appareil PC/Mac et 2 appareils mobiles.
Kaspersky Next EDR Optimum	Pour les licences commerciales : 300 utilisateurs Pour les licences commerciales (abonnement) : 100 utilisateurs Chaque licence utilisateur peut être appliquée à 1 appareil PC/Mac et 2 appareils mobiles.
Kaspersky Next EDR Expert	250 utilisateurs Chaque licence utilisateur peut être appliquée à 1 appareil PC/Mac et 2 appareils mobiles.
Kaspersky Next XDR Expert	250 utilisateurs Chaque licence utilisateur peut être appliquée à 1 appareil PC/Mac et 2 appareils mobiles.

Si vous souhaitez protéger plus de 10 000 appareils, il faut envoyer une demande au support technique de Kaspersky et indiquer les informations sur votre entreprise et sur l'espace de travail que vous souhaitez créer.

Événements de dépassement de la restriction de licence

Kaspersky Security Center Cloud Console permet d'obtenir des informations sur les événements de dépassement de la restriction de licence des applications Kaspersky installées sur les appareils clients.

Le niveau d'importance des événements de dépassement de la limite de licence est défini conformément aux règles suivantes :

- Si le nombre d'unités de licence utilisées se trouve entre 90 et 100 % du total des unités de licence de cette licence, l'événement avec le niveau d'importance **Information** est publié.
- Si le nombre d'unités de licence utilisées se trouve entre 100 et 110 % du total d'unités de licence de cette licence, l'événement avec le niveau d'importance **Avertissement** est publié.
- Si le nombre d'unités de licence utilisées dépasse 110 % du total d'unités de licence de cette licence, l'événement avec le niveau d'importance **Événement critique** est publié.

Méthodes de distribution des codes d'activation aux appareils administrés

Les applications Kaspersky installées sur les appareils administrés doivent disposer d'une licence sous la forme d'un code d'activation pour chaque application. Vous ne pouvez pas utiliser de fichiers clés pour ajouter des licences à des applications administrées ; seuls les codes d'activation sont acceptés. Le déploiement d'un code d'activation peut s'effectuer comme suit :

- Déploiement automatique
- La tâche Ajout de clé de licence pour une application administrée
- L'activation manuelle d'une application administrée

Les applications Kaspersky peuvent utiliser plusieurs clés de licence en même temps. Par exemple, Kaspersky Endpoint Security for Windows peut utiliser deux clés de licence : une pour Kaspersky Endpoint Security for Windows et une pour l'activation des fonctionnalités Endpoint Detection and Response.

De plus, les applications Kaspersky peuvent avoir non seulement une clé de licence active, mais aussi une clé de licence de réserve. 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. Vous pouvez ajouter une nouvelle clé de licence active ou de réserve par l'une des méthodes répertoriées ci-dessus. 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.

Ajout de la clé de licence du Serveur d'administration

Pour ajouter une clé de licence du Serveur d'administration, procédez comme suit :

1. Dans le menu principal, cliquez sur l'icône des paramètres ( ) à côté du Serveur d'administration.

   La fenêtre des propriétés du Serveur d'administration s'ouvre avec l'onglet **Général** sélectionné.

2. Accédez à **Clés de licence**, puis cliquez sur le bouton **Sélectionner** dans l'une des sections suivantes :

   - **Licence actuelle**, si vous souhaitez ajouter une clé de licence active.
   - **Clé de licence de réserve**, si vous souhaitez ajouter une clé de licence de réserve.

     Vous pouvez ajouter une clé de licence de réserve uniquement si une clé de licence active a déjà été ajoutée.

3. Dans la fenêtre qui s'ouvre, sélectionnez une clé de licence requise dans le tableau.

   Si nécessaire, vous pouvez ajouter une nouvelle clé de licence en cliquant sur le bouton **Ajouter une nouvelle clé de licence**, puis en saisissant la clé de licence dans le volet droit qui s'ouvre.

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

La fenêtre se ferme, la clé de licence du Serveur d'administration est ajoutée, et les informations la concernant s'affichent dans la section **Clés de licence**.

Si nécessaire, vous pouvez modifier la clé de licence sélectionnée en cliquant sur le bouton **Modifier** et en indiquant une autre clé de licence. Vous pouvez également supprimer une clé de licence.

Ajout de la clé de licence dans le stockage du Serveur d'administration

Lors de l'ajout de la clé de licence à l'aide de Kaspersky Security Center Cloud Console, 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.

Pour ajouter une clé de licence dans le stockage du Serveur d'administration, procédez comme suit :

1. Dans le menu principal, accédez à **Opérations → Licence → Licences pour les logiciels de Kaspersky**.
2. Cliquez sur le bouton **Ajouter**.
3. 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 Cloud Console vous permet de distribuer une clé de licence aux appareils clients automatiquement ou via la tâche **Activation de l'application**. Vous pouvez utiliser la tâche pour distribuer des clés à un groupe d'appareils particulier. Lors de la distribution de la clé de licence via la tâche, la limite de licences sur le nombre d'appareils n'est pas prise en compte. La distribution automatique des clés permet d'interrompre automatiquement la distribution d'une clé de licence lorsque la limite de licence est atteinte.

Si vous activez la distribution automatique d'une clé de licence, ne créez pas de tâche **Activation de l'application** pour distribuer cette clé sur les appareils clients. Dans le cas contraire, la charge sur le Serveur d'administration augmentera en raison de la fréquence des synchronisations.

Avant le déploiement, ajoutez une clé de licence au stockage du Serveur d'administration.

*Pour diffuser une clé de licence sur les appareils clients via la tâche **Activation de l'application**, procédez comme suit :*

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Tâches**.
2. Cliquez sur **Ajouter**.

   Ceci permet de lancer l'**Assistant de création d'une tâche**. Parcourez les étapes de l'assistant à l'aide du bouton **Suivant**.
3. Dans la liste déroulante **Application**, sélectionnez l'application pour laquelle vous voulez ajouter une clé de licence.
4. À partir de la liste **Type de tâche**, sélectionnez la tâche **Activation de l'application**.
5. Dans le champ **Nom de la tâche**, indiquez le nom de la nouvelle tâche.
6. Sélectionnez les appareils auxquels les tâches seront affectées.
7. À l'étape **Sélection d'une clé de licence** de l'Assistant, cliquez sur le lien **Ajouter une clé** pour ajouter la clé de licence.
8. Dans le volet de l'ajout de clé, ajoutez la clé de licence à l'aide d'une des options suivantes :

   Il faut ajouter la clé de licence uniquement si vous ne l'avez pas ajoutée au stockage du Serveur d'administration avant la création de la tâche **Activation de l'application**.

   - Sélectionnez l'option **Saisir un code d'activation** pour saisir le code d'activation, puis procédez comme suit :

     a. Indiquez le code d'activation, puis cliquez sur le bouton **Envoyer**.

     Les informations sur la clé de licence apparaissent dans le volet d'ajout de clé.

     b. Cliquez sur le bouton **Enregistrer**.

     Si vous souhaitez diffuser automatiquement la clé de licence sur les appareils administrés, activez l'option **Distribuer automatiquement la clé de licence sur les appareils administrés**.

     La fenêtre d'ajout de clés se ferme.

   - Sélectionnez l'option **Ajouter un fichier clé** pour ajouter un fichier clé, puis procédez comme suit :

     a. Cliquez sur le bouton **Sélectionner le fichier clé**.

     b. Dans la fenêtre qui s'ouvre, sélectionnez un fichier clé, puis cliquez sur le bouton **Ouvrir**.

     Les informations sur la clé de licence apparaissent dans le volet d'ajout d'une clé de licence.

     c. Cliquez sur le bouton **Enregistrer**.

     Si vous souhaitez diffuser automatiquement la clé de licence sur les appareils administrés, activez l'option **Distribuer automatiquement la clé de licence sur les appareils administrés**.

     La fenêtre d'ajout de clés se ferme.
9. Sélectionnez la clé de licence dans le tableau des clés.

10. À l'étape **Informations sur la licence** de l'Assistant, décochez la case par défaut **Utiliser comme clé de réserve** si vous souhaitez remplacer la clé de licence active.

    Par exemple, cela est nécessaire lorsque l'organisation change et que la clé d'une autre organisation est requise sur l'appareil, ou si la clé a été réémise et qu'une nouvelle licence expire avant la licence actuelle. Pour éviter les erreurs, il convient de décocher la case **Utiliser comme clé de réserve**.

    Si vous souhaitez en savoir plus sur les problèmes qui peuvent survenir lors de l'ajout d'une clé de licence à Kaspersky Security Center et les moyens de les résoudre, consultez la Base de connaissances de Kaspersky Security Center.

11. À l'étape **Fin de la création de la tâche** de l'Assistant, activez l'option **Ouvrir les détails de la tâche à la fin de la création** pour modifier les paramètres de la tâche par défaut.

    Si vous n'activez pas cette tâche, la tâche sera créée selon les paramètres par défaut. Vous pourrez modifier ces paramètres par défaut plus tard.

12. Cliquez sur le bouton **Terminer**.

    L'Assistant crée la tâche. Si vous avez activé l'option **Ouvrir les détails de la tâche à la fin de la création**, la fenêtre des propriétés de la tâche s'ouvre automatiquement. Cette fenêtre permet de définir les paramètres généraux de la tâche et, si nécessaire, de modifier les paramètres définis lors de la création de la tâche.

    > Vous pouvez également ouvrir la fenêtre des propriétés de la tâche en cliquant sur le nom de la tâche créée dans la liste des tâches.

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

13. Pour exécuter la tâche, sélectionnez-la dans la liste des tâches, puis cliquez sur le bouton **Démarrer**.

    Vous pouvez également programmer le lancement d'une tâche dans l'onglet **Programmation** de la fenêtre des propriétés de la tâche.

    Pour obtenir la description détaillée des paramètres du lancement programmé, consultez les paramètres généraux de la tâche.

Une fois la tâche terminée, la clé de licence est déployée sur les appareils sélectionnés.

Diffusion automatique de la clé de licence

Kaspersky Security Center Cloud Console permet de diffuser automatiquement sur les appareils administrés les clés de licence placées dans le stockage des clés sur le Serveur d'administration.

Afin de diffuser automatiquement une clé de licence sur les appareils administrés, procédez comme suit :

1. Dans le menu principal, accédez à **Opérations** → **Licence** → **Licences pour les logiciels de Kaspersky**.
2. Sélectionnez la clé de licence que vous souhaitez diffuser automatiquement sur l'appareil.
3. Dans la fenêtre ouverte des propriétés de la clé de licence, placez le commutateur sur **Distribuer automatiquement la clé de licence sur les appareils administrés**.
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 licence est définie dans les propriétés de la clé de licence. Si la limite liée à la restriction de licence est atteinte, la diffusion de la clé de licence sur les appareils s'arrête automatiquement.

Veuillez noter qu'une clé de licence diffusée automatiquement peut ne pas s'afficher dans le stockage du Serveur d'Administration virtuel dans les cas suivants :

- La clé de licence n'est pas valide pour l'application.
- Le Serveur d'administration virtuel n'a pas d'appareils administrés.
- La clé de licence a déjà été utilisée pour des appareils administrés par un autre Serveur d'administration virtuel et la limite du nombre d'appareils a été atteinte.

Si vous indiquez l'option **Distribuer automatiquement la clé de licence sur les appareils administrés** pour une clé de licence d'abonnement dans le but d'activer une application sur un appareil administré et que vous disposez parallèlement d'une clé de licence d'essai active, votre clé de licence d'essai sera automatiquement remplacée par la clé de licence d'abonnement huit jours avant la date d'expiration.

Affichage des informations sur les clés de licence utilisées dans le stockage du Serveur d'administration

Pour voir la liste des clés de licence ajoutées au stockage du serveur d'administration,

Dans le menu principal, accédez à **Opérations → Licence → Licences pour les logiciels de Kaspersky**.

La liste affichée contient les codes d'activation ajoutés au stockage du serveur d'administration.

Pour voir les informations détaillées d'une clé de licence :

1. Dans le menu principal, accédez à **Opérations → Licence → Licences pour les logiciels de Kaspersky**.
2. Cliquez sur le nom de la clé de licence concernée.

Dans la fenêtre des propriétés de la clé de licence qui s'ouvre, vous pouvez voir :

- Dans l'onglet **Général**, les principales informations sur la clé de licence
- Dans l'onglet **Appareils**, la liste des appareils clients où la clé de licence a été utilisée pour l'activation de l'application Kaspersky installée

Affichage des informations sur les clés de licence utilisées pour une application Kaspersky particulière

Pour découvrir les clés de licence utilisées pour une application Kaspersky, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Appareils administrés**.

   Si l'appareil appartient au groupe Appareils non définis, accédez au lieu de cela 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 la section **Applications**.

4. Dans la liste des applications qui s'ouvre, sélectionnez celle dont vous souhaitez afficher les clés de licence.

5. Dans la fenêtre des propriétés du Serveur d'administration qui s'ouvre, sous l'onglet **Généralités**, sélectionnez la section **Clés de licence**.

   Les informations sont affichées dans l'espace de travail de cette section.

Suppression de la clé de licence du Serveur d'administration

Pour supprimer une clé de licence du Serveur d'administration, procédez comme suit :

1. Dans le menu principal, cliquez sur l'icône des paramètres ( ) à côté du Serveur d'administration.

2. Dans la fenêtre des propriétés du Serveur d'administration qui s'ouvre, sélectionnez la section **Clés de licence**.

3. Cliquez sur le bouton **Supprimer la clé de licence active** ou **Supprimer la clé de licence de réserve** en fonction de la clé de licence que vous souhaitez supprimer, puis confirmez l'opération dans la fenêtre qui s'ouvre.

Ceci supprime la clé de licence.

Si une clé de licence de réserve a été ajoutée, la clé de licence de réserve devient automatiquement la clé de licence active après la suppression de l'ancienne clé de licence active.

Suite à la suppression de la clé de licence active, les fonctions Gestion des vulnérabilités et des correctifs et Administration des appareils mobiles ne seront plus accessibles au Serveur d'administration. Vous pouvez ajouter de nouveau la clé de licence supprimée ou ajouter une autre clé de licence.

Suppression d'une clé de licence du stockage

Vous pouvez supprimer une clé de licence du stockage du Serveur d'administration. Notez que Kaspersky Security Center Cloud Console supprime automatiquement votre espace de travail après 90 jours dans les cas suivants :

- Vous supprimez la dernière clé de licence (active, réservée ou non utilisée) ajoutée manuellement dans le stockage.

- La dernière clé de licence expire.

Si votre espace de travail est supprimé, vous ne pouvez plus administrer la protection de votre réseau à l'aide de Kaspersky Security Center Cloud Console. Vous perdez également définitivement vos données de Kaspersky Security Center Cloud Console. Si nécessaire, vous pouvez supprimer votre espace de travail manuellement. Sinon, nous vous recommandons de conserver au moins une clé de licence dans le stockage du Serveur d'administration.

Si vous supprimez une clé de licence et que vous avez ajouté une clé de licence de réserve plus tôt, la clé de licence de réserve devient automatiquement la clé de licence active après la suppression ou l'expiration de l'ancienne clé active.

Lorsque vous supprimez la clé de licence active, qui est déployée sur un appareil administré, l'application continue de fonctionner sur cet appareil administré.

Pour supprimer une clé de licence du stockage du Serveur d'administration, procédez comme suit :

1. Vérifiez que le Serveur d'administration n'utilise pas une clé de licence que vous souhaitez supprimer. Si le Serveur d'administration le fait, vous ne pouvez pas supprimer la clé. Pour effectuer le contrôle :

   a. Dans le menu principal, cliquez sur l'icône des paramètres ( ) à côté du Serveur d'administration.

   La fenêtre des propriétés du Serveur d'administration s'ouvre.

   b. Sous l'onglet **Général**, sélectionnez la section **Clés de licence**.

   c. Si la clé de licence requise 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 la clé de licence requise ne s'affiche pas, le Serveur d'administration ne l'utilise pas.

2. Dans le menu principal, accédez à **Opérations** → **Licence** → **Licences pour les logiciels de Kaspersky**.

3. Sélectionnez la clé de licence requise, puis cliquez sur le bouton **Supprimer ;**.

4. Dans la fenêtre qui s'affiche, cochez la case **Je comprends le risque et je veux supprimer la clé de licence**. Cela signifie que si vous supprimez la dernière clé de licence, vous êtes conscient de la suppression ultérieure de l'espace de travail et de la perte de contrôle sur les appareils administrés. Ensuite, cliquez sur le bouton **Supprimer**.

Par conséquent, la clé de licence sélectionnée est supprimée du stockage.

Vous pouvez ajouter de nouveau la clé de licence supprimée ou ajouter une autre clé de licence. Si vous avez supprimé la dernière clé de licence, vous pouvez également ajouter une clé de licence tant que votre espace de travail n'est pas supprimé. Kaspersky Security Center Cloud Console informe les administrateurs de l'espace de travail 30 jours, 7 jours et 1 jour avant la suppression.

Affichage de la liste des appareils sur lesquels aucune application Kaspersky n'est activée

Vous pouvez afficher la liste de tous les appareils sur lesquels une application Kaspersky est installée, mais pas activée (par exemple, une licence est manquante ou a expiré).

Pour afficher les appareils sur lesquels une application Kaspersky n'est pas activée, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Tâches**.

   La liste des tâches s'affiche.

2. Cliquez sur le nom de la tâche de mise à jour liée à l'application Kaspersky en question.

   La fenêtre des propriétés de la tâche s'affiche avec plusieurs onglets nommés.

3. Dans la fenêtre des propriétés des tâches, sélectionnez la section **Résultats**.

   La colonne **Appareil ou Serveur secondaire** affiche les appareils sur lesquels la tâche a réussi.

4. Triez la colonne **Appareil ou Serveur secondaire**.

   La colonne **Appareil ou Serveur secondaire** affiche les appareils sur lesquels la tâche a réussi. Les appareils sur lesquels la tâche a échoué en raison d'une licence manquante sont les appareils sur lesquels l'application n'est pas activée.

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 ainsi que ses paquets d'installation avant de révoquer son CLUF. Les paquets d'installation doivent être supprimés du Serveur d'administration et de ses Serveurs d'administration virtuels.

Les CLUF qui ont été acceptés sur un Serveur d'administration virtuel peuvent être révoqués sur le Serveur d'administration virtuel ou sur le Serveur d'administration principal. Les CLUF qui ont été acceptés sur un Serveur d'administration principal ne peuvent être révoqués que sur le Serveur d'administration principal.

Pour révoquer un CLUF pour les applications Kaspersky administrées :

1. Dans le menu principal, cliquez sur l'icône des paramètres ( ) en regard du nom du Serveur d'administration requis.

   La fenêtre des propriétés du Serveur d'administration s'ouvre.

2. Sous l'onglet **Général** de la fenêtre des propriétés du Serveur d'administration, choisissez la section **Contrats de licence utilisateur final**.

   Une liste des CLUF acceptés s'affiche lors de la création des paquets d'installation ou lors de l'installation transparente des mises à jour.

3. 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
   - Si le CLUF peut être révoqué ou non

4. 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) liés au CLUF et leurs noms et types respectifs

5. Dans la partie inférieure de la fenêtre des propriétés du CLUF, cliquez sur le bouton **Révoquer le Contrat de licence**.

   Si le CLUF sélectionné ne peut être révoqué qu'en désinstallant l'application ou si ce CLUF ne peut être révoqué que sur le Serveur d'administration principal, une notification de cette restriction s'affiche à la place du 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.

6. 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).

Si la dernière clé de licence a expiré, Kaspersky Security Center Cloud Console supprime automatiquement votre espace de travail au bout de 90 jours. Par conséquent, vous ne pouvez pas administrer la protection de votre réseau à l'aide de Kaspersky Security Center Cloud Console. Vous perdez également définitivement vos données de Kaspersky Security Center Cloud Console. Nous vous recommandons de renouveler les clés de licence obsolètes ou d'en ajouter de nouvelles dans le stockage du Serveur d'administration pour conserver votre espace de travail.

Pour afficher une notification concernant une licence expirée ou une licence sur le point d'expirer :

1. Réalisez une des opérations suivantes :

   - Dans le menu principal, accédez à **Opérations → Licence → Licences pour les logiciels de Kaspersky**.
   - Dans le menu principal, accédez à **Surveillance et rapports → Tableau de bord**, puis cliquez sur le lien **Afficher les licences arrivant à expiration** à côté d'une notification.

   La fenêtre **Licences pour les logiciels de Kaspersky** s'ouvre, dans laquelle vous pouvez afficher et renouveler les licences expirées ou sur le point d'expirer.

2. Si vous souhaitez renouveler une licence, cliquez sur le lien **Renouveler la licence** à côté de la licence requise.

   En cliquant sur un lien de renouvellement de licence, vous acceptez de transférer les données suivantes vers Kaspersky : ID du logiciel, version du logiciel, localisation du logiciel, ID de licence et un attribut indiquant si la licence a été fournie par une entreprise partenaire. Les données sont nécessaires pour déterminer les conditions de renouvellement de votre licence.

3. Dans la fenêtre du service de renouvellement de licence qui s'ouvre, suivez les instructions pour renouveler une licence.

   La licence qui expire est renouvelée.

Dans Kaspersky Security Center Cloud 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 Kaspersky Security Center Cloud Console après expiration de la licence

Après l'expiration de la licence, Kaspersky peut vous permettre d'utiliser Kaspersky Security Center Cloud Console pendant 90 jours maximum sans limitation. Pendant cette période, le Serveur d'administration, l'Agent d'administration et l'interface Web de Kaspersky Security Center Cloud Console fonctionnent sans restriction. Kaspersky Security Center Cloud Console envoie également des statistiques KSN à Kaspersky conformément aux paramètres d'accès KSN en vigueur. Les applications administrées fonctionnent avec des fonctionnalités limitées (pour plus de détails, consultez la documentation de ces applications).

Une fois la licence expirée depuis 90 jours, Kaspersky Security Center Cloud Console supprime automatiquement votre espace de travail. Si vous souhaitez conserver l'espace de travail, renouvelez au moins une clé de licence expirée ou ajoutez-en une nouvelle dans le stockage.

Définitions des licences

Cette section contient des définitions pour les concepts relatifs aux licences des applications Kaspersky administrées via Kaspersky Security Center Cloud Console.

À propos de la licence

La *licence* est un droit d'utilisation limité dans le temps de Kaspersky Security Center Cloud Console, 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, Kaspersky Security Center Cloud Console cesse de remplir toutes ces fonctions. Pour continuer à utiliser l'application, vous devez acheter une licence commerciale.

Vous pouvez utiliser l'application à l'aide d'une licence d'évaluation pendant une seule période d'évaluation.

- *Commerciale*

  Une licence payante.

  À l'expiration de la licence commerciale, les fonctionnalités clés de l'application sont désactivées. Pour continuer à utiliser Kaspersky Security Center Cloud Console, il faut renouveler la licence commerciale. Après l'expiration de la licence commerciale, vous ne pouvez plus utiliser l'application et vous devez la supprimer de votre appareil.

  Il est conseillé de renouveler votre licence avant son expiration, pour garantir une protection ininterrompue contre toutes les menaces de sécurité.

À propos du certificat de licence

Le *certificat de licence* est un document qui vous est transmis avec le fichier clé ou le code d'activation.

Il comporte les informations suivantes à propos de la licence :

- Clé de licence ou numéro de commande
- informations relatives à l'utilisateur qui reçoit la licence
- informations relatives à l'application qui peut être activée à l'aide de la licence
- restrictions associées au nombre d'unités concernées par la licence (par exemple, le nombre d'appareils sur lesquels l'application peut être utilisée avec la licence)
- début de durée de validité de la licence
- date de fin de la durée de validité de la licence ou durée de validité de la licence
- type de licence

À propos de la clé de licence

Une *clé de licence* est une séquence de caractères qui vous permet d'activer puis d'utiliser l'application conformément aux conditions du Contrat de licence utilisateur final. Les clés de licence sont créées par les experts de Kaspersky.

Vous pouvez ajouter une clé de licence à l'application en saisissant un *code d'activation*. Une fois ajoutée, la clé de licence s'affiche dans l'interface de l'application sous la forme d'une séquence alphanumérique unique.

La clé de licence peut être bloquée par Kaspersky en cas de non-respect des conditions du Contrat de licence. Si la clé de licence est bloquée, vous devez ajouter une autre clé pour pouvoir utiliser l'application.

Une clé de licence peut être active ou complémentaire (ou de réserve).

Une *clé de licence active* est une clé actuellement utilisée par l'application. Une clé de licence active peut être ajoutée pour une licence d'évaluation ou commerciale. Il ne peut pas y avoir plus d'une clé de licence active par application.

Une *clé de licence complémentaire (ou de réserve)* est une clé de licence qui permet à l'utilisateur d'utiliser l'application, mais qui n'est pas active. La clé de licence complémentaire est automatiquement active si la validité de la licence associée à la clé de licence active expire. Une clé de licence complémentaire ne peut être ajoutée que si une clé de licence active a déjà été ajoutée.

Une clé de licence d'évaluation ne peut être ajoutée qu'en tant que clé de licence active. Une clé de licence d'essai ne sera pas acceptée comme clé de licence complémentaire.

À propos du code d'activation

Le *code d'activation* est une suite unique de 20 caractères alphanumériques. Vous le saisissez pour ajouter une clé de licence activant Kaspersky Security Center Cloud Console. Vous recevez le code d'activation à l'adresse email que vous avez indiquée après l'achat de Kaspersky Security Center Cloud Console ou après la commande d'une version d'essai de Kaspersky Security Center Cloud Console.

Pour activer l'application à l'aide du code d'activation, vous avez besoin d'un accès Internet pour vous connecter aux serveurs d'activation de Kaspersky. Si l'accès aux serveurs via le DNS système n'est pas possible, l'application utilise les serveurs DNS publics.

Si l'application a été activée à l'aide d'un code d'activation, dans certains cas après l'activation, l'application envoie des requêtes régulières au serveur d'activation de Kaspersky pour vérifier le statut de la clé de licence. Pour pouvoir envoyer des requêtes, vous devez fournir un accès Internet pour l'application.

Si vous avez perdu votre code d'activation après l'installation de l'application, contactez le partenaire Kaspersky auprès duquel vous avez acheté la licence.

Vous ne pouvez pas utiliser de fichiers clés pour activer des applications administrées ; seuls les codes d'activation sont acceptés.

À propos de l'abonnement

Abonnement à Kaspersky Security Center Cloud Console 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 Cloud Console peut être enregistré auprès du prestataire 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 Cloud Console 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 prestataire 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 prestataire de services détermine l'existence et la durée de la période de grâce.

L'utilisation de Kaspersky Security Center Cloud Console sur abonnement nécessite l'application d'un code d'activation communiqué par le prestataire de services.

Vous pouvez appliquer un autre code d'activation pour l'utilisation de Kaspersky Security Center Cloud Console 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 prestataire 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 Cloud Console.

Lors de l'utilisation de l'application sur abonnement, Kaspersky Security Center Cloud Console s'adresse automatiquement au serveur d'activation dans un laps de temps déterminé jusqu'à la date de fin de l'abonnement. Si l'accès au serveur via le DNS système n'est pas possible, l'application utilise les serveurs DNS publics. Vous pouvez prolonger l'abonnement sur le site Internet du prestataire de services.

À propos des données

Kaspersky Security Center Cloud Console permet à l'utilisateur d'identifier et de contrôler des appareils (et les propriétaires de ces appareils) connectés à Kaspersky Security Center Cloud Console, au moyen des fonctionnalités d'applications administrées.

Méthodes de collecte de données :

1. L'utilisateur saisit les données dans l'interface Kaspersky Security Center Cloud Console.
2. L'Agent d'administration reçoit les données de l'appareil et les transfère au Serveur d'administration.
3. L'Agent d'administration reçoit les données récupérées par l'application administrée Kaspersky et les transfère au Serveur d'administration. La liste des données traitées par les applications Kaspersky administrées est fournie dans l'Aide des applications correspondantes.
4. Les données sont transférées à partir des Serveurs d'administration secondaires exécutés sur site.

Kaspersky Security Center Cloud Console supprime automatiquement les espaces de travail 30 jours après l'expiration de la licence de la période d'essai et 90 jours après la fin de la durée de validité de la licence commerciale.

Après l'expiration de la durée de validité de la licence, Kaspersky enregistre les données de l'utilisateur relatives aux alertes et aux incidents dans les espaces de travail de l'utilisateur pendant 30 jours.

Sous la licence actuelle, la durée de conservation des alertes et des incidents est de 360 jours. Passé ce délai, les alertes les plus anciennes et les incidents les plus anciens sont automatiquement supprimés.

La suppression définitive des données répertoriées dans cette section peut prendre jusqu'à 24 heures.

Données envoyées aux serveurs Kaspersky

Données envoyées lors de l'activation

Lors de l'utilisation du code d'activation pour activer le Logiciel, afin de vérifier la légitimité de l'utilisation du logiciel, l'utilisateur s'engage à fournir périodiquement à Kaspersky les informations suivantes :

- Code d'activation
- Identifiant d'activation unique pour la licence actuelle

Kaspersky peut également utiliser ces informations pour générer des informations statistiques sur la distribution et l'utilisation du logiciel Kaspersky.

Données envoyées lors de la mise à jour

Dès réception des mises à jour des serveurs de mises à jour du Détenteur des droits, afin d'améliorer la qualité du mécanisme de mise à jour, l'utilisateur s'engage à fournir périodiquement les informations suivantes à Kaspersky :

- Identifiant de logiciel reçu de la licence

- Version complète du logiciel
- ID de licence de logiciel
- Identifiant d'installation du logiciel (PCID)
- ID du démarrage de la mise à jour du logiciel

Kaspersky peut également utiliser ces informations pour générer des informations statistiques sur la distribution et l'utilisation du logiciel Kaspersky.

Données permettant d'assurer un fonctionnement ininterrompu, un travail efficace et de vérifier l'utilisation légitime de Kaspersky Security Center Cloud Console

Les informations suivantes peuvent être utilisées dans le but spécifié :

- Noms et versions des applications de sécurité de Kaspersky connectées à l'espace de travail, et nombre d'appareils sur lesquels ces applications de sécurité sont installées.
- Nombre d'appareils avec les applications de sécurité Kaspersky installées qui ont été connectés à tous les espaces de travail et répartition de ces appareils connectés par type.
- Identifiant de l'espace de travail, identifiant de l'entreprise, pays et région de l'espace de travail, et date de création de l'espace de travail.
- Nombre d'utilisateurs dans l'espace de travail, date de la dernière authentification dans l'espace de travail.
- Informations sur la licence actuellement utilisée (type de licence, restriction de la licence par rapport au nombre d'appareils, nombre d'appareils connectés, date d'expiration de la licence précédemment utilisée).

Données transférées en suivant les liens dans l'interface de la Kaspersky Security Center Cloud Console

En suivant les liens de la Console d'administration ou de Kaspersky Security Center Cloud Console, l'utilisateur accepte le transfert automatique des données suivantes :

- Localisation de la Kaspersky Security Center Cloud Console
- ID 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.

Données nécessaires au fonctionnement de l'espace de travail

Kaspersky Security Center Cloud Console traite les données suivantes :

1. Détails relatifs aux appareils détectés sur le réseau d'entreprise

   L'agent d'administration reçoit les données répertoriées ci-après des appareils connectés au réseau et les transfère vers le serveur d'administration :

a. Spécifications techniques de l'appareil détecté et de ses composants nécessaires à l'identification de l'appareil qui ont été reçues au moyen d'un sondage du réseau :

- Sondage Active Directory :

  Appareils Active Directory : nom unique de l'appareil ; nom du domaine Windows reçu du contrôleur de domaine ; nom de l'appareil dans l'environnement Windows ; nom de domaine NetBIOS ; domaine DNS et nom DNS de l'appareil ; compte du gestionnaire des comptes de sécurité (SAM) (nom pour la connexion au système utilisé pour le support des clients et des serveurs utilisant des versions antérieures du système d'exploitation, telles que Windows NT 4.0, Windows 95, Windows 98 et LAN Manager) ; nom unique du domaine ; noms uniques des groupes auxquels appartient l'appareil ; nom unique de l'utilisateur qui administre l'appareil ; identificateur global unique (GUID) et GUID parent de l'appareil.

  Lorsque le réseau Active Directory est sondé, les types de données suivants sont également traités afin d'afficher des informations concernant l'infrastructure administrée et l'utilisation de ces informations par l'utilisateur, par exemple pendant le déploiement de la protection :

- Unités organisationnelles Active Directory : nom unique de l'unité organisationnelle ; nom unique du domaine ; GUID et GUID parent de l'unité organisationnelle.

- Domaines Active Directory : nom du domaine Windows reçu du contrôleur de domaine ; domaine DNS ; GUID du domaine.

- Utilisateurs Active Directory : nom d'affichage de l'utilisateur ; nom unique de l'utilisateur ; nom unique du domaine ; nom de l'organisation de l'utilisateur ; nom du département où l'utilisateur travaille ; nom unique d'un autre utilisateur agissant en tant que gestionnaire de l'utilisateur ; nom complet de l'utilisateur ; compte SAM ; adresse email ; adresse email alternative ; numéro de téléphone principal ; numéro de téléphone alternatif ; numéro de téléphone portable ; nom de la position de l'utilisateur ; noms uniques des groupes auxquels appartient l'utilisateur ; identificateur global unique de l'utilisateur (GUID) ; identifiant de sécurité de l'utilisateur (SID) (valeur binaire unique utilisée pour identifier l'utilisateur en tant qu'utilisateur principal de sécurité) ; et nom principal de l'utilisateur principal (UPN) : nom d'utilisateur de type Internet pour un utilisateur basé sur la norme Internet RFC 822. L'UPN est plus court que le nom distinctif et plus facile à retenir. Par convention, l'UPN mappe vers le nom de l'adresse email de l'utilisateur.

- Groupes Active Directory : nom unique du groupe ; adresse email ; nom unique du domaine ; compte SAM ; noms uniques des autres groupes auxquels le groupe appartient ; groupe SID ; GUID du groupe.

b. Sondage du domaine Samba :

Appareils Samba : nom unique de l'appareil ; nom de domaine obtenu du contrôleur de domaine ; nom de l'appareil NetBIOS ; nom de domaine NetBIOS ; domaine DNS et nom DNS de l'appareil ; compte du gestionnaire des comptes de sécurité (SAM) ; nom unique du domaine ; noms uniques des groupes auxquels appartient l'appareil ; nom unique de l'utilisateur qui administre l'appareil ; identificateur global unique (GUID) et GUID parent de l'appareil.

- Unités d'organisation Samba : nom unique de l'unité organisationnelle ; nom unique du domaine ; GUID et GUID parent de l'unité organisationnelle.

- Domaine Samba : nom du domaine Windows reçu du contrôleur de domaine ; domaine DNS ; GUID du domaine.

- Utilisateurs Samba : nom d'affichage de l'utilisateur ; nom unique de l'utilisateur ; organisation de l'utilisateur ; nom du département où l'utilisateur travaille ; nom unique d'un autre utilisateur agissant en tant que gestionnaire de l'utilisateur ; nom complet de l'utilisateur ; compte SAM ; adresse email ; adresse email alternative ; numéro de téléphone principal ; numéro de téléphone alternatif ; numéro de téléphone portable ; nom de la position de l'utilisateur ; noms uniques des groupes auxquels appartient l'utilisateur ; identificateur global unique de l'utilisateur (GUID) ; identifiant de sécurité de l'utilisateur (SID) (valeur binaire unique utilisée pour identifier l'utilisateur en tant qu'utilisateur principal de sécurité) ; nom principal de l'utilisateur principal (UPN) : nom d'utilisateur de type Internet pour un utilisateur basé sur la norme

Internet RFC 822. L'UPN est plus court que le nom distinctif et plus facile à retenir. Par convention, l'UPN mappe vers le nom de l'adresse email de l'utilisateur.

- Groupes Samba : nom unique du groupe ; adresse email ; nom unique du domaine ; compte SAM ; noms uniques des autres groupes auxquels le groupe appartient ; groupe SID ; GUID du groupe.

c. Sondage du domaine Windows :

- Nom du domaine ou du groupe de travail Windows
- Nom NetBIOS de l'appareil
- Domaine DNS et nom DNS de l'appareil
- Nom et description de l'appareil
- Visibilité de l'appareil sur le réseau
- Adresse IP de l'appareil
- Type d'appareil (poste de travail, serveur, serveur SQL, contrôleur de domaine, etc.)
- Type de système d'exploitation sur l'appareil
- Version du système d'exploitation de l'appareil
- Date et heure de la dernière mise à jour des informations sur l'appareil
- Date et heure de la dernière fois où l'appareil a été visible sur le réseau

d. Sondage des plages IP :

- Adresse IP de l'appareil
- Nom DNS ou nom NetBIOS de l'appareil
- Nom et description de l'appareil
- Adresse MAC de l'appareil
- Date et heure de la dernière fois où l'appareil a été visible sur le réseau

2. 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 Cloud Console :

a. Caractéristiques techniques de l'appareil administré et ses composants qui sont requis en vue de l'identification de l'appareil :

- Nom affiché (généré sur la base du nom NetBIOS, susceptible d'être modifié manuellement) et description de l'appareil (saisie manuellement)
- Nom et type du domaine Windows (domaine Windows NT/groupe de travail Windows)
- Nom de l'appareil dans l'environnement Windows

- Domaine DNS et nom DNS de l'appareil
- Adresse IP de l'appareil
- Masque de sous-réseau de l'appareil
- Emplacement réseau de l'appareil
- Adresse MAC de l'appareil
- Numéro de série de l'appareil (le cas échéant)
- Type de système d'exploitation sur l'appareil
- Indique si l'appareil est une machine virtuelle quel est le type d'hyperviseur
- Indique si l'appareil est une machine virtuelle dynamique membre d'une Virtual Desktop Infrastructure (VDI)
- GUID de l'appareil
- Identifiant de l'instance de l'agent d'administration
- Identifiant d'installation de l'Agent d'administration
- Identifiant permanent de l'agent d'administration

b. Autres caractéristiques des appareils administrés et leurs composants qui sont requis pour auditer les appareils administrés et décider si des correctifs et mises à jour spécifiques sont applicables :

- État de l'Agent de mises à jour Windows
- 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 : type de machine virtuelle
- Temps d'attente de réponse de l'appareil
- Si l'agent d'administration s'exécute en mode autonome

c. Informations détaillées sur l'activité sur les appareils administrés :

- Date et heure de la dernière mise à jour
- Date et heure où l'appareil a été visible sur le réseau pour la dernière fois
- État d'attente de redémarrage (" Redémarrage requis. ")

- Heure d'activation de l'appareil

d. Détails des comptes utilisateurs de l'appareil et de leurs sessions de travail

e. Statistiques sur le fonctionnement en tant que point de distribution si l'appareil en est un :

- Date et heure de création du point de distribution
- Nom du dossier de travail
- Taille du dossier de travail
- Nombre de synchronisations avec le serveur d'administration
- Date et heure de la dernière synchronisation de l'appareil avec le serveur d'administration
- Nombre et taille totale des fichiers transférés
- Nombre et taille totale des fichiers téléchargés par les clients
- Volume de données téléchargées par les clients via TCP (Transmission Control Protocol)
- Volume de données envoyées aux clients via multidiffusion
- Volume de données téléchargées par les clients via multidiffusion
- Nombre de distributions via multidiffusion
- Volume total de distribution via multidiffusion
- Nombre de synchronisations avec les clients depuis la dernière synchronisation avec le serveur d'administration

f. Nom du Serveur d'administration virtuel qui administre cet appareil

g. Détails relatifs aux appareils Cloud :

- Région du cloud
- Cloud privé virtuel (VPC)
- Zone de disponibilité du cloud
- Sous-réseau du cloud
- Groupe de placement Cloud

h. Détails relatifs aux appareils mobiles. L'application administrée transfère ces données de l'appareil mobile vers le Serveur d'administration. La liste complète des données est disponible dans la documentation de l'application administrée.

3. 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 :

a. Applications administrées de Kaspersky et composants de Kaspersky Security Center Cloud Console installés sur l'appareil

b. Paramètres de l'application Kaspersky installée 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 dont la désinfection a échoué
- Tâches pour l'application de sécurité de Kaspersky
- Disponibilité et état des composants de l'application
- Heure de la dernière mise à jour et version des bases antivirus
- Détails des paramètres de l'application Kaspersky
- Informations relatives aux clés de licence active
- Informations relatives aux clés de licence de réserve
- Date d'installation de l'application
- Identifiant d'installation de l'application

c. Statistiques sur le fonctionnement de l'application : événements liés aux modifications de l'état des composants de l'application de Kaspersky sur l'appareil administré et aux performances des tâches lancées par les composants de l'application

d. État de l'appareil défini par l'application Kaspersky

e. Tags attribués par l'application Kaspersky

f. Ensemble de mises à jour installées et applicables pour l'application Kaspersky :

- Nom affiché, version et langue de l'application
- Nom interne de l'application
- Nom et version de l'application d'après la clé de registre
- Dossier d'installation de l'application
- Version de correctif
- Liste des correctifs automatiques de l'application installés
- Si l'application est prise en charge par Kaspersky Security Center Cloud Console

- Si l'application est installée sur un cluster

g. Détails des erreurs de chiffrement des données sur les appareils : identifiant d'erreur, heure de l'occurrence, type d'opération (chiffrement/déchiffrement), description de l'erreur, chemin d'accès au fichier, description de la règle de chiffrement, identifiant de l'appareil et nom d'utilisateur

4. Événements des composants Kaspersky Security Center Cloud Console et des applications administrées par Kaspersky.

   L'Agent d'administration transfère les données de l'appareil vers le Serveur d'administration.

   La description d'un événement peut contenir les données suivantes :

   a. Nom de l'appareil

   b. Nom d'utilisateur de l'appareil

   c. Nom de l'administrateur qui s'est connecté à l'appareil à distance

   d. Nom, version et prestataire de l'application installée sur l'appareil

   e. Chemin du dossier d'installation de l'application sur l'appareil

   f. Chemin vers le fichier sur l'appareil et nom du fichier

   g. Nom de l'application et paramètres de la ligne de commande sous laquelle l'application a été exécutée

   h. Nom du correctif, nom du fichier du correctif, identifiant du correctif, niveau de la vulnérabilité corrigée par le correctif, description de l'erreur d'installation du correctif

   i. Adresse IP de l'appareil

   j. Adresse MAC de l'appareil

   k. État de redémarrage de l'appareil

   l. Nom de la tâche qui a publié l'événement

   m. Si l'appareil a basculé en mode autonome et le motif de ce basculement

   n. Informations relatives au problème de sécurité sur l'appareil : type et nom du problème de sécurité, niveau de gravité, description du problème de sécurité et caractéristiques du problème de sécurité transmises par l'application Kaspersky

   o. Espace disque disponible sur l'appareil

   p. Si l'application Kaspersky s'exécute en mode limité, les ID des zone de fonction

   q. Ancienne et nouvelle valeur du paramètre de l'application Kaspersky

   r. Description de l'erreur rencontrée lorsque l'application Kaspersky ou l'un de ses composants a effectué l'opération

5. Paramètres des composants Kaspersky Security Center Cloud Console et des applications administrées par Kaspersky présentés dans les stratégies et les profils de stratégie.

   L'utilisateur saisit les données dans l'interface Kaspersky Security Center Cloud Console.

6. Paramètres des tâches des composants Kaspersky Security Center Cloud Console et des applications administrées par Kaspersky

   L'utilisateur saisit les données dans l'interface Kaspersky Security Center Cloud Console.

7. Données traitées par la fonction de la gestion des vulnérabilités et des correctifs.

   L'Agent d'administration transfère les données répertoriées ci-dessous de l'appareil vers le Serveur d'administration :

   a. Détails relatifs aux applications et aux correctifs installés sur les appareils administrés (registre des applications). Les applications peuvent être identifiées sur la base d'informations sur les fichiers exécutables détectés sur les appareils administrés par la fonctionnalité Contrôle des applications :

      - Identifiant de l'application/du correctif
      - Identifiant de l'application parente (pour un correctif)
      - Nom et version de l'application/du correctif
      - Si l'application/le correctif est un fichier msi du service Windows Installer
      - Fournisseur de l'application/du correctif
      - Identifiant de la langue de localisation
      - Date d'installation de l'application/du correctif
      - Chemin d'installation de l'application
      - Site Internet du Support Technique du fournisseur de l'application/du correctif
      - Numéro de téléphone du Support Technique
      - Identifiant de l'instance de l'application installée
      - Commentaire
      - Clé de désinstallation
      - Clé d'installation en mode silencieux
      - Classification du correctif
      - Adresse Internet pour obtenir des informations supplémentaires concernant le correctif
      - Clé de registre de l'application
      - Numéro de version de l'application
      - SID d'utilisateur
      - Type de système d'exploitation (Windows, Unix)

   b. Informations relatives aux composants matériels détectés sur les appareils administrés (registre du matériel) :

      - Identificateur de l'appareil

- Type d'appareil (carte mère, processeur central, RAM, appareil de stockage de masse, carte vidéo, carte audio, contrôleur d'interface réseau, moniteur, appareil à disque optique)
- Nom de l'appareil
- Description
- Fournisseur
- Numéro de série
- Révision
- Informations sur le pilote : développeur, version, description et date de publication
- Informations sur le BIOS : développeur, version, numéro de série et date de publication
- Puce
- Fréquence d'horloge
- Nombre de cœurs du processeur
- Nombre de threads du processeur
- Plateforme du processeur
- Vitesse de rotation de l'appareil de stockage
- RAM : type, numéro de pièce
- Mémoire vidéo
- Codec de la carte son

c. Détails des vulnérabilités dans les applications tierces détectées sur les appareils administrés :

- Identificateur de vulnérabilités
- Niveau de gravité de la vulnérabilité (avertissement, élevé, critique)
- Type de vulnérabilité (Microsoft, tierce)
- Adresse Internet de la page sur laquelle est décrite la vulnérabilité
- Heure de création de l'entrée concernant la vulnérabilité
- Nom du fournisseur
- Nom du fournisseur localisé
- Identifiant du fournisseur
- Nom de l'application
- Nom localisé de l'application

- Code d'installation de l'application
- Version de l'application
- Langue de localisation de l'application
- Liste d'identifiants CVE de la description de la vulnérabilité
- Technologies de protection de Kaspersky bloquant la vulnérabilité (Protection contre les fichiers malicieux, Détection comportementale, Protection contre les menaces Internet, Protection contre les menaces par emails, Prévention des intrusions, ZETA Shield)
- Chemin vers le fichier de l'objet dans lequel la vulnérabilité a été détectée
- Heure de détection de la vulnérabilité
- Identifiants des articles de la Base de connaissances de la description de la vulnérabilité
- Identifiants des bulletins de sécurité de la description de la vulnérabilité
- Liste des mises à jour relatives à la vulnérabilité
- S'il existe ou non un code malveillant exploitant cette vulnérabilité
- S'il existe ou non une application malveillante exploitant cette vulnérabilité

d. Détails des mises à jour disponibles pour les applications tierces installées sur les appareils administrés :

- Nom et version de l'application
- Fournisseur
- Langue de localisation de l'application
- Système d'exploitation
- Liste des correctifs d'après la séquence d'installation
- Version originale de l'application à laquelle est appliqué le correctif
- Version de l'application après l'installation du correctif
- Identifiant du correctif
- Numéro de version
- Indicateurs d'installation
- Contrats de licence pour le correctif
- Indique si le correctif est une condition indispensable pour l'installation d'autres correctifs
- Liste des applications dont l'installation et la mise à jour sont requises
- Sources d'informations sur le correctif

- Informations supplémentaires sur le correctif (adresses des pages Internet)
- Adresse Internet pour le téléchargement de correctifs, nom de fichier, version, révision et SHA256

e. Détails des mises à jour Microsoft trouvées par la fonctionnalité WSUS :

- Numéro de révision de la mise à jour
- Type de mise à jour Microsoft (pilote, logiciel, catégorie, detectoid)
- Mettre à jour le niveau d'importance selon le bulletin Microsoft Security Response Center (MSRC) (faible, moyen, élevé, critique)
- Identifiants des bulletins MSRC liés à la mise à jour
- Identifiants des articles dans la Base de connaissances MSRC
- Nom de la mise à jour (en-tête)
- Description de la mise à jour
- Si le programme d'installation de la mise à jour est interactif
- Indicateurs d'installation
- Classification des mises à jour (mises à jour critiques, mises à jour des définitions, pilotes, paquets des modules complémentaires, mises à jour de la protection, Service Packs, instruments, paquets cumulatifs de mise à jour, mises à jour, mise à niveau)
- Informations sur l'application mise à jour
- Identifiant du Contrat de licence utilisateur final (CLUF)
- Texte du CLUF
- Si le CLUF doit être accepté pour l'installation de la mise à jour
- Informations sur les mises à jour associées (identifiant et numéro de révision)
- Identifiant de la mise à jour (identité de mise à jour Global Microsoft Windows)
- Identifiants des mises à jour remplacées
- Si la mise à jour est masquée
- Si la mise à jour est obligatoire
- État de l'installation de la mise à jour (Non applicable, Non désigné pour l'installation, Désigné, Installation en cours, Installé, Échec, Redémarrage requis, Non désigné pour l'installation (nouvelle version))
- Identifiants CVE de la mise à jour
- Entreprise qui a publié la mise à jour, ou valeur " Entreprise manquante "

f. Liste des mises à jour Microsoft trouvées par la fonctionnalité WSUS qui doivent être installées sur l'appareil.

8. Informations relatives aux fichiers exécutables détectés sur les appareils administrés par la fonction Contrôle des applications (susceptibles d'être associées à des informations du registre des applications). Une liste complète des données figure dans la section décrivant les données pour les appareils administrés via l'application correspondante.

   L'application administrée transfère les données de l'appareil vers le Serveur d'administration via l'Agent d'administration.

9. Informations sur les fichiers placés dans Sauvegarde. Une liste complète des données figure dans la section décrivant les données pour les appareils administrés via l'application correspondante.

   L'application administrée transfère les données de l'appareil vers le Serveur d'administration via l'Agent d'administration.

10. Informations sur les fichiers demandés par les experts de Kaspersky pour une analyse détaillée. Une liste complète des données figure dans la section décrivant les données pour les appareils administrés via l'application correspondante.

    L'application administrée transfère les données de l'appareil vers le Serveur d'administration via l'Agent d'administration.

11. Informations concernant l'état et le déclenchement des règles du Contrôle évolutif des anomalies. Une liste complète des données figure dans la section décrivant les données pour les appareils administrés via l'application correspondante.

    L'application administrée transfère les données de l'appareil vers le Serveur d'administration via l'Agent d'administration.

12. Informations sur les appareils (unités de mémoire, outils de transfert d'informations, outils de copie papier d'informations et bus de connexion) installés ou connectés à l'appareil administré et détecté par la fonction Contrôle des appareils. Une liste complète des données figure dans la section décrivant les données pour les appareils administrés via l'application correspondante.

    L'application administrée transfère les données de l'appareil vers le Serveur d'administration via l'Agent d'administration.

13. Données sur les alertes :

    - Date et heure du premier événement de télémétrie dans l'alerte
    - Date et heure du dernier événement de télémétrie dans l'alerte
    - Nom de la règle déclenchée (l'utilisateur le saisit dans l'interface de Kaspersky Security Center Cloud Console)
    - État de l'alerte
    - Résolution (faux positif, vrai positif, faible priorité)
    - Identifiant et nom de l'utilisateur attribué à l'alerte
    - Identifiant unique dans la base de données de Kaspersky Security Center Cloud Console et le nom de l'appareil lié aux événements qui sont des sources d'alerte
    - SID et nom de l'utilisateur de l'appareil lié aux événements qui sont des sources d'alerte
    - Les observables, c'est-à-dire les données observables liées aux événements sources d'alerte :
        - Adresse IP

- Somme de hachage MD5 du fichier et du chemin d'accès au fichier
- Adresse Internet
- Domaine

- Détails supplémentaires de l'objet lié à l'alerte (reçus de l'application)
- Commentaires à l'alerte :
  - Date et heure d'ajout du commentaire
  - Utilisateur qui a ajouté le commentaire
  - Texte du commentaire
- Journal des modifications de l'alerte :
  - Date et heure de la modification
  - Utilisateur qui a effectué le changement
  - Changer la description

14. Données sur les problèmes de sécurité :

- Date et heure du premier événement du problème de sécurité
- Date et heure du dernier événement du problème de sécurité
- Nom du problème de sécurité (saisi par l'utilisateur dans l'interface de Kaspersky Security Center Cloud Console)
- Brève description du problème de sécurité
- Priorité au problème de sécurité
- État du problème de sécurité
- Identifiant et nom de l'utilisateur attribué pour le problème de sécurité
- Résolution (faux positif, vrai positif, faible priorité, fusionné)
- Commentaire relatif au problème de sécurité :
  - Date et heure d'ajout du commentaire
  - Utilisateur qui a ajouté le commentaire
  - Texte du commentaire
- Journal des modifications du problème de sécurité :
  - Date et heure de la modification
  - Utilisateur qui a effectué le changement

- Changer la description

15. Données traitées par la fonctionnalité de chiffrement des données des applications Kaspersky.

    L'application administrée transfère les données de l'appareil indiquées ci-dessous vers le Serveur d'administration via l'Agent d'administration. L'utilisateur saisit la description du disque dans l'interface de Kaspersky Security Center Cloud Console :

    a. Liste des disques sur les appareils :

    - Nom du disque
    - État de chiffrement
    - Type de disque (disque de démarrage, disque)
    - Numéro de série du disque
    - Description

    b. Détails des erreurs de chiffrement des données sur les appareils :

    - Date et heure auxquelles l'erreur s'est produite
    - Type d'opération (chiffrement, déchiffrement)
    - Description de l'erreur
    - Chemin d'accès au fichier
    - Description de la règle
    - Identificateur de l'appareil
    - Nom d'utilisateur
    - Identifiant de l'erreur

    c. Paramètres de chiffrement des données de l'application Kaspersky.

    Une liste complète des données figure dans la section décrivant les données pour les appareils administrés via l'application correspondante.

16. Détails des codes d'activation saisis.

    L'utilisateur saisit les données dans l'interface Kaspersky Security Center Cloud Console.

17. Comptes utilisateurs.

    L'utilisateur saisit les données répertoriées ci-dessous dans l'interface de Kaspersky Security Center Cloud Console :

    a. Nom

    b. Description

    c. Nom complet

    d. Adresse email

e. Numéro de téléphone principal

f. Mot de passe

g. Code de sécurité unique pour la vérification en deux étapes

18. Données requises pour l'authentification de l'utilisateur à l'aide d'Active Directory :

    a. Paramètres AD FS (Active Directory Federation Services) :

    - URL principale du fournisseur d'authentification
    - Certificats racine de confiance pour AD FS
    - ID client généré dans AD FS
    - Clé secrète pour la protection de l'accès à AD FS
    - Zone de fonctionnement des jetons
    - Domaine Active Directory avec lequel l'intégration est effectuée
    - Nom du champ de jeton contenant le SID de l'utilisateur
    - Nom du champ de jeton contenant le tableau des SID des groupes de l'utilisateur

    L'utilisateur saisit les données dans l'interface Kaspersky Security Center Cloud Console.

19. Données requises pour l'authentification des utilisateurs à l'aide de Microsoft Entra ID.

    a. Paramètres d'intégration de Microsoft Entra ID :

    - ID du locataire Microsoft Entra ID
    - ID client généré dans le locataire Microsoft Entra ID
    - Clé secrète client créée dans le locataire Microsoft Entra ID

    L'utilisateur saisit les données dans l'interface Kaspersky Security Center Cloud Console.

    a. Données relatives aux utilisateurs et aux groupes dans le locataire Microsoft Entra ID, que Kaspersky Security Center Cloud Console reçoit à la suite du sondage Microsoft Entra ID :

    - Données relatives aux utilisateurs dans le client Microsoft Entra ID : identificateur d'objet utilisateur ; identifiant de sécurité de l'utilisateur ; nom d'affichage de l'utilisateur ; nom de l'organisation de l'utilisateur ; nom du service dans lequel travaille l'utilisateur ; poste de l'utilisateur ; adresse email ; numéro de téléphone principal ; numéro de téléphone mobile ; identifiant de l'utilisateur ; noms des groupes dont l'utilisateur fait partie.
    - Données relatives aux utilisateurs créés dans Microsoft Entra ID à la suite de la synchronisation avec l'instance Active Directory sur site : identifiant de sécurité de l'utilisateur dans l'instance Active Directory sur site ; nom de domaine dans l'instance Active Directory sur site ; connexion de l'utilisateur à l'instance Active Directory sur site ; compte SAM de l'utilisateur dans l'instance Active Directory sur site ; nom d'utilisateur distinctif dans l'instance Active Directory sur site.

- Données relatives aux groupes dans le client Microsoft Entra ID : identificateur d'objet de groupe ; identifiant de sécurité du groupe ; nom d'affichage du groupe ; adresse email ; noms des autres groupes dont le groupe fait partie.

- Données relatives aux groupes créés dans Microsoft Entra ID à la suite de la synchronisation avec l'instance Active Directory sur site : l'identifiant de sécurité du groupe dans l'instance Active Directory sur site ; compte SAM du groupe dans l'instance Active Directory sur site.

20. Historique des révisions des objets d'administration. : Serveur d'administration ; groupe d'administration ; stratégie ; tâche ; groupe de sécurité/des utilisateurs ; paquet d'installation.

    a. L'utilisateur saisit les données répertoriées ci-dessous dans l'interface de Kaspersky Security Center Cloud Console :

    - Serveur d'administration
    - Groupe d'administration
    - Stratégie
    - Tâche
    - Groupe d'utilisateurs/de sécurité
    - Paquet d'installation

    b. Adresse IP de l'appareil sur lequel l'utilisateur a créé une révision. Le Serveur d'administration détecte l'adresse IP automatiquement.

21. Registre des objets de gestion supprimés.

    L'utilisateur saisit les données dans l'interface Kaspersky Security Center Cloud Console.

22. Paquets d'installation créés à partir du fichier, ainsi que les paramètres d'installation.

    L'utilisateur saisit les données dans l'interface Kaspersky Security Center Cloud Console.

23. Données requises pour l'affichage des annonces de Kaspersky dans la Kaspersky Security Center Cloud Console :

    a. Informations sur les applications Kaspersky administrées utilisées par l'utilisateur : identifiant de l'application, numéro de version complet.

    b. Localisation de l'utilisateur de Kaspersky Security Center Cloud Console.

    c. Informations sur l'activation du Logiciel sur l'appareil : ID de licence du logiciel ; durée de validité de la licence du logiciel ; date et heure de fin de la durée de validité de la licence du Logiciel ; type de licence de logiciel utilisée ; type d'abonnement logiciel ; date et heure d'expiration de l'abonnement au logiciel ; état actuel de l'abonnement au Logiciel ; motif du statut actuel/changeant de l'abonnement au Logiciel ; ID de l'article de la liste de prix sur la base duquel la licence du logiciel a été achetée.

    d. Informations sur l'accord juridique accepté par l'utilisateur dans le cadre de l'utilisation du Logiciel : type de l'accord juridique ; version de l'accord juridique ; indicateur signalant si l'utilisateur a accepté les conditions de l'accord juridique.

    e. Informations sur les annonces reçues du Détenteur des droits : identifiant de l'annonce ; heure de réception de l'annonce ; état de réception de l'annonce.

L'utilisateur saisit les données dans l'interface Kaspersky Security Center Cloud Console.

24. Paramètres utilisateur de Kaspersky Security Center Cloud Console.

    L'utilisateur saisit les données répertoriées ci-dessous dans l'interface de Kaspersky Security Center Cloud Console :

    a. Langue de localisation de l'interface utilisateur

    b. Thème de l'interface utilisateur

    c. Paramètres d'affichage du panneau de surveillance

    d. Informations sur l'état des notifications : déjà lues/pas encore lues

    e. État des colonnes dans les feuilles de calcul : affichées/masquées

    f. Progression du didacticiel

25. Données reçues lors de l'utilisation de la fonctionnalité Diagnostics à distance sur un appareil administré : fichiers de trace, informations système, détails des applications Kaspersky installées sur l'appareil, fichiers dump, fichiers journaux, résultats de l'exécution des scripts de diagnostic reçus du Support Technique.

26. Données saisies par l'utilisateur dans l'interface de Kaspersky Security Center Cloud Console :

    a. Nom du groupe d'administration lors de la création d'une hiérarchie dans les groupes d'administration

    b. Adresse email lors de la configuration de notifications par email

    c. Balises d'appareils et règles pour l'attribution de balises

    d. Balises d'applications

    e. Catégories d'utilisateur des applications

    f. Nom du rôle lors de l'attribution d'un rôle à un utilisateur

    g. Informations sur les sous-réseaux : nom du sous-réseau, description, adresse et masque

    h. Paramètres des rapports et des sélections

    i. Toute autre donnée saisie par l'utilisateur

27. Données reçues d'un Serveur d'administration secondaire déployé sur site.

    Les données traitées par le Serveur d'administration de Kaspersky Security Center sont décrites dans l'Aide en ligne de Kaspersky Security Center.

    Lors de la connexion d'un Serveur d'administration de Kaspersky Security Center déployé sur site en tant qu'esclave par rapport à Kaspersky Security Center Cloud Console, Kaspersky Security Center Cloud Console traite les types de données suivants du Serveur d'administration secondaire :

    a. Informations sur les appareils du réseau de l'organisation, reçues à la suite d'une recherche d'appareils sur le réseau Active Directory ou le réseau Windows, ou par analyse des intervalles IP

    b. Informations sur les unités organisationnelles, les domaines, les utilisateurs et les groupes Active Directory reçues à la suite du sondage du réseau Active Directory

c. Informations sur les appareils administrés, leurs caractéristiques techniques, y compris les informations requises pour l'identification de l'appareil, comptes des utilisateurs de l'appareil et leurs sessions de travail

d. Informations sur les appareils mobiles transférées à l'aide du protocole Exchange ActiveSync

e. Informations sur les appareils mobiles transférées à l'aide du protocole MDM iOS

f. Détails relatifs aux applications Kaspersky installées sur l'appareil : paramètres, statistiques de fonctionnement, état de l'appareil défini par l'application, mises à jour installées et applicables, balises

g. Informations transférées avec des paramètres d'événement depuis des composants Kaspersky Security Center et des applications administrées par Kaspersky

h. Paramètres des composants Kaspersky Security Center et des applications administrées par Kaspersky présentés dans les stratégies et les profils stratégiques

i. Paramètres des tâches des composants Kaspersky Security Center et des applications administrées par Kaspersky

j. Données traitées par la fonction de la gestion des vulnérabilités et des correctifs : détails relatifs aux applications et aux correctifs ; informations sur les équipements ; détails relatifs aux vulnérabilités dans les applications tierces détectées sur des appareils administrés ; détails relatifs aux mises à jour disponibles pour des applications tierces ; détails des mises à jour Microsoft trouvées par la fonction WSUS

k. Catégories d'utilisateur des applications

l. Détails des fichiers exécutables détectés sur des appareils administrés par la fonction Contrôle des applications

m. Détails des fichiers placés dans Sauvegarde

n. Détails des fichiers placés en quarantaine

o. Détails des fichiers demandés par des spécialistes Kaspersky en vue d'une analyse approfondie

p. Informations concernant l'état et le déclenchement des règles du Contrôle évolutif des anomalies

q. Détails sur les appareils (unités de mémoire, outils de transfert d'informations, outils de copie papier d'informations et bus de connexion) installés ou connectés à l'appareil administré et détecté par la fonction Contrôle des applications

r. Paramètres de chiffrement de l'application Kaspersky : stockage de clés de chiffrement, état de chiffrement de l'appareil

s. Informations sur les erreurs de chiffrement des données sur les appareils utilisant la fonction de chiffrement des données des applications Kaspersky

t. Liste des automates programmables industriels administrés (API)

u. Détails des codes d'activation saisis

v. Comptes utilisateurs

w. Historique de révision des objets de gestion

x. Registre des objets de gestion supprimés

y. Paquets d'installation créés à partir du fichier, ainsi que les paramètres d'installation

z. Paramètres utilisateur de Kaspersky Security Center Web Console

aa. Toutes les données saisies par l'utilisateur dans la Console d'administration ou l'interface de Kaspersky Security Center Cloud Console

ab. Certificat de connexion sécurisée des appareils administrés aux composants Kaspersky Security Center

28. Informations chargées depuis l'appareil administré lors de l'utilisation de la fonction de diagnostic à distance : fichiers de diagnostic (fichiers dump, fichiers journaux, fichiers de traçage, etc.) et données contenues dans ces fichiers.

29. Données requises pour l'intégration de Kaspersky Security Center Cloud Console avec un système SIEM pour l'exportation d'événements :

- Données requises pour la connexion et l'authentification :
  - Adresse et port de connexion du système SIEM
  - Certificat d'authentification du serveur SIEM
  - Certificat de confiance et clé privée pour l'authentification client de Kaspersky Security Center Cloud Console dans le système SIEM

  L'utilisateur saisit les données dans l'interface Kaspersky Security Center Cloud Console.
- Données que Kaspersky Security Center Cloud Console reçoit du système SIEM : clé publique du certificat du serveur SIEM pour l'authentification du serveur SIEM.

30. Données requises pour l'interaction de Kaspersky Security Center Cloud Console avec l'environnement cloud :

a. Amazon Web Services (AWS) :

- ID de clé d'accès du compte utilisateur IAM
- Clé secrète du compte utilisateur IAM

b. Microsoft Azure :

- Identifiant de l'application Azure
- Identifiant de l'abonnement Azure
- Mot de passe de l'application Azure
- Nom du compte pour le stockage Azure
- Clé d'accès au compte pour le stockage Azure

c. Google Cloud :

- Email client Google
- Identifiant du projet

- Clé privée

L'utilisateur saisit les données dans l'interface Kaspersky Security Center Cloud Console.

31. Données transférées par une application Kaspersky non prise en charge

    Lorsque vous installez l'Agent d'administration sur un appareil sur lequel une application Kaspersky est installée mais non prise en charge par Kaspersky Security Center Cloud Console, cette application Kaspersky transfère toujours les données vers Kaspersky Security Center Cloud Console. (la liste de données est fournie dans la section " À propos de la collecte des données " du système d'aide de l'application.) Cependant, Kaspersky Security Center Cloud Console ne pourra pas traiter les données transférées par une application non prise en charge de la même manière que le processus décrit pour les principales fonctionnalités de Kaspersky Security Center Cloud Console.

    La liste des applications Kaspersky prises en charge est présentée dans l'Aide en ligne de Kaspersky Security Center Cloud Console.

32. Informations statistiques sur les tentatives des utilisateurs d'accéder aux services cloud.

    L'application administrée transfère les données de l'appareil vers le Serveur d'administration via l'Agent d'administration. Pour obtenir la liste complète des données transférées, consultez l'aide de l'application administrée.

33. Données pour la création d'une chaîne de développement de la menace.

    L'application administrée transfère les données de l'appareil vers le Serveur d'administration via l'Agent d'administration. Pour obtenir la liste complète des données transférées, consultez l'aide de l'application administrée.

34. Données requises pour l'intégration de Kaspersky Security Center avec le service Kaspersky Managed Detection and Response.

    Jeton de lancement de l'intégration, jeton d'intégration et jeton de session d'utilisateur. L'utilisateur saisit le jeton pour lancer l'intégration dans l'interface de Kaspersky Security Center Cloud Console. Le service Kaspersky Managed Detection and Response transfère le jeton d'intégration et le jeton de session d'utilisateur via le plug-in MDR.

Données nécessaires au fonctionnement des applications administrées

Les applications administrées suivantes transfèrent les données de l'appareil vers le Serveur d'administration via l'Agent d'administration.

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Linux
- Kaspersky Endpoint Security for Mac
- Kaspersky Endpoint Agent
- Kaspersky Security for Windows Server
- Kaspersky Security for Mobile
- Kaspersky Embedded Systems Security for Windows
- Kaspersky Embedded Systems Security for Linux

La liste des données traitées est publiée sur le site https://ksc.kaspersky.com/home/legaldocuments?locale=fr, dans l'Accord relatif au traitement des données de Kaspersky Security Center Cloud Console. Sur la page Internet des documents juridiques, recherchez le bloc de texte intitulé Contrat Kaspersky Security Center Cloud Console, puis faites défiler le bloc de texte jusqu'à la section Données pour les appareils administrés par l'application administrée adéquate. Vous pouvez également utiliser la fonction Rechercher standard de votre navigateur dans le même but.

Données de l'utilisateur traitées localement

L'Agent d'administration est le seul module de Kaspersky Security Center pouvant être déployé localement dans Kaspersky Security Center Cloud Console.

Liste des données de l'utilisateur traitées localement :

- Toutes les données répertoriées dans la section Données de l'utilisateur traitées dans le cadre et l'infrastructure de Kaspersky, à l'exception des données que l'administrateur saisit via l'interface de Kaspersky Security Center Cloud Console
- Journal des événements Kaspersky de l'Agent d'administration
- Traces de l'Agent d'administration
- Journaux, y compris les journaux créés par le programme d'installation de l'Agent d'administration, les utilitaires Kaspersky Security Center

Les fichiers de vidage, journaux et de trace de l'Agent d'administration contiennent des données aléatoires et peuvent contenir des données personnelles. Les fichiers sont stockés sous forme non chiffrée sur l'appareil sur lequel l'Agent d'administration est installé. Les fichiers ne sont pas transférés automatiquement à Kaspersky. L'utilisateur peut transférer ces données à Kaspersky manuellement à la demande du Support Technique pour résoudre les problèmes de fonctionnement de Kaspersky Security Center.

À propos des documents juridiques de Kaspersky Security Center Cloud Console

Pour utiliser Kaspersky Security Center Cloud Console, vous devez lire et exprimer votre accord avec les conditions des documents juridiques indiqués sur le site Internet de Kaspersky Security Center Cloud Console. Vous pouvez consulter les conditions de la politique de confidentialité d'AO Kaspersky Lab pour les sites Internet lorsque vous vous connectez à Kaspersky Security Center Cloud Console pour administrer un espace de travail. Vous pouvez lire l'accord de Kaspersky Security Center Cloud Console et l'Accord relatif au traitement des données de Kaspersky Security Center Cloud Console lorsque vous créez un espace de travail d'entreprise.

Veuillez attentivement lire les textes de tous les documents juridiques avant de commencer à utiliser Kaspersky Security Center Cloud Console.

Contrat de licence utilisateur final pour les applications Kaspersky

Le Contrat de licence utilisateur final (ci-après également appelé Contrat de licence ou CLUF) est un accord légal entre vous et AO Kaspersky Lab stipulant les conditions dans lesquelles vous pouvez utiliser les applications Kaspersky.

Vous pouvez prendre connaissance des conditions du Contrat de licence utilisateur final de l'une des manières suivantes :

- Dans la fenêtre qui s'affiche lors de la création du paquet d'installation de l'application Kaspersky.
- Dans le fichier license.txt, dans le dossier d'installation de l'application Kaspersky, sur l'appareil administré.

Vous pouvez à tout moment révoquer votre acceptation du Contrat de licence utilisateur final.

Si vous refusez les dispositions du Contrat de licence d'une application de Kaspersky, vous ne pouvez pas utiliser l'application.

Guide de renforcement

Kaspersky Security Center Cloud Console est une application hébergée et maintenue par Kaspersky. Vous n'avez pas besoin d'installer Kaspersky Security Center Cloud Console sur votre ordinateur ou votre serveur. Kaspersky Security Center Cloud Console permet à l'administrateur d'installer des applications de sécurité 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.

Kaspersky Security Center Cloud Console 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 Cloud Console permet de configurer tous les modules de protection créés à l'aide des applications de Kaspersky.

Kaspersky Security Center Cloud Console 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 Kaspersky Security Center Cloud Console.

Le guide renforcement décrit les recommandations et les fonctionnalités de configuration de Kaspersky Security Center Cloud Console et de ses modules, dans le but de réduire les risques de compromission.

Le Guide de renforcement contient les informations suivantes :

- Configuration des comptes pour accéder à Kaspersky Security Center Cloud Console
- Gestion de la protection des appareils clients
- Configuration de la protection des applications administrées
- Transfert d'informations vers des applications tierces

Avant de commencer à travailler avec Kaspersky Security Center Cloud Console, vous serez invité à lire la version abrégée du guide de renforcement.

Notez que vous ne pouvez pas utiliser Kaspersky Security Center Cloud Console tant que vous n'avez pas confirmé avoir lu le guide de renforcement.

Pour lire le Guide de renforcement :

1. Ouvrez Kaspersky Security Center Cloud Console et connectez-vous. Kaspersky Security Center Cloud Console vérifie si vous avez confirmé la lecture de la version actuelle du guide de renforcement.

   Si vous n'avez pas encore lu le Guide de renforcement, une fenêtre s'ouvre et affiche une version succincte de celui-ci.

2. Exécutez une des actions suivantes :

   - Si vous souhaitez consulter la version abrégée du Guide de renforcement sous la forme d'un document texte, cliquez sur le lien **Ouvrir dans une nouvelle fenêtre**.
   - Si vous souhaitez consulter la version complète du Guide de renforcement, cliquez sur le lien **Ouvrir le guide de renforcement dans l'aide en ligne**.

3. Après avoir lu le Guide de renforcement, cochez la case **Je confirme que j'ai entièrement lu et que je comprends le guide de sécurisation renforcée**, puis cliquez sur le bouton **Accepter**.

Vous pouvez désormais Kaspersky Security Center Cloud Console.

Lorsqu'une nouvelle version du guide de renforcement de la sécurité apparaît, Kaspersky Security Center Cloud Console vous invite à la lire.

Planification de l'architecture Kaspersky Security Center Cloud Console

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.

Au stade initial du développement de l'architecture, nous vous recommandons de vous familiariser avec les modules de Kaspersky Security Center Cloud Console et leur interaction les uns avec les autres, 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 :

- Organisation des espaces de travail de l'administrateur et modes de connexion à Kaspersky Security Center Cloud Console
- 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

Comptes et authentification

Utilisation de la vérification en deux étapes avec Kaspersky Security Center Cloud Console

Kaspersky Security Center Cloud Console propose une vérification en deux étapes pour les utilisateurs.

La vérification en deux étapes peut vous aider à renforcer la sécurité de votre compte dans Kaspersky Security Center Cloud Console. Lorsque cette fonction est activée, chaque fois que vous vous connectez à Kaspersky Security Center Cloud Console avec votre adresse email et votre mot de passe, vous saisissez un code de sécurité supplémentaire à usage unique. Vous pouvez recevoir un code de sécurité à usage unique par SMS ou en générant ce code dans votre application d'authentification (selon la méthode de vérification en deux étapes que vous avez configurée).

Il est fortement déconseillé d'installer l'application d'authentification sur le même appareil à partir duquel la connexion à Kaspersky Security Center Cloud Console est établie. Vous pouvez installer une application d'authentification sur votre appareil mobile.

Interdiction d'enregistrer le mot de passe administrateur

Si vous utilisez Kaspersky Security Center Cloud Console, **il est fortement déconseillé** d'enregistrer le mot de passe administrateur dans le navigateur installé sur l'appareil de l'utilisateur.

Si le navigateur est compromis, un intrus peut accéder aux mots de passe enregistrés. De plus, si l'appareil de l'utilisateur avec les mots de passe enregistrés est volé ou perdu, un intrus peut accéder aux données protégées.

Restriction de l'appartenance au rôle de l'Administrateur principal

Nous vous recommandons de restreindre l'appartenance au rôle Administrateur principal.

Par défaut, une fois qu'un utilisateur a créé un espace de travail, le rôle Administrateur principal lui est attribué. Il est utile pour l'administration, mais il est critique du point de vue de la sécurité, car le rôle Administrateur principal dispose d'une plage de privilèges étendue. L'attribution de ce rôle aux utilisateurs doit être strictement réglementée.

Vous pouvez utiliser les rôles d'utilisateur prédéfinis avec un ensemble de droits préconfigurés pour administrer Kaspersky Security Center Cloud Console.

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 Cloud Console 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.

Gestion de la protection des appareils clients

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.

L'utilisation de règles automatiques pour le déplacement d'appareils peut entraîner la propagation de stratégies qui accordent plus de privilèges à l'appareil déplacé que ce dernier n'en avait avant le déplacement.

De plus, le déplacement d'un appareil client vers un autre groupe d'administration peut entraîner la propagation des paramètres de la stratégie. Ces paramètres de stratégie peuvent être indésirables pour la distribution aux appareils invités et non approuvés.

Cette recommandation ne s'applique pas à l'affectation initiale unique des appareils aux groupes d'administration.

Exigences de sécurité pour les points de distribution et les passerelles de connexion

Les appareils sur lesquels l'Agent d'administration est installé peuvent remplir le rôle de point de distribution et exécuter 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.
- Agir en tant que serveur proxy KSN pour les appareils clients.

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 physique).

Configuration de la protection des applications administrées

Configuration de la protection réseau

Assurez-vous d'avoir terminé le scénario de configuration initiale de Kaspersky Security Center Cloud Console. Ce scénario inclut également la réalisation des étapes de l'assistant de démarrage rapide de l'application.

Lorsque l'assistant de démarrage rapide de l'application fonctionne, des stratégies et des tâches avec des paramètres par défaut sont créées. Ces paramètres peuvent ne pas être optimaux ou peuvent même être interdits dans votre organisation. Par conséquent, nous vous recommandons de configurer les stratégies et les tâches créées et de créer des stratégies et des tâches supplémentaires si nécessaire pour le réseau de votre organisation.

Définition du mot de passe pour la désactivation de la protection et la désinstallation de l'application

Pour empêcher les intrus de désactiver les applications de sécurité de Kaspersky, nous vous recommandons fortement d'activer la protection par mot de passe pour désactiver la protection et de désinstaller les applications de sécurité de Kaspersky. Vous pouvez définir le mot de passe, par exemple, pour Kaspersky Endpoint Security for Windows, Kaspersky Security for Windows Servers, l'Agent d'administration et d'autres applications de Kaspersky. Après avoir activé la protection par mot de passe, nous vous recommandons de verrouiller ces paramètres en fermant le " cadenas ".

Spécification du mot de passe pour la connexion manuelle de l'appareil client au Serveur d'administration (utilitaire klmover)

L'utilitaire klmover vous permet de connecter manuellement un appareil client au Serveur d'administration. Lors de l'installation de l'Agent d'administration sur l'appareil client, l'utilitaire est automatiquement copié dans le dossier d'installation de l'Agent d'administration.

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

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

L'utilitaire klmover est utilisé uniquement pour déplacer des appareils administrés sous la gestion d'un Serveur d'administration virtuel.

Utilisation de Kaspersky Security Network

Dans toutes les stratégies des applications administrées et dans les propriétés de Kaspersky Security Center Cloud Console, nous vous recommandons d'activer l'utilisation de Kaspersky Security Network (KSN) et d'accepter la Déclaration KSN. Lorsque vous mettez à jour ou mettez à niveau Kaspersky Security Center Cloud Console, vous pouvez accepter la Déclaration KSN mise à jour.

Découverte de nouveaux appareils

Nous vous recommandons de configurer correctement les paramètres de recherche d'appareils : configurez l'intégration à Active Directory et spécifiez les plages d'adresses IP pour la recherche de nouveaux appareils.

Pour des raisons de sécurité, vous pouvez utiliser le groupe d'administration par défaut qui inclut tous les nouveaux appareils et les stratégies par défaut affectant ce groupe.

Transfert d'événements vers des systèmes tiers

Surveillance et rapports

Pour une réponse rapide aux problèmes de sécurité, nous vous recommandons de configurer les fonctionnalités de surveillance et de création de rapports.

Exportation des événements dans les systèmes SIEM

Pour une réponse rapide aux problèmes de sécurité avant que des dommages importants ne surviennent, nous vous recommandons d'utiliser l'exportation d'événements dans un système SIEM.

Notifications par e-mail des événements de l'audit

Pour une réponse rapide aux urgences, nous vous recommandons de configurer Kaspersky Security Center Cloud Console pour envoyer des notifications sur les événements de l'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.

Interface de Kaspersky Security Center Cloud Console

Kaspersky Security Center Cloud Console est administré via l'interface Web.

La fenêtre de l'application contient les éléments suivants :

- Menu principal dans la partie gauche de la fenêtre
- Zone de travail dans la partie droite de la fenêtre

Menu principal

Le menu principal contient les sections suivantes :

- **Liens rapides**. Contient les onglets suivants :
  - **Paramètres de page d'accueil**. Affiche la carte du menu principal. Par défaut, l'onglet **Paramètres de page d'accueil** de la section **Liens rapides** est défini comme page d'accueil. Vous pouvez modifier ces paramètres.
  - **Introduction et tutoriels**. Contient des vidéos sur la configuration et l'utilisation de Kaspersky Security Center Cloud Console et des applications de sécurité.

    Dans le navigateur Mozilla Firefox, si vous lisez une vidéo dans la section **Introduction et tutoriels** de la fenêtre contextuelle, ouvrez la vidéo dans le mode image dans image, puis fermez la vidéo dans la fenêtre contextuelle, la vidéo dans l'image en mode image est également fermée.
- **Serveur d'administration**. Affiche le nom du Serveur d'administration auquel vous êtes actuellement connecté. Cliquez sur l'icône des paramètres ( ) pour ouvrir les propriétés du Serveur d'administration.
- **Surveillance et rapports**. Fournit une vue d'ensemble de votre infrastructure, des états de la protection et des statistiques.
- **Ressources (Appareils)**. Contient les outils d'administration des appareils clients, 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 une variété d'opérations, y compris l'administration des licences d'applications, l'administration des correctifs et la gestion 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. Celui-ci 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**. Contient les paramètres d'intégration de Kaspersky Security Center Cloud Console à d'autres applications de Kaspersky. Il contient également vos paramètres personnels liés à l'apparence de l'interface, tels

que la langue de l'interface ou le thème.

- **Menu de votre compte**. Contient un lien vers l'aide en ligne et des informations sur le Support Technique de Kaspersky. Il vous permet également de vous déconnecter de Kaspersky Security Center Cloud Console.

Zone de travail

La zone de travail affiche les informations que vous choisissez d'afficher dans les sections de la fenêtre de l'interface Web de l'application. Il contient également des éléments de contrôle qui permettent de configurer l'affichage des informations.

Modification de la langue de l'interface de Kaspersky Security Center Cloud Console

Vous pouvez sélectionner la langue de l'interface de Kaspersky Security Center Cloud 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 page d'accueil de Kaspersky Security Center Cloud Console

La page d'accueil s'affiche après votre connexion à Kaspersky Security Center Cloud Console.

Par défaut, l'onglet **Paramètres de page d'accueil** de la section **Liens rapides** 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 **Liens rapides**, 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 et l'élément sélectionné comme page d'accueil est marqué de 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 Cloud 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 **Ressources (Appareils)** → **Appareils administrés**, une page avec le tableau des appareils s'ouvre. Vous pouvez donc ajouter la section **Appareils administrés** 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 ajouter aux signets.
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 éléments des signets dans la section **Liens rapides** en les 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 **Liens rapides**.

Configuration initiale de Kaspersky Security Center Cloud Console

Cette section présente le scénario principal du déploiement de Kaspersky Security Center Cloud Console, en commençant par la création d'un espace de travail et en finissant par la surveillance de l'état de la protection du réseau.

Pour plus d'informations sur le déploiement de Kaspersky Security Center, reportez-vous à l'Aide en ligne de Kaspersky Security Center.

Nous vous recommandons d'affecter au minimum un jour ouvrable à la réalisation de ce scénario.

Le scénario vous guide à travers les éléments suivants :

- Commencer à travailler avec un espace de travail de votre entreprise en tant qu'administrateur
- Découvrir les appareils de votre réseau (si nécessaire, vous leur affecterez des points de distribution et installerez manuellement des paquets de distribution sur ceux-ci)
- Déployer des applications de Kaspersky administrées sur les appareils clients et configurer des outils pour la protection du réseau, la surveillance et les mises à jour régulières des bases de données, des modules logiciels et applications de Kaspersky

Une fois ce scénario terminé, la protection réseau basée sur les applications Kaspersky sera configurée. Vous pourrez alors surveiller l'état de la protection du réseau.

Prérequis

Avant de commencer :

- Observez l'architecture de Kaspersky Security Center Cloud Console pour comprendre les interactions entre les principaux composants de l'application.
- Lisez les informations sur les licences de Kaspersky Security Center Cloud Console et des applications administrées.
- Veillez à disposer d'un code d'activation valide pour Kaspersky Security Center Cloud Console (si vous créez un espace de travail commercial).

Étapes

La configuration de Kaspersky Security Center Cloud Console se déroule par étapes :

1. **Configuration des ports**

   Assurez-vous que tous les ports nécessaires sont ouverts pour l'interaction entre votre réseau et l'infrastructure Kaspersky. De plus, si vous prévoyez d'utiliser la hiérarchie du Serveur d'administration, assurez-vous que tous les ports nécessaires sont ouverts pour les interactions impliquant le Serveur d'administration secondaire (ou les Serveurs d'administration secondaires) et les appareils clients.

2. **Création de l'espace de travail pour votre entreprise**

   Créez un compte, puis créez un espace de travail pour votre entreprise.

3. **Exécution de l'assistant de démarrage rapide de l'application**

Ouvrez et connectez-vous à Kaspersky Security Center Cloud Console. Lorsque vous vous connectez pour la première fois, vous êtes automatiquement invité à exécuter l'assistant de démarrage rapide de l'application. Vous pouvez aussi lancer l'assistant de démarrage rapide de l'application manuellement à tout moment.

Une fois l'assistant de démarrage rapide de l'application terminé, vous disposez des paquets d'installation de l'Agent d'administration et des applications de sécurité. Ces paquets d'installation sont requis pour le déploiement ultérieur de Kaspersky Security Center Cloud Console.

4. **Déploiement d'applications Kaspersky**

   Exécutez le scénario de déploiement initial des applications Kaspersky. L'une des étapes du scénario fait référence à l'opération de sondage du réseau. Cette opération est nécessaire pour détecter les appareils clients de votre réseau. Le sondage réseau et ses paramètres sont décrits dans le scénario de découverte des appareils en réseau.

   Si vous déployez Kaspersky Security for Windows Server, assurez-vous que les bases de données de cette application sont à jour.

5. **Octroi de licences pour les applications de sécurité Kaspersky**

   Lorsque des applications de sécurité Kaspersky sont déployées sur les appareils administrés, vous devez obtenir une licence pour ces derniers en appliquant un code d'activation à chacun de ces programmes. Déployez vos codes d'activation sur les applications Kaspersky installées sur les appareils administrés. Vous disposez de plusieurs options pour obtenir une licence pour les applications de sécurité Kaspersky.

6. **Configuration de la protection réseau**

   Effectuez la configuration de la protection réseau pour affiner les stratégies et les tâches créées à l'aide de l'assistant de démarrage rapide de l'application.

7. **Mise à jour régulière des bases de données, des modules logiciels et des applications Kaspersky**

   Pour protéger votre réseau contre les virus et d'autres menaces, vous devez configurer des mises à jour régulières des bases de données, des modules logiciels et des applications Kaspersky.

8. **Mise à jour du logiciel tiers et correction des vulnérabilités dans les applications tierces (facultatif)**

   Kaspersky Security Center Cloud Console permet d'administrer les mises à jour des applications de Microsoft installées sur les appareils client. Vous pouvez également corriger les vulnérabilités dans les applications Microsoft en installant les mises à jour nécessaires.

9. **Configuration des outils de surveillance de l'état de la protection du réseau**

   Sélectionnez et configurez des widgets, des rapports et d'autres outils vous permettant de surveiller l'état de la protection du réseau.

Lorsque Kaspersky Security Center Cloud Console est déployée et configurée, vous pouvez passer au contrôle de l'état de la protection du réseau.

Gestion de l'espace de travail

Ce document décrit comment utiliser les comptes et les espaces de travail dans Kaspersky Security Center Cloud Console.

À propos de l'administration de l'espace de travail dans Kaspersky Security Center Cloud Console

Kaspersky Security Center Cloud Console vous permet exécuter les actions suivantes :

- Créer un compte.
- Modifier un compte.
- Enregistrer une entreprise et créer un espace de travail.
- Modifier les informations sur l'entreprise et les espaces de travail.
- Supprimer un espace de travail et une entreprise.
- Supprimer un compte.

Prise en main de Kaspersky Security Center Cloud Console

Cette section décrit comment s'inscrire sur Kaspersky Security Center Cloud Console et commencer à l'utiliser.

L'inscription à Kaspersky Security Center Cloud Console comprend les étapes suivantes :

1. Création et confirmation d'un compte.
2. Enregistrement d'une entreprise et création d'un espace de travail.

Création d'un compte

Cet article décrit comment créer un compte dans Kaspersky Security Center Cloud Console.

Vous pouvez également créer un compte sur My Kaspersky, puis l'utiliser pour vous connecter à Kaspersky Security Center Cloud Console et créer votre espace de travail.

> Votre compte My Kaspersky doit être créé directement sur le site Internet et non à l'aide d'un fournisseur d'authentification externe (comme Google). Sinon, vous ne pourrez pas utiliser Kaspersky Security Center Cloud Console.

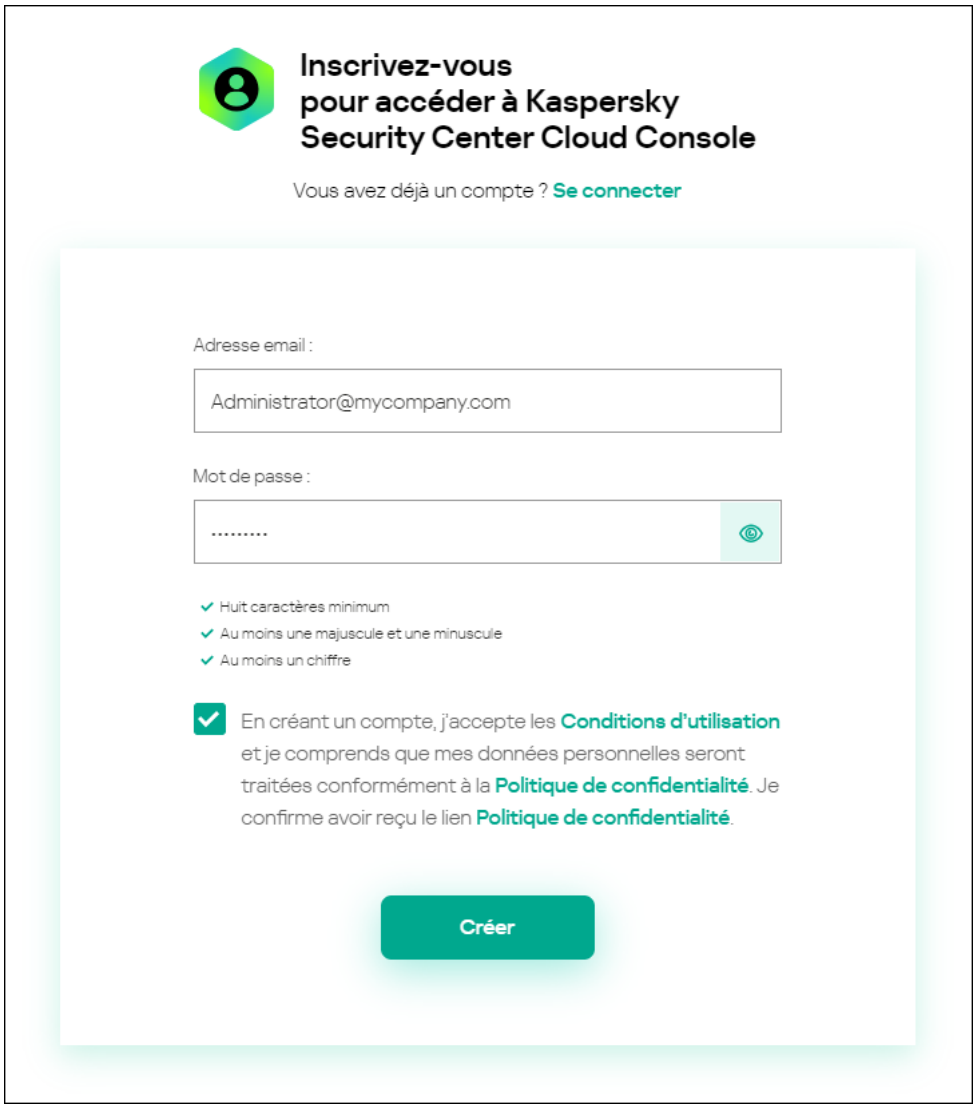
Pour créer un compte sur Kaspersky Security Center Cloud Console :

1. Dans votre navigateur, accédez à Kaspersky Security Center Cloud Console.

2. Cliquez sur le bouton **Créer un compte** sur la page d'accueil de Kaspersky Security Center Cloud Console.

   Le portail Kaspersky Account s'ouvre.

3. Sur la page **Inscription pour accéder à Kaspersky Security Center Cloud Console**, saisissez l'adresse email et le mot de passe de votre compte (voir la figure ci-dessous).



Création d'un compte dans Kaspersky Security Center Cloud Console

4. Cliquez sur le lien **Politique de confidentialité** et lisez-la attentivement.

5. 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, et que vous confirmez que vous avez bien lu et compris la Politique de confidentialité, cochez la case en regard du texte sur l'accord pour le traitement des données conformément à la Politique de confidentialité, et cliquez sur le bouton **Créer**.

   Si vous n'acceptez pas la Politique de confidentialité, n'utilisez pas Kaspersky Security Center Cloud Console.

6. Kaspersky envoie un message à l'adresse email que vous avez renseignée. Le message contient un code de sécurité à usage unique.

   Ouvrez l'email, puis copiez le code de sécurité à usage unique qu'il contient.

7. Revenez à Kaspersky Account, puis collez le code dans le champ de saisie.

La création d'un compte sur Kaspersky Security Center Cloud Console est terminée.

Enregistrement d'une entreprise et création d'un espace de travail

Immédiatement après la création du compte, vous pouvez enregistrer une entreprise et créer un espace de travail pour celle-ci.

Si vous souhaitez protéger plus de 10 000 appareils, inutile d'enregistrer une entreprise et de créer un espace de travail sur Kaspersky Security Center Cloud Console comme décrit ci-dessous. Envoyez plutôt une demande au support technique de Kaspersky. Dans la demande, indiquez les informations relatives à votre entreprise et à l'espace de travail que vous souhaitez créer.

Avant de commencer, veillez à obtenir les opérations suivantes :

- le nom de l'entreprise où vous avez l'intention d'utiliser le logiciel.
- le pays où se trouve l'entreprise. Si l'entreprise est située au Canada, il faut aussi connaître la province.
- Le nombre total d'ordinateurs et d'appareils mobiles que vous voulez protéger dans l'entreprise.

Pour enregistrer une entreprise et créer un espace de travail sur Kaspersky Security Center Cloud Console :

1. Dans votre navigateur, accédez à Kaspersky Security Center Cloud Console.
2. Cliquez sur le bouton **Se connecter** sur la page d'accueil de Kaspersky Security Center Cloud Console.
3. Saisissez l'adresse email et le mot de passe spécifiés lors de la création de votre compte, puis cliquez sur le bouton **Se connecter**.

   L'Assistant de création d'un espace de travail démarre. Parcourez les étapes de l'assistant à l'aide du bouton **Suivant**.
4. Sur la page **Étape 01 : Conditions d'utilisation de Kaspersky Security Center Cloud Console** de l'assistant, procédez comme suit :

   a. Lisez attentivement le Contrat, la Politique de confidentialité et l'Accord relatif au traitement des données pour la solution logicielle.

   b. Si vous acceptez les Conditions de l'accord et l'Accord relatif au traitement des données et 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, et que vous confirmez que vous avez lu et compris la Politique de confidentialité, cochez les cases en regard des trois documents énumérés, puis cliquez sur le bouton **Accepter**.

   Si vous n'acceptez pas les conditions, n'utilisez pas Kaspersky Security Center Cloud Console.

   Si vous cliquez sur le bouton **Refuser**, la création de l'espace de travail s'arrête.
5. Sur la page **Étape 02 : Informations sur l'entreprise** de l'assistant, indiquez les principales informations relatives à votre entreprise.

Remplissez les champs suivants :

- **Nom de votre entreprise** (obligatoire)

  Indiquez le nom de l'entreprise où vous allez utiliser la solution logicielle. Vous pouvez saisir un texte comptant jusqu'à 255 caractères. Le texte peut comporter des lettres majuscules et minuscules, des chiffres, les espaces, des points, des virgules, des signes moins, un tiret et des caractères de soulignement. Le nom de l'entreprise spécifié sera affiché dans Kaspersky Security Center Cloud Console.

- Champ **Description complémentaire de l'entreprise** (facultatif)

  Vous pouvez spécifier des informations complémentaires sur l'entreprise que vous enregistrez. Vous pouvez saisir un texte comptant jusqu'à 255 caractères. Le texte peut comporter des lettres majuscules et minuscules, des chiffres, les espaces, des points, des virgules, des signes moins, un tiret et des caractères de soulignement.

6. Sur la page **Étape 03 : Informations sur l'espace de travail** de l'assistant, indiquez les informations sur l'espace de travail que vous souhaitez créer pour votre entreprise.

   Remplissez les champs obligatoires suivants :

   - **Nom de l'espace de travail**. Indiquez le nom de l'espace de travail où vous allez utiliser la solution logicielle. Vous pouvez saisir un texte comptant jusqu'à 255 caractères. Le texte peut comporter des lettres majuscules et minuscules, des chiffres, les espaces, des points, des virgules, des signes moins, un tiret et des caractères de soulignement. Le nom de l'espace de travail spécifié sera affiché dans Kaspersky Security Center Cloud Console.

   - **Pays**. Choisissez dans la liste déroulante le pays où se trouve l'espace de travail. Si vous avez choisi le Canada, indiquez aussi la province dans la liste déroulante **État** qui figure sous ce champ.

   - **Nombre d'appareils**. Indiquez le nombre total d'ordinateurs et d'appareils mobiles que vous voulez protéger dans l'espace de travail.

     Saisissez dans ce champ un nombre compris entre 20 et 10 000. Le nombre minimum exact d'appareils que vous pouvez protéger dépend de la licence que vous avez achetée.

7. Sur la page **Étape 04 : Licence pour un nouvel espace de travail** de l'assistant, effectuez une des opérations suivantes :

   - Si vous souhaitez essayer Kaspersky Security Center Cloud Console, cliquez sur le lien **Je souhaite solliciter un espace de travail d'essai**.

     Nous vous recommandons de connecter vos propres appareils à votre espace de travail d'essai et de tester toute modification des paramètres, en notant les résultats.

     > Vous ne pourrez pas basculer un espace de travail d'essai en mode commercial via la saisie d'un code d'activation. Pour passer en mode commercial, vous devez supprimer l'espace de travail et le recréer.

   - Si vous souhaitez utiliser Kaspersky Security Center Cloud Console en mode commercial, saisissez le code d'activation et cliquez sur le bouton **Vérifier**.

L'enregistrement d'une entreprise et la création d'un espace de travail sur Kaspersky Security Center Cloud Console sont terminés.

Une fois l'espace de travail préparé, vous recevez un message électronique contenant le lien d'accès à l'espace de travail.

Protection de plus de 10 000 appareils

Si vous souhaitez protéger plus de 10 000 appareils, vous n'avez pas besoin d'enregistrer une entreprise et de créer un espace de travail. Envoyez plutôt une demande au support technique de Kaspersky.

Votre demande doit contenir les informations suivantes :

- **E-mail de l'utilisateur** : l'adresse e-mail de l'utilisateur enregistré sur Kaspersky Security Center Cloud Console. Cet utilisateur dispose des droits d'administrateur sur l'espace de travail créé.

  Après avoir créé un compte sur Kaspersky Security Center Cloud Console, vous n'avez pas besoin d'enregistrer une entreprise et de créer un espace de travail pour celle-ci. Indiquez les informations sur l'entreprise et l'espace de travail dans la demande.

- **Nom de l'entreprise** : le nom de l'entreprise dans laquelle vous souhaitez utiliser Kaspersky Security Center Cloud Console.

- **Pays de l'entreprise** : le pays où se trouve l'entreprise.

- **Nom de l'espace de travail** : le nom de l'espace de travail à créer pour l'entreprise.

- **Estimation du nombre de points de terminaison** : le nombre total d'appareils clients (y compris les appareils mobiles) que vous souhaitez protéger dans le nouvel espace de travail.

- **Pays de l'espace de travail** : le pays dans lequel vous souhaitez installer votre nouvel espace de travail. Ce paramètre affecte la sélection du centre de données où stocker l'espace de travail.

  Les paramètres **Pays de l'entreprise** et **Pays de l'espace de travail** peuvent être les mêmes.

- **Code d'activation** : le code d'activation que vous recevez après l'achat de Kaspersky Security Center Cloud Console. Assurez-vous que la licence que vous souhaitez acheter couvre tous les appareils clients qui doivent être protégés.

Une fois la demande envoyée, les spécialistes de Kaspersky enregistrent l'entreprise indiquée et créent un espace de travail pour celle-ci. Une fois la création de l'espace de travail terminée, vous recevrez une notification par e-mail. Vous pouvez vous connecter à votre compte sur Kaspersky Security Center Cloud Console pour voir le résultat.

Ouverture de l'espace de travail de Kaspersky Security Center Cloud Console

Dès que vous avez créé un espace de travail pour Kaspersky Security Center Cloud Console, l'espace de travail s'ouvre automatiquement. Par la suite, vous pouvez ouvrir votre espace de travail comme indiqué dans cette section.

Si vous êtes administrateur d'un Serveur d'administration virtuel, vous n'avez accès qu'au Serveur d'administration virtuel. Une fois que vous vous êtes connecté et que vous avez ouvert l'espace de travail, Kaspersky Security Center Cloud Console vous fournit l'interface du Serveur d'administration virtuel. Vous ne pouvez pas basculer sur le Serveur d'administration principal ou sur d'autres Serveurs d'administration secondaires.

L'administrateur d'un Serveur d'administration virtuel doit avoir accès à un seul Serveur d'administration virtuel. Si vous ne disposez pas des droits d'accès sur le Serveur primaire et que vous disposez des droits d'accès sur plusieurs Serveurs virtuels, vous ne pouvez pas vous connecter à Kaspersky Security Center Cloud Console.

Pour ouvrir votre espace de travail dans Kaspersky Security Center Cloud Console :

1. Dans votre navigateur, accédez à Kaspersky Security Center Cloud Console.
2. Connectez-vous à votre compte utilisateur sur Kaspersky Security Center Cloud Console à l'aide de votre nom d'utilisateur et mot de passe.
3. Si vous configurez la vérification en deux étapes, saisissez le code de sécurité unique qui vous est envoyé par SMS ou généré dans votre application d'authentification (selon la méthode de vérification en deux étapes que vous avez configurée).

   La page du portail affiche l'entreprise pour laquelle vous êtes administrateur et la liste de ses espaces de travail.
4. Cliquez sur le nom de l'espace de travail requis ou sur le lien **Accéder à l'espace de travail** pour accéder à l'espace de travail.

   Un espace de travail peut parfois être inaccessible pour raison de maintenance. Dans pareil cas, vous ne pouvez pas accéder à l'espace de travail de Kaspersky Security Center Cloud Console.

   Il est impossible d'accéder à un espace de travail sélectionné pour la suppression.
5. Si l'un des documents juridiques de Kaspersky Security Center Cloud Console a été modifié depuis que vous avez accepté ses conditions générales, la page du portail affiche les documents modifiés.

   Procédez comme suit :

   a. Lisez attentivement les documents affichés.

   b. Si vous acceptez les dispositions des Contrats de licence utilisateur final, cochez les cases en regard des Contrats en question, puis cliquez sur le bouton **J'accepte les dispositions**.

   Si vous n'acceptez pas les dispositions, n'utilisez pas la solution logicielle de Kaspersky sélectionnée.

   Si vous cliquez sur le bouton **Je refuse**, l'opération s'arrête.

Votre espace de travail Kaspersky Security Center Cloud Console s'ouvre.

Retour à la liste des espaces de travail

Après avoir ouvert votre espace de travail, vous pouvez revenir à la page du portail qui contient la liste des espaces de travail enregistrés sous votre compte dans Kaspersky Security Center Cloud Console.

Pour revenir à la liste des espaces de travail, procédez comme suit :

Dans le menu principal, accédez aux paramètres de votre compte et sélectionnez **Gérer les espaces de travail**.

La page du portail affiche l'entreprise pour laquelle vous êtes administrateur et la liste de ses espaces de travail. Si Kaspersky Security Center Cloud Console est ouvert sur plusieurs onglets, vous êtes déconnecté de tous les onglets.

Déconnexion de Kaspersky Security Center Cloud Console

Lorsque vous avez terminé votre travail, vous devez fermer la session en cours de manière sécurisée en vous déconnectant de Kaspersky Security Center Cloud Console.

Pour vous déconnecter de Kaspersky Security Center Cloud Console,

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

Kaspersky Security Center Cloud Console se ferme, et la page du compte s'affiche. Vous pouvez fermer cette page du navigateur, si nécessaire. Toutes les données de votre espace de travail seront enregistrées.

Gestion de l'entreprise et la liste des espaces de travail

Cette section décrit comment afficher les informations sur l'entreprise et la liste des espaces de travail enregistrés sous votre compte sur Kaspersky Security Center Cloud Console, comment modifier les informations sur l'entreprise et les espaces de travail, et comment supprimer un espace de travail et une entreprise.

À l'heure actuelle, vous ne pouvez enregistrer qu'une seule entreprise et créer un espace de travail. Dans les futures versions de Kaspersky Security Center Cloud Console, vous pourrez créer des espaces de travail supplémentaires pour votre entreprise. Cela vous aidera à mapper la structure de votre entreprise sur des espaces de travail en créant un espace de travail distinct pour chaque succursale de l'entreprise.

Modification d'informations sur une entreprise et un espace de travail

Vous pouvez modifier les informations sur une entreprise et un espace de travail que vous avez spécifié lorsque vous avez ajouté cette entreprise à Kaspersky Security Center Cloud Console.

Pour modifier des informations sur une entreprise et/ou un espace de travail :

1. Dans votre navigateur, accédez à Kaspersky Security Center Cloud Console.
2. Connectez-vous à votre compte utilisateur sur Kaspersky Security Center Cloud Console à l'aide de votre nom d'utilisateur et mot de passe.
3. Si vous configurez la vérification en deux étapes, saisissez le code de sécurité unique qui vous est envoyé par SMS ou généré dans votre application d'authentification (selon la méthode de vérification en deux étapes que vous avez configurée).

   La page du portail affiche l'entreprise pour laquelle vous êtes administrateur et une liste de ses espaces de travail.
4. Si vous souhaitez modifier le nom et la description de l'entreprise, procédez comme suit :

   a. Cliquez sur **Modifier** () dans la zone contenant les informations sur l'entreprise.

b. Modifiez le nom et/ou la description de l'entreprise comme vous le voulez.

c. Cliquez sur **Enregistrer**.

Pour annuler la modification, cliquez sur le bouton **Annuler**.

5. Si vous souhaitez modifier le nom de l'espace de travail, procédez comme suit :

a. Cliquez sur l'icône **Modifier** (✎) dans la zone contenant les informations sur l'espace de travail.

b. Modifiez le nom de l'espace de travail comme vous le souhaitez.

c. Cliquez sur **Enregistrer**.

Pour annuler la modification, cliquez sur le bouton **Annuler**.

Les informations modifiées s'affichent dans Kaspersky Security Center Cloud Console.

Suppression d'un espace de travail et d'une entreprise

Un espace de travail d'entreprise peut être supprimé manuellement ou automatiquement. Une fois le dernier espace de travail supprimé, les informations sur l'entreprise sont également supprimées automatiquement.

Suppression manuelle

Vous pouvez supprimer un espace de travail d'une entreprise si elle a décidé d'arrêter de l'utiliser.

> Une fois l'espace de travail supprimé, toutes les applications de sécurité restent sur les appareils administrées. Par conséquent, avant de supprimer l'espace de travail, nous vous recommandons de désactiver la protection par mot de passe de toutes les applications de sécurité ou de désinstaller les applications de sécurité des appareils administrées.

Pour supprimer un espace de travail et une entreprise :

1. Dans votre navigateur, accédez à Kaspersky Security Center Cloud Console.
2. Connectez-vous à votre compte utilisateur sur Kaspersky Security Center Cloud Console à l'aide de votre nom d'utilisateur et mot de passe.
3. Si vous configurez la vérification en deux étapes, saisissez le code de sécurité unique qui vous est envoyé par SMS ou généré dans votre application d'authentification (selon la méthode de vérification en deux étapes que vous avez configurée).

   La page du portail affiche l'entreprise pour laquelle vous êtes administrateur et une liste de ses espaces de travail.
4. Sélectionnez l'espace de travail que vous souhaitez supprimer.
5. A droite, dans la section contenant l'espace de travail sélectionné, cliquez sur l'icône **Supprimer** (🗑).

   La fenêtre **Supprimer l'espace de travail** s'ouvre.
6. Dans la fenêtre **Supprimer l'espace de travail**, confirmez l'intention de supprimer l'espace de travail.

L'espace de travail est sélectionné pour la suppression. Le groupe d'informations sur l'espace de travail est encadré en rouge.

Le groupe d'informations sur l'espace de travail apparaît également en bas de la page, dans la section **Sélectionnés pour la suppression**.

Vous ne pouvez pas accéder à un espace de travail marqué pour suppression et le gérer.

Si vous n'avez pas réussi à désigner un espace de travail pour sa suppression, contactez le Support Technique de Kaspersky. Après avoir reçu votre requête, un ingénieur du Support Technique de Kaspersky supprimera l'espace de travail et l'entreprise.

Les espaces de travail sélectionnés pour la suppression peuvent se présenter cet état pendant sept jours à compter de la sélection. Après sept jours, ils sont automatiquement supprimés.

Au cours de cette période, vous pouvez forcer la suppression d'un espace de travail sélectionné ou annuler sa suppression.

Pour forcer la suppression d'un espace de travail :

1. Dans votre navigateur, accédez à Kaspersky Security Center Cloud Console.
2. Connectez-vous à votre compte utilisateur sur Kaspersky Security Center Cloud Console à l'aide de votre nom d'utilisateur et mot de passe.
3. Si vous configurez la vérification en deux étapes, saisissez le code de sécurité unique qui vous est envoyé par SMS ou généré dans votre application d'authentification (selon la méthode de vérification en deux étapes que vous avez configurée).

   La page du portail affiche l'entreprise pour laquelle vous êtes administrateur et une liste de ses espaces de travail.
4. Dans la section **Sélectionnés pour la suppression**, cliquez sur l'option **Forcer la suppression** dans le groupe d'informations de l'espace de travail à supprimer.

   La fenêtre **Supprimer l'espace de travail** s'ouvre.
5. Dans la fenêtre **Supprimer l'espace de travail**, saisissez dans le champ de saisie l'identificateur de l'espace de travail que vous voulez supprimer.

   L'identificateur de l'espace de travail est demandé en vue de confirmer que vous ne supprimez pas l'espace de travail par erreur. Une fois l'espace de travail supprimé, il est impossible de le restaurer.

   L'identificateur de l'espace de travail s'affiche dans le bloc des informations sur l'espace de travail sous son nom.
6. Dans la fenêtre **Supprimer l'espace de travail**, cliquez sur le bouton **OK**.

L'espace de travail est supprimé. Toutes les données relatives aux utilisateurs, aux appareils administrés et à leurs paramètres, sont supprimées.

Suppression automatique

Kaspersky Security Center Cloud Console supprime automatiquement un espace de travail :

- 30 jours après l'expiration de la licence d'essai.
- 90 jours après l'expiration de toutes les licences commerciales ou d'abonnement dans le stockage du Serveur d'administration.
- 90 jours après la suppression de la dernière clé de licence (active, réservée ou non utilisée) ajoutée manuellement dans le stockage.

Kaspersky Security Center Cloud Console informe les administrateurs de l'espace de travail 30 jours, 7 jours et 1 jour avant la suppression.

Annulation de la suppression de l'espace de travail

Vous pouvez annuler la suppression de l'espace de travail marqué pour la suppression.

Il est impossible d'annuler la suppression d'un espace de travail qui était supprimé.

Pour annuler la suppression de l'espace de travail, procédez comme suit :

1. Dans votre navigateur, accédez à Kaspersky Security Center Cloud Console.
2. Connectez-vous à votre compte utilisateur sur Kaspersky Security Center Cloud Console à l'aide de votre nom d'utilisateur et mot de passe.
3. Si vous configurez la vérification en deux étapes, saisissez le code de sécurité unique qui vous est envoyé par SMS ou généré dans votre application d'authentification (selon la méthode de vérification en deux étapes que vous avez configurée).

   La page du portail affiche l'entreprise pour laquelle vous êtes administrateur et une liste de ses espaces de travail.
4. Dans la section **Sélectionnés pour la suppression**, cliquez sur le lien **Annuler la suppression** dans le groupe d'informations de l'espace de travail à supprimer.

La suppression de l'espace de travail est annulée. Vous pouvez retourner à l'espace de travail et continuer à l'utiliser.

Gestion de l'accès à l'entreprise et à ses espaces de travail

Cette section contient des informations sur l'octroi et la révocation de l'accès à votre entreprise et à ses espaces de travail.

Kaspersky Security Center Cloud Console vous propose deux niveaux d'accès :

- **Administrateur ;**

  Un utilisateur doté de ce niveau d'accès peut gérer entièrement l'entreprise et ses espaces de travail.
- **Utilisateur**

  Un utilisateur doté de ce niveau d'accès peut afficher la liste des espaces de travail disponibles et entrer dans ceux-ci.

Octroi de l'accès à votre entreprise et à ses espaces de travail

Vous pouvez autoriser l'accès à votre entreprise et à ses espaces de travail si vous souhaitez qu'un autre utilisateur puisse se connecter à votre entreprise et la gérer selon le niveau d'accès sélectionné.

Avant de pouvoir accorder l'accès à un utilisateur, celui-ci doit créer un compte dans Kaspersky Security Center Cloud Console.

Pour donner accès à votre entreprise et à ses espaces de travail :

1. Dans votre navigateur, accédez à Kaspersky Security Center Cloud Console.
2. Connectez-vous à votre compte utilisateur sur Kaspersky Security Center Cloud Console à l'aide de votre nom d'utilisateur et mot de passe.
3. Si vous configurez la vérification en deux étapes, saisissez le code de sécurité unique qui vous est envoyé par SMS ou généré dans votre application d'authentification (selon la méthode de vérification en deux étapes que vous avez configurée).

   La page du portail affiche l'entreprise pour laquelle vous êtes administrateur et une liste de ses espaces de travail.
4. Cliquez sur le lien **Afficher le contrôle d'accès**.

   La liste des comptes ayant accès à l'entreprise se développe.
5. Cliquez sur le lien **Accorder l'accès**.
6. Dans le champ **Adresse email**, indiquez l'adresse email du compte auquel vous souhaitez accorder l'accès.
7. Dans la liste **Niveau d'accès**, sélectionnez le niveau d'accès que vous souhaitez attribuer au compte saisi :

   - **Administrateur ;**

     Un utilisateur doté de ce niveau d'accès peut gérer entièrement l'entreprise et ses espaces de travail.
   - **Utilisateur**

     Un utilisateur doté de ce niveau d'accès peut afficher la liste des espaces de travail disponibles et entrer dans ceux-ci.

   Vous ne pouvez pas accorder plusieurs niveaux d'accès au même compte au sein d'une même entreprise.
8. Cliquez sur le bouton **Accorder**.

Le compte spécifié a accès à votre entreprise et à ses espaces de travail. L'utilisateur peut se connecter à l'entreprise et la gérer selon le niveau d'accès sélectionné.

Si vous avez accordé le niveau d'accès **Utilisateur** au compte, vous devez attribuer un rôle à l'utilisateur ajouté. Dans le cas contraire, l'utilisateur ne pourra pas entrer dans l'espace de travail.

Révocation de l'accès à votre entreprise et à ses espaces de travail

Vous pouvez révoquer l'accès à votre entreprise et à ses espaces de travail si vous ne souhaitez plus qu'un utilisateur puisse se connecter à votre entreprise et la gérer (par exemple, après que l'utilisateur a quitté l'entreprise).

Vous ne pouvez pas révoquer votre propre accès à l'entreprise.

Pour révoquer l'accès à votre entreprise et à ses espaces de travail :

1. Dans votre navigateur, accédez à Kaspersky Security Center Cloud Console.
2. Connectez-vous à votre compte utilisateur sur Kaspersky Security Center Cloud Console à l'aide de votre nom d'utilisateur et mot de passe.
3. Si vous configurez la vérification en deux étapes, saisissez le code de sécurité unique qui vous est envoyé par SMS ou généré dans votre application d'authentification (selon la méthode de vérification en deux étapes que vous avez configurée).

   La page du portail affiche l'entreprise pour laquelle vous êtes administrateur et une liste de ses espaces de travail.
4. Cliquez sur le lien **Afficher le contrôle d'accès**.

   La liste des comptes ayant accès à l'entreprise se développe.
5. Cliquez sur l'icône **Révoquer** (🗑) en regard du compte dont vous souhaitez révoquer l'accès.
6. Dans la fenêtre **Révoquer l'accès à l'entreprise** qui s'ouvre, cliquez sur **OK** pour valider l'opération.

L'accès du compte sélectionné à votre entreprise et à ses espaces de travail est révoqué. L'utilisateur ne peut plus se connecter à l'entreprise et la gérer.

Réinitialisation de votre mot de passe

Si vous oubliez le mot de passe de votre compte Kaspersky Security Center Cloud Console, vous pouvez rétablir l'accès à votre compte en réinitialisant votre mot de passe.

Pour réinitialiser le mot de passe de votre compte :

1. Dans votre navigateur, accédez à Kaspersky Security Center Cloud Console.
2. Cliquez sur le bouton **S'identifier**.
3. Dans la fenêtre **Connexion à Kaspersky Security Center Cloud Console** du portail Kaspersky Account qui s'ouvre, cliquez sur le lien **Mot de passe oublié ?**.
4. Saisissez l'adresse email que vous avez indiquée lors de la création de votre compte.
5. Cliquez sur **Suivant**.

6. Kaspersky envoie un message à l'adresse email que vous avez renseignée. Le message contient un code de sécurité à usage unique.

   Ouvrez l'email, puis copiez le code de sécurité à usage unique qu'il contient.

7. Revenez à Kaspersky Account, puis collez le code dans le champ de saisie.

8. Si vous avez configuré une question secrète, répondez à cette question.

   Si vous configurez la vérification en deux étapes, saisissez le code de sécurité unique qui vous est envoyé par SMS ou généré dans votre application d'authentification (selon la méthode de vérification en deux étapes que vous avez configurée).

9. Dans la fenêtre qui s'ouvre, saisissez un nouveau mot de passe.

10. Cliquez sur **Enregistrer**.

    Le nouveau mot de passe de connexion à Kaspersky Security Center Cloud Console est enregistré.

Si vous n'avez pas reçu de message électronique, vérifiez l'adresse email que vous avez saisie, votre dossier spam, puis réessayez. Si vous ne recevez pas de message lorsque vous réessayez, l'adresse email que vous avez indiquée n'est probablement pas enregistrée sur le site Internet. Veuillez contacter le Support Technique de Kaspersky.

Modification des paramètres du compte sur Kaspersky Security Center Cloud Console

Cette section explique comment modifier et supprimer un compte sur Kaspersky Security Center Cloud Console.

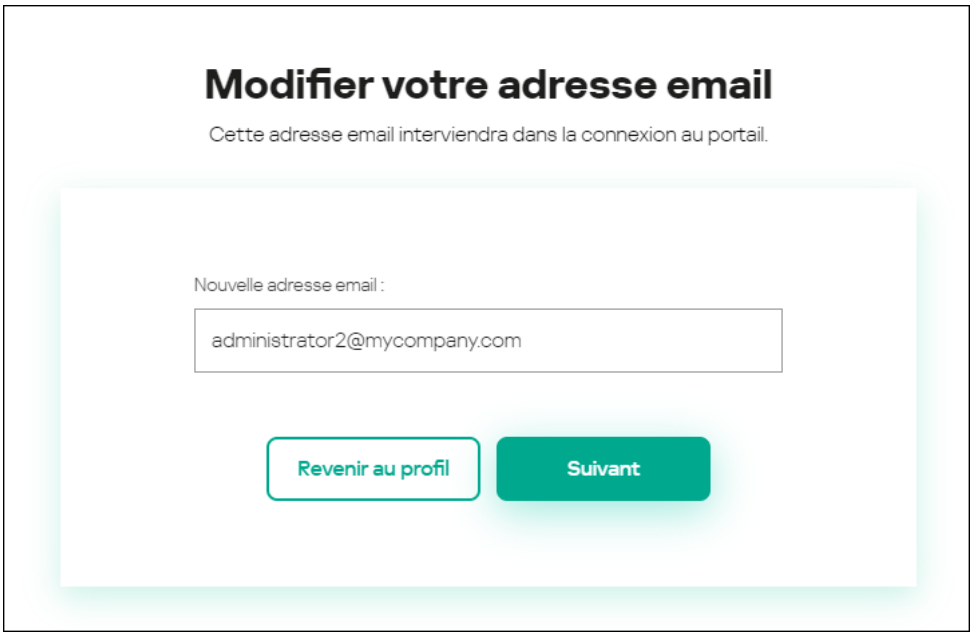
Modification d'une adresse email

Pour modifier l'adresse email dans les paramètres du compte sur le portail Kaspersky Security Center Cloud Console, procédez comme suit :

1. Dans Kaspersky Security Center Cloud Console, cliquez sur le lien contenant le nom de votre compte utilisateur, puis choisissez l'option **Administration du compte**.

   La fenêtre **Mon profil** du portail Kaspersky Account s'ouvre.

2. Cliquez sur le lien **Modifier votre adresse email** (voir la figure ci-dessous).



Modification de l'adresse email dans les paramètres du compte sur Kaspersky Security Center Cloud Console

3. Saisissez votre nouvelle adresse email dans le champ **Nouvelle adresse email**.

   Soyez attentif lors de la saisie de l'adresse email. Si vous commettez une erreur lors de la saisie, vous ne pourrez plus accéder à votre compte et utiliser Kaspersky Security Center Cloud Console.

4. Cliquez sur le bouton **Suivant**.

5. Dans la fenêtre **Saisissez votre mot de passe actuel** qui s'ouvre, indiquez le mot de passe de votre compte dans Kaspersky Security Center Cloud Console, puis cliquez sur le bouton **Suivant**.

6. Kaspersky envoie un message à l'adresse email que vous avez renseignée. Le message contient un code de sécurité à usage unique.

   Ouvrez l'email, puis copiez le code de sécurité à usage unique qu'il contient.

7. Revenez à Kaspersky Account, puis collez le code dans le champ de saisie.

8. Revenez à Kaspersky Security Center Cloud Console en cliquant sur le lien **Revenir à Kaspersky Security Center Cloud Console** ou quittez le portail en cliquant sur le lien **Compte → Se déconnecter**.

Votre adresse email dans les paramètres du compte Kaspersky Security Center Cloud Console et dans les paramètres du compte My Kaspersky est modifiée. Vous recevrez à votre nouvelle adresse email un message vous indiquant que l'adresse email de récupération du compte a été modifiée. La prochaine fois que vous souhaiterez vous connecter à Kaspersky Security Center Cloud Console, il faudra saisir la nouvelle adresse email.

Modification d'un mot de passe

Pour modifier le mot de passe dans les paramètres du compte sur Kaspersky Security Center Cloud Console, procédez comme suit :

1. Dans Kaspersky Security Center Cloud Console, cliquez sur le lien contenant le nom de votre compte utilisateur, puis choisissez l'option **Administration du compte**.

   La fenêtre **Mon profil** du portail Kaspersky Account s'ouvre.

2. Cliquez sur le lien **Modifier le mot de passe** (voir la figure ci-dessous).

Modification du mot de passe d'un compte sur le Kaspersky Security Center Cloud Console

3. Dans le champ de saisie **Mot de passe**, saisissez votre nouveau mot de passe.

   Les exigences relatives au mot de passe sont affichées sous le champ de saisie. Il sera impossible d'enregistrer le mot de passe tant que les exigences n'auront pas été remplies.

4. Cliquez sur **Enregistrer**.

5. Dans la fenêtre **Saisissez votre mot de passe actuel** qui s'ouvre, indiquez le mot de passe de votre compte dans Kaspersky Security Center Cloud Console, puis cliquez sur le bouton **Suivant**.

6. Cochez ou décochez la case **Demander automatiquement la modification du mot de passe tous les 180 jours**.

   Par défaut, cette case est cochée.

7. Revenez à Kaspersky Security Center Cloud Console en cliquant sur le lien **Revenir à Kaspersky Security Center Cloud Console** ou quittez le portail en cliquant sur le lien **Compte → Se déconnecter**.

Votre mot de passe est désormais changé. Par la suite, il faudra saisir le nouveau mot de passe pour ouvrir une session sur Kaspersky Security Center Cloud Console et sur My Kaspersky.

Utilisation de la vérification en deux étapes

Cette section décrit la vérification en deux étapes qui peut vous aider à renforcer la sécurité de votre compte dans Kaspersky Security Center Cloud Console.

À propos de la vérification en deux étapes

La vérification en deux étapes peut vous aider à renforcer la sécurité de votre compte dans Kaspersky Security Center Cloud Console. Lorsque cette fonction est activée, chaque fois que vous vous connectez à Kaspersky Security Center Cloud Console avec votre adresse email et votre mot de passe, vous saisissez un code de sécurité supplémentaire à usage unique. Avec la vérification en deux étapes, les criminels ne peuvent pas se connecter à votre compte ; s'ils volent ou devinent votre mot de passe, ils doivent également avoir accès à votre téléphone mobile. De plus, lorsque la vérification en deux étapes est activée, vous devez saisir un code de sécurité supplémentaire à usage unique si vous oubliez votre mot de passe.

Après avoir configuré la vérification en deux étapes, vous êtes responsable de la sécurité physique de votre téléphone mobile et du maintien de l'accès à votre numéro de téléphone.

Vous pouvez obtenir un code de sécurité unique de l'une des manières suivantes :

- Un code de sécurité est envoyé par SMS à votre numéro de téléphone mobile.

  Dans ce cas, si vous perdez l'accès à votre téléphone mobile, vous ne pourrez pas vous connecter à votre compte dans Kaspersky Security Center Cloud Console tant que vous n'aurez pas rétabli l'accès à votre numéro de téléphone.

- Un code de sécurité est généré dans une application d'authentification qui est installée sur votre téléphone mobile.

  Nous vous recommandons vivement de configurer la vérification en deux étapes à l'aide d'une application d'authentification. Dans ce cas, vous pouvez vous connecter à votre compte même si votre téléphone mobile n'est pas connecté à Internet ou à un réseau mobile.

  Nous n'avons testé que Google Authenticator et Microsoft Authenticator pour la compatibilité avec Kaspersky Security Center Cloud Console, et ces applications étaient alors libres d'utilisation. Il se peut que les interfaces de ces applications ne soient pas disponibles dans la langue de votre choix. Veuillez également vérifier la conformité des applications avec le RGPD et les politiques de confidentialité avant de les utiliser. Kaspersky n'est en aucun cas parrainé, approuvé ou autrement affilié à l'un des propriétaires de ces applications.

  > Microsoft Authenticator ne peut être installé que sur des appareils mobiles.

  Nous vous recommandons également d'installer une application d'authentification sur un autre appareil que votre téléphone mobile. Cela vous permettra de vous connecter à votre compte si jamais votre téléphone mobile est perdu ou volé.

  Dans ce cas, si vous perdez l'accès à votre téléphone mobile et si aucune application d'authentification n'est installée sur un autre appareil, vous ne pourrez pas vous connecter à votre compte dans Kaspersky Security Center Cloud Console tant que vous n'aurez pas rétabli l'accès à votre numéro de téléphone. Après cela, utilisez le code de sécurité qui vous est envoyé par SMS.

> Si vous avez précédemment configuré une question secrète pour restaurer votre mot de passe en cas de perte, la fonction de question de sécurité sera définitivement désactivée après avoir configuré la vérification en deux étapes.

Scénario : Configuration de la vérification en deux étapes

La vérification en deux étapes peut vous aider à renforcer la sécurité de votre compte dans Kaspersky Security Center Cloud Console. Une fois le scénario de cette section terminé, la vérification en deux étapes de votre compte sera configurée.

Le scénario se déroule par étapes :

1. **Ajout de votre numéro de téléphone**

   À ce stade, vous configurez la vérification en deux étapes par SMS.

2. **Installation et configuration d'une app d'authentification**

   Installer et configurer une application d'authentification.

   Nous vous recommandons vivement de configurer la vérification en deux étapes à l'aide d'une application d'authentification. Dans ce cas, vous pouvez vous connecter à votre compte même si votre téléphone mobile n'est pas connecté à Internet ou à un réseau mobile.

   Nous vous recommandons également d'installer une application d'authentification sur un autre appareil que votre téléphone mobile. Cela vous permettra de vous connecter à votre compte si jamais votre téléphone mobile est perdu ou volé.

3. **Modification de votre numéro de téléphone**

   Si nécessaire, vous pouvez modifier le numéro de téléphone que vous utilisez pour la vérification en deux étapes.

Configuration de la vérification en deux étapes par SMS

Pour configurer la vérification en deux étapes par SMS :

1. Dans Kaspersky Security Center Cloud Console, cliquez sur le lien contenant le nom de votre compte utilisateur, puis choisissez l'option **Administration du compte**.

   La fenêtre **Mon profil** du portail Kaspersky Account s'ouvre.

2. Si la vérification en deux étapes est désactivée, activez le commutateur **La vérification en deux étapes est désactivée**.

3. Dans la fenêtre **Aucun numéro de téléphone fourni** qui s'affiche, cliquez sur le bouton **Confirmer**.

4. Sous la section **Indiquez votre numéro de téléphone mobile**, indiquez le numéro de téléphone mobile que vous souhaitez utiliser pour la vérification en deux étapes, puis cliquez sur le bouton **Fournir un numéro de téléphone**.

   > Vous pouvez utiliser le même numéro de téléphone pour cinq comptes au maximum.

   Un code de sécurité à 6 chiffres est envoyé au numéro de téléphone indiqué.

5. Sous **Saisissez le code de vérification qui a été envoyé au numéro <numéro de téléphone>**, saisissez le code de sécurité reçu.

6. Dans la fenêtre **Saisissez votre mot de passe actuel** qui s'ouvre, indiquez le mot de passe de votre compte dans Kaspersky Security Center Cloud Console, puis cliquez sur le bouton **Suivant**.

La vérification en deux étapes est configurée. Désormais, chaque fois que vous vous connectez avec votre adresse email et votre mot de passe, ou si vous oubliez votre mot de passe, vous devrez saisir un code de sécurité unique que vous recevrez par SMS au numéro de téléphone indiqué.

Vous pouvez maintenant installer et configurer une application d'authentification, changer votre numéro de téléphone ou désactiver la vérification en deux étapes.

Configuration de la vérification en deux étapes à l'aide d'une application d'authentification

Les applications d'authentification ne peuvent pas être utilisées dans Kaspersky Security Center Cloud Console comme méthode de vérification distincte. Vous devez d'abord configurer la vérification en deux étapes par SMS. Si vous désactivez la vérification en deux étapes via votre numéro de téléphone mobile, la vérification via une application d'authentification est automatiquement désactivée. Après avoir configuré la vérification par SMS et via une application, vous pourrez choisir une méthode de vérification sur la page de connexion ou si vous oubliez votre mot de passe.

Pour configurer la vérification en deux étapes par une application d'authentification :

1. Configurez la vérification en deux étapes par SMS.

2. Téléchargez, installez et exécutez l'application d'authentification que vous souhaitez utiliser.

   Nous n'avons testé que Google Authenticator et Microsoft Authenticator pour la compatibilité avec Kaspersky Security Center Cloud Console, et ces applications étaient alors libres d'utilisation. Il se peut que les interfaces de ces applications ne soient pas disponibles dans la langue de votre choix. Veuillez également vérifier la conformité des applications avec le RGPD et les politiques de confidentialité avant de les utiliser. Kaspersky n'est en aucun cas parrainé, approuvé ou autrement affilié à l'un des propriétaires de ces applications.

   > Microsoft Authenticator ne peut être installé que sur des appareils mobiles.

   Si vous le souhaitez, vous pouvez utiliser d'autres applications à vos propres risques. L'application que vous utilisez doit prendre en charge les codes de sécurité à 6 chiffres.

   Nous vous recommandons également d'installer une application d'authentification sur un autre appareil que votre téléphone mobile. Cela vous permettra de vous connecter à votre compte si jamais votre téléphone mobile est perdu ou volé.

3. Dans Kaspersky Security Center Cloud Console, cliquez sur le lien contenant le nom de votre compte utilisateur, puis choisissez l'option **Administration du compte**.

   La fenêtre **Mon profil** du portail Kaspersky Account s'ouvre.

4. Si la vérification en deux étapes est désactivée, activez le commutateur **La vérification en deux étapes est désactivée**.

5. Activez le commutateur **L'application d'authentification est désactivée**.

   La page du portail affiche un code QR.

   Si vous souhaitez configurer l'application d'authentification sur un appareil qui ne permet pas de scanner les codes QR, cliquez sur le lien **Je ne peux pas le scanner**. Une clé secrète à 16 caractères s'affiche.

6. Dans l'application d'authentification sur chaque appareil, scannez le code QR pour créer un compte. Veuillez vous reporter à la documentation de votre application pour plus d'informations.

   Si vous souhaitez configurer l'application d'authentification sur un appareil qui ne permet pas de scanner les codes QR, créez un compte dans l'application d'authentification, puis saisissez la clé secrète affichée.

   Un code de sécurité à 6 chiffres est généré dans vos applications d'authentification.

7. Vérifiez que les codes de sécurité générés dans vos applications sont les mêmes sur chaque appareil.

8. Revenez sur le portail Kaspersky Account, puis cliquez sur le bouton **Suivant**.

9. Saisissez le code de sécurité généré.

10. Dans la fenêtre **Saisissez votre mot de passe actuel** qui s'ouvre, indiquez le mot de passe de votre compte dans Kaspersky Security Center Cloud Console, puis cliquez sur le bouton **Suivant**.

La vérification en deux étapes par une application d'authentification est configurée. Désormais, chaque fois que vous vous connecterez avec votre adresse email et votre mot de passe, ou si vous oubliez votre mot de passe, vous devrez saisir un code de sécurité unique qui est généré dans votre application d'authentification.

Vous pouvez désormais désactiver l'utilisation d'une application d'authentification ou désactiver complètement la vérification en deux étapes.

Modification de votre numéro de téléphone mobile

Pour modifier le numéro de téléphone mobile utilisé dans la vérification en deux étapes par SMS :

1. Dans Kaspersky Security Center Cloud Console, cliquez sur le lien contenant le nom de votre compte utilisateur, puis choisissez l'option **Administration du compte**.

   La fenêtre **Mon profil** du portail Kaspersky Account s'ouvre.

2. Si la vérification en deux étapes est désactivée, activez le commutateur **La vérification en deux étapes est désactivée**.

3. Sous **Numéro de téléphone**, cliquez sur le lien **Changer de numéro de téléphone**.

4. Sous la section **Indiquez votre numéro de téléphone mobile**, indiquez le nouveau numéro de téléphone mobile que vous souhaitez utiliser pour la vérification en deux étapes, puis cliquez sur le bouton **Fournir un numéro de téléphone**.

   Un code de sécurité à 6 chiffres est envoyé au numéro de téléphone indiqué.

5. Sous **Saisissez le code de vérification qui a été envoyé au numéro <numéro de téléphone>**, saisissez le code de sécurité reçu.

Votre numéro de téléphone mobile est modifié. Désormais, les codes de sécurité uniques seront envoyés au nouveau numéro de téléphone.

Désactivation de la vérification en deux étapes

Si vous ne souhaitez plus utiliser la vérification en deux étapes, vous pouvez la désactiver, comme décrit dans cette section.

La désactivation de la vérification en deux étapes diminuera la sécurité de votre compte. Nous vous recommandons vivement de continuer à utiliser la vérification en deux étapes.

Si vous configurez la vérification en deux étapes par SMS, vous pouvez la désactiver. Si vous configurez la vérification en deux étapes par une application d'authentification, vous pouvez désactiver l'utilisation de l'application ou désactiver complètement la vérification en deux étapes.

Pour désactiver l'utilisation de l'application d'authentification :

1. Dans Kaspersky Security Center Cloud Console, cliquez sur le lien contenant le nom de votre compte utilisateur, puis choisissez l'option **Administration du compte**.

   La fenêtre **Mon profil** du portail Kaspersky Account s'ouvre.

2. Désactivez le commutateur **L'application d'authentification est activée**.

3. Dans la fenêtre de confirmation qui s'ouvre, cliquez sur le bouton **Confirmer**.

4. Dans la fenêtre **Saisissez votre mot de passe actuel** qui s'ouvre, indiquez le mot de passe de votre compte dans Kaspersky Security Center Cloud Console, puis cliquez sur le bouton **Suivant**.

L'utilisation de l'application d'authentification est désactivée. Les paramètres de la vérification en deux étapes par une application d'authentification sont supprimés. Vous pouvez désormais supprimer les comptes dans vos applications d'authentification.

Plus tard, vous pourrez à nouveau configurer la vérification en deux étapes via une application d'authentification.

Pour désactiver complètement la vérification en deux étapes :

1. Dans Kaspersky Security Center Cloud Console, cliquez sur le lien contenant le nom de votre compte utilisateur, puis choisissez l'option **Administration du compte**.

   La fenêtre **Mon profil** du portail Kaspersky Account s'ouvre.

2. Désactivez le commutateur **La vérification en deux étapes est activée**.

3. Dans la fenêtre de confirmation qui s'ouvre, cliquez sur le bouton **Confirmer**.

4. Dans la fenêtre **Saisissez votre mot de passe actuel** qui s'ouvre, indiquez le mot de passe de votre compte dans Kaspersky Security Center Cloud Console, puis cliquez sur le bouton **Suivant**.

La vérification en deux étapes est désactivée. Si vous avez utilisé la vérification en deux étapes par une application d'authentification, les paramètres de la vérification en deux étapes sont supprimés. Vous pouvez désormais supprimer les comptes dans vos applications d'authentification.

Plus tard, vous pourrez à nouveau configurer la vérification en deux étapes.

Suppression d'un compte sur Kaspersky Security Center Cloud Console

Si vous souhaitez arrêter d'utiliser Kaspersky Security Center Cloud Console, vous pouvez supprimer votre compte.

Suite à la suppression du compte, toutes les informations associées à ce dernier sont perdues.

Après avoir supprimé votre compte, vous ne pouvez plus accéder à vos espaces de travail dans Kaspersky Endpoint Security Cloud, Kaspersky Security for Microsoft Office 365 et Kaspersky Security Center Cloud Console. Si vous étiez le seul administrateur dans un espace de travail, l'espace de travail sera dûment supprimé. De plus, vous perdez l'accès à votre compte My Kaspersky.

Pour supprimer un compte sur Kaspersky Security Center Cloud Console :

1. Dans Kaspersky Security Center Cloud Console, cliquez sur le lien contenant le nom de votre compte utilisateur, puis choisissez l'option **Administration du compte**.

   La fenêtre **Mon profil** du portail Kaspersky Account s'ouvre.

2. Cliquez sur le lien **Compte** → **Supprimer**.

3. Dans la fenêtre **Supprimer le compte** qui s'ouvre, lisez les informations concernant les conséquences de la suppression du compte, puis cliquez sur le bouton **Supprimer** pour confirmer la suppression du compte.

4. Dans la fenêtre **Saisissez votre mot de passe actuel** qui s'ouvre, indiquez le mot de passe de votre compte dans Kaspersky Security Center Cloud Console, puis cliquez sur le bouton **Suivant**.

Votre compte est supprimé.

A propos du choix des centres de données pour la conservation des informations de Kaspersky Security Center Cloud Console

Un espace de travail pour Kaspersky Security Center Cloud Console est créé en utilisant les serveurs d'un réseau de centres de données mondiaux basé sur une plateforme cloud. Le choix du centre de données pour le placement de l'espace de travail dépend du pays que vous avez indiqué à l'étape de l'enregistrement du lieu de travail dans Kaspersky Security Center Cloud Console (cf. tableau ci-dessous). Les paquets de distribution des applications de sécurité sont placés sur les mêmes serveurs que les espaces de travail.

Mise en conformité du pays où se trouve l'entreprise avec une région de centre de données

Pays où se trouve l'entreprise	Région du centre de données
Argentine	Brésil
Bolivie	Brésil
Brésil	Brésil
Chili	Brésil
Colombie	Brésil
Équateur	Brésil
Guyana	Brésil
Pérou	Brésil
Paraguay	Brésil
Surinam	Brésil
Uruguay	Brésil
Venezuela	Brésil
Antigua et Barbuda	Mexique ou Brésil
Anguilla	Mexique ou Brésil
Aruba	Mexique ou Brésil
Barbade	Mexique ou Brésil
Saint-Barthélemy	Mexique ou Brésil
Pays-Bas caribéens	Mexique ou Brésil
Belize	Mexique ou Brésil
Costa Rica	Mexique ou Brésil
Cuba	Mexique ou Brésil
Curaçao	Mexique ou Brésil

Dominique	Mexique ou Brésil
République dominicaine	Mexique ou Brésil
La Grenade	Mexique ou Brésil
Guadeloupe	Mexique ou Brésil
Guatemala	Mexique ou Brésil
Honduras	Mexique ou Brésil
Haïti	Mexique ou Brésil
Jamaïque	Mexique ou Brésil
Saint-Christophe-et-Niévès	Mexique ou Brésil
Iles Caïmans	Mexique ou Brésil
Sainte-Lucie	Mexique ou Brésil
Saint-Martin	Mexique ou Brésil
Martinique	Mexique ou Brésil
Montserrat	Mexique ou Brésil
Nicaragua	Mexique ou Brésil
Panama	Mexique ou Brésil
Sint Maarten	Mexique ou Brésil
Trinidad et Tobago	Mexique ou Brésil
Saint-Vincent-et-les-Grenadines	Mexique ou Brésil
Iles Vierges (Grande-Bretagne)	Mexique ou Brésil
Japon	Mexique ou Irlande
Canada (Nouveau-Brunswick)	Mexique ou Brésil
Canada (Terre-neuve et Labrador)	Mexique ou Brésil
Canada (Nouvelle-Ecosse)	Mexique ou Brésil
Canada (Ontario)	Mexique ou Brésil
Canada (Ile du Prince Edouard)	Mexique ou Brésil
Canada (Québec)	Mexique ou Brésil
Albanie	Irlande
Bosnie-Herzégovine	Irlande
Bulgarie	Irlande
Biélorussie	Irlande
République tchèque	Irlande
Danemark	Irlande
Estonie	Irlande
Finlande	Irlande
Grande Bretagne	Irlande
Groenland	Irlande
Grèce	Irlande
Croatie	Irlande
Hongrie	Irlande
Irlande	Irlande
Islande	Irlande

Kirghizie	Irlande
Kazakhstan	Irlande
Lituanie	Irlande
Lettonie	Irlande
Moldavie	Irlande
Monténégro	Irlande
Macédoine	Irlande
Mongolie	Irlande
Norvège	Irlande
Pologne	Irlande
Roumanie	Irlande
Serbie	Irlande
Russie	Irlande
Suède	Irlande
Slovénie	Irlande
Slovaquie	Irlande
Tadjikistan	Irlande
Turkménie	Irlande
Ouzbékistan	Irlande
Canada (Alberta)	Mexique ou Brésil
Canada (Colombie Britannique)	Mexique ou Brésil
Canada (Manitoba)	Mexique ou Brésil
Canada (Territoires du Nord-Ouest)	Mexique ou Brésil
Canada (Nunavut)	Mexique ou Brésil
Canada (Yukon)	Mexique ou Brésil
Canada (Saskatchewan)	Mexique ou Brésil
Mexique	Mexique ou Brésil
Autres pays	Irlande

Accès aux serveurs DNS publics

Si l'accès aux serveurs Kaspersky via le système DNS n'est pas possible, Kaspersky Security Center Cloud Console 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. CleanBrowsing (185.228.168.168)

Les requêtes adressées à ces serveurs DNS peuvent contenir des adresses de domaine et l'adresse IP publique des appareils clients, car l'Agent d'administration établit une connexion TCP/UDP avec le serveur DNS. Si Kaspersky Security Center Cloud Console utilise un serveur DNS public, le traitement des données est régi par la politique de confidentialité du service concerné.

Scénario : création d'une hiérarchie de Serveurs d'administration administrés par Kaspersky Security Center Cloud Console

Ce scénario décrit les actions que vous devez effectuer pour créer une hiérarchie de Serveurs d'administration administrés par Kaspersky Security Center Cloud Console, qui remplit ainsi le rôle de Serveur d'administration principal. Cette hiérarchie peut ensuite être utilisée pour la migration des appareils et des objets administrés de Kaspersky Security Center vers Kaspersky Security Center Cloud Console, ainsi que pour l'administration des Serveurs d'administration secondaires et des appareils par Kaspersky Security Center Cloud Console.

Kaspersky Security Center Cloud Console ne peut agir que comme un Serveur d'administration principal, tandis que les Serveurs d'administration fonctionnant sur site ne peuvent agir que comme Serveurs d'administration secondaires. Il n'existe pas d'autres schémas hiérarchiques.

Prérequis

Avant de commencer, assurez-vous que les conditions préalables suivantes sont remplies :

- Mise à jour du Serveur d'administration fonctionnant sur site vers la version 12 ou version ultérieure.
- Installation de Kaspersky Security Center Web Console sur le Serveur d'administration fonctionnant sur site.
- Installation des plug-ins Internet pour les applications que vous avez l'intention d'administrer via Kaspersky Security Center Cloud Console.
- Mise à niveau des applications administrées vers des versions prises en charge par Kaspersky Security Center Cloud Console.
- Vérification que la tâche de téléchargement des mises à jour sur le stockage du Serveur d'administration sur le Serveur d'administration fonctionnant sur site n'a pas pour source de mises à jour le Serveur d'administration principal ; modification des paramètres de la tâche en conséquence, si nécessaire.

Une fois la hiérarchie créée, les stratégies et les tâches en vigueur dans Kaspersky Security Center Cloud Console sont appliquées sur le Serveur d'administration secondaire, remplaçant ainsi ses stratégies et ses tâches existantes. Si vous souhaitez éviter ce comportement, supprimez toutes les stratégies et les tâches de Kaspersky Security Center Cloud Console avant la création de la hiérarchie. Vous pouvez également modifier l'état de chaque stratégie de Kaspersky Security Center Cloud Console en **Inactive** dans ses paramètres et désactiver l'option **Distribuer aux Serveurs d'administration secondaires et virtuels** dans les paramètres de chaque tâche de Kaspersky Security Center Cloud Console.

Vous pouvez supprimer votre hiérarchie de Serveurs d'administration à tout moment, si nécessaire.

Étapes de création d'une hiérarchie

Le scénario de base prévoit un Serveur d'administration secondaire inaccessible sur Internet. Cependant, la série d'actions dans le cadre de certaines des étapes décrites ci-dessous peut varier si le Serveur d'administration secondaire est accessible sur Internet. En outre, certaines étapes doivent être ignorées dans ce cas.

La création d'une hiérarchie de Serveurs d'administration comprend les étapes suivantes :

1. **Récupération du certificat du Serveur d'administration secondaire**

   Si le Serveur d'administration secondaire est accessible sur Internet, ignorez cette étape.

   Dans Kaspersky Security Center Web Console fonctionnant sur site, ouvrez les propriétés du Serveur d'administration et, sous l'onglet **Général**, ouvrez la section **Général**. Cliquez sur le lien **Afficher le certificat du Serveur d'administration**. Le fichier du certificat, au format CER, est automatiquement enregistré dans le dossier indiqué dans les paramètres de votre navigateur.

2. **Récupération des paramètres de connexion et des certificats à partir de Kaspersky Security Center Cloud Console**

   Si le Serveur d'administration secondaire est accessible sur Internet, ignorez cette étape.

   Dans Kaspersky Security Center Cloud Console, ouvrez les propriétés du Serveur d'administration et, sous l'onglet **Général**, ouvrez la section **Hiérarchie des Serveurs d'administration**. Les paramètres de connexion suivants s'affichent :

   - Adresse HDS

     Affiche l'adresse Internet utilisée pour établir la connexion au service de découverte hébergé (HDS).

   - Port HDS

     Affiche le numéro du port utilisé pour la connexion au service HDS.

   La section contient également deux liens :

   - Afficher le certificat du Serveur d'administration

     Cliquez sur ce lien pour lancer le téléchargement de la clé publique du certificat de l'instance de Kaspersky Security Center Cloud Console.

   - Certificat CA de la racine HDS

     Cliquez sur ce lien pour démarrer le téléchargement du fichier au format.pem qui contient une liste de certificats racines de confiance émis par des autorités de certification (CA). Ce fichier est conçu pour être utilisé par le Serveur d'administration secondaire : il est nécessaire pour vérifier le certificat HDS.

   Copiez les paramètres de connexion manuellement (en utilisant le presse-papiers ou toute autre solution pratique) et enregistrez-les dans un fichier au format qui vous convient. Cliquez sur le lien **Afficher le certificat du Serveur d'administration** et attendez que le fichier du certificat soit téléchargé. Cliquez sur le lien **Certificat CA de la racine HDS** et attendez que le fichier contenant la liste de certificats racines de confiance émis par des autorités de certification soit téléchargé. Les deux fichiers sont enregistrés dans le dossier défini dans les paramètres de votre navigateur.

3. **Sélection du Serveur d'administration secondaire pour établir la connexion**

Dans les propriétés du Serveur d'administration, accédez à l'onglet **Serveurs d'administration**. Dans la hiérarchie des groupes d'administration, cochez la case en regard du groupe d'administration qui doit contenir le Serveur d'administration secondaire avec tous ses appareils administrés. Cliquez sur le bouton **Connecter un Serveur d'administration secondaire**.

Sur la page qui s'ouvre, dans le champ **Nom d'affichage du Serveur d'administration secondaire**, indiquez le nom sous lequel le Serveur d'administration secondaire doit être affiché dans la hiérarchie. Il est utilisé uniquement pour votre facilité et peut donc différer du nom réel du Serveur d'administration secondaire, si nécessaire. Cliquez sur **Suivant**.

Si le Serveur d'administration secondaire est accessible sur Internet, vous devez également indiquer l'adresse du Serveur d'administration secondaire dans le champ **Adresse du Serveur d'administration secondaire (facultative)**.

Sur la page suivante, cliquez sur le bouton **Parcourir** et sélectionnez le fichier .pem que vous avez enregistré à partir du Serveur d'administration secondaire. Cliquez sur **Suivant**.

4. **Activation et configuration du serveur proxy**

Les actions décrites dans cette étape sont facultatives. Effectuez-les uniquement si votre connexion nécessite l'utilisation d'un serveur proxy.

Cliquez sur **Suivant**. Sur la page **Paramètres de connexion et d'authentification**, vous pouvez activer et configurer l'utilisation du serveur proxy, si nécessaire. Cochez la case **Utiliser un serveur proxy** et définissez les paramètres de proxy suivants :

- Adresse du serveur proxy

  L'adresse du serveur proxy.

- Nom d'utilisateur

  Le nom d'utilisateur pour se connecter au serveur proxy.

- Mot de passe

  Le mot de passe pour se connecter au serveur proxy.

5. **Définition des paramètres d'authentification et ajout du Serveur d'administration secondaire à la hiérarchie**

Cliquez sur **Suivant**. Sur la page **Identifiants du Serveur d'administration secondaire**, veuillez spécifier les paramètres suivants :

- Nom d'utilisateur

  Le nom d'utilisateur que vous utilisez pour vous connecter au Serveur d'administration secondaire.

- Mot de passe

  Le mot de passe que vous utilisez pour vous connecter au Serveur d'administration secondaire.

Cliquez sur **Suivant** et attendez que le Serveur d'administration secondaire s'affiche dans la hiérarchie.

Si le Serveur d'administration secondaire est accessible sur Internet, il se connecte au Serveur d'administration principal.

Si le Serveur d'administration secondaire est accessible sur Internet et que la connexion entre les deux Serveurs d'administration est établie avec succès, ignorez toutes les étapes suivantes.

Si le Serveur d'administration secondaire n'est pas accessible sur Internet, il devient visible, mais vous devez effectuer des actions supplémentaires sur le Serveur d'administration secondaire pour en prendre le contrôle.

6. **Configuration de la connexion dans Kaspersky Security Center Web Console fonctionnant sur site**

Dans Kaspersky Security Center Web Console fonctionnant sur site, ouvrez les propriétés du Serveur d'administration et, sous l'onglet **Général**, ouvrez la section **Hiérarchie des Serveurs d'administration**. Cochez la case **Ce Serveur d'administration est secondaire dans la hiérarchie**. Dans la liste **Type de Serveur d'administration principal**, sélectionnez l'option **Kaspersky Security Center Cloud Console**.

Kaspersky Security Center Web Console vérifie si le Serveur d'administration principal est défini comme source de mises à jour dans la tâche de *téléchargement des mises à jour sur le stockage du Serveur d'administration*. Si le Serveur d'administration principal est défini comme source de mises à jour, vous obtenez le message d'avertissement correspondant et un lien vers les paramètres de la tâche. Vous pouvez modifier les paramètres, puis revenir à la création de la hiérarchie, ou vous pouvez ignorer cette action et poursuivre la création de la hiérarchie.

Dans le groupe **Paramètres de connexion entre les Serveurs d'administration principal et secondaire**, définissez les paramètres suivants :

- Adresse du serveur HDS (à partir du Serveur d'administration principal sur Cloud Console)

  Saisissez l'adresse du serveur HDS au format Nom de domaine pleinement qualifié (FQDN) que vous avez copiée et enregistrée à partir des propriétés du Serveur d'administration dans Kaspersky Security Center Cloud Console.

- Ports du serveur HDS

  Saisissez le ou les numéros de ports du serveur HDS que vous avez copiés et enregistrés à partir des propriétés du Serveur d'administration dans Kaspersky Security Center Cloud Console.

7. **Ajout des certificats au Serveur d'administration secondaire**

Cliquez sur le bouton **Indiquer le certificat du Serveur d'administration principal** et sélectionnez le fichier de certificat que vous avez enregistré à partir des propriétés du Serveur d'administration dans Kaspersky Security Center Cloud Console.

Cliquez sur le bouton **Indiquer les certificats du service de découverte hébergé** et sélectionnez le fichier .pem que vous avez enregistré à partir des propriétés du Serveur d'administration dans Kaspersky Security Center Cloud Console.

Si vous avez activé l'utilisation du serveur proxy lors de la connexion du Serveur d'administration secondaire dans Kaspersky Security Center Cloud Console, cochez la case **Utiliser un serveur proxy** et définissez les mêmes paramètres de proxy que ceux utilisés dans Kaspersky Security Center Cloud Console.

Vous pouvez également cocher la case **Connecter le Serveur d'administration principal au Serveur d'administration secondaire dans la DMZ** si le Serveur d'administration secondaire est dans une zone démilitarisée (DMZ).

Le Serveur d'administration secondaire se connecte au Serveur d'administration principal.

Résultats

Après avoir effectué les étapes ci-dessus, vous pouvez vous assurer que la hiérarchie est bien créée :

- Les stratégies actives du Serveur d'administration principal prennent effet sur le Serveur d'administration secondaire. Les tâches du Serveur d'administration principal sont distribuées au Serveur d'administration secondaire. Si l'option **Distribuer aux Serveurs d'administration secondaires et virtuels** est activée dans les paramètres d'une tâche de groupe, chacune de ces tâches est également distribuée au Serveur d'administration secondaire.

- Les paramètres de la stratégie qui sont verrouillés contre toute modification sur le Serveur d'administration principal sont affichés comme étant verrouillés contre toute modification dans toutes les stratégies sur le Serveur d'administration secondaire.

- Les stratégies appliquées par le Serveur d'administration principal sont affichées dans la liste des stratégies du Serveur d'administration secondaire (**Ressources (Appareils)** → **Stratégies et profils**).

- Les tâches de groupe distribuées par le Serveur d'administration principal sont affichées dans la liste des tâches du Serveur d'administration secondaire (**Ressources (Appareils)** → **Tâches**).

- Les stratégies et les tâches créées sur le Serveur d'administration principal ne peuvent pas être modifiées sur le Serveur d'administration secondaire.

- Dans Kaspersky Security Center Cloud Console, dans la structure des groupes d'administration, le Serveur d'administration secondaire s'affiche dans le groupe que vous avez sélectionné lors de l'ajout de ce Serveur d'administration.

Migration vers Kaspersky Security Center Cloud Console

Cette section décrit le processus de migration vers Kaspersky Security Center Cloud Console à partir de :

- Kaspersky Security Center Web Console version 12 (ou version ultérieure) fonctionnant sur site.
- Kaspersky Endpoint Security Cloud.

À propos de la migration depuis Kaspersky Security Center Web Console

Cette section décrit le processus de migration à partir de la version 12 (ou une version ultérieure) de Kaspersky Security Center Web Console fonctionnant sur site vers Kaspersky Security Center Cloud Console.

Méthodes de migration vers Kaspersky Security Center Cloud Console

En utilisant la fonctionnalité de migration, vous pouvez transférer vos appareils en réseau de Kaspersky Security Center, dans le cadre d'administration de Kaspersky Security Center Cloud Console. Vos appareils administrés seront commutés sans entraîner la perte des paramètres principaux, comme l'appartenance à des groupes d'administration, ni des objets essentiels, comme les stratégies et les tâches liées aux applications administrées.

Vous pouvez choisir l'une des deux méthodes disponibles pour migrer vos Serveurs d'administration vers Kaspersky Security Center Cloud Console :

- Migration sans hiérarchie de Serveurs d'administration :
  - Permet le transfert des appareils administrés et des objets associés vers Kaspersky Security Center Cloud Console, même si le Serveur d'administration sur site n'est pas un serveur secondaire par rapport à Kaspersky Security Center Cloud Console.
  - Peut nécessiter le transfert de fichiers (sur un disque amovible, par email, via des dossiers partagés ou de toute autre manière appropriée) si Kaspersky Security Center Web Console et Kaspersky Security Center Cloud Console sont ouverts sur différents appareils physiques.

  Vous pouvez également effectuer une migration avec des Serveurs d'administration virtuels si votre réseau en inclut.

- Migration à l'aide de la hiérarchie de Serveurs d'administration :
  - Permet le transfert des appareils administrés et des objets associés vers Kaspersky Security Center Cloud Console en utilisant uniquement l'interface de Kaspersky Security Center Cloud Console afin qu'aucun transfert physique des fichiers ne soit nécessaire.
  - Nécessite que le Serveur d'administration fonctionnant sur site agisse comme serveur secondaire de Kaspersky Security Center Cloud Console. Vous pouvez créer une telle hiérarchie avant de démarrer la migration.

Pour le chiffrement du disque, Kaspersky Security Center Cloud Console prend en charge BitLocker uniquement.

Scénario : migration sans hiérarchie de Serveurs d'administration

Cette section décrit la migration des appareils administrés et des objets associés (tels que les stratégies, les tâches, les rapports) de Kaspersky Security Center Web Console fonctionnant sur site vers Kaspersky Security Center Cloud Console. Vous ne pouvez inclure qu'un seul groupe d'administration dans la zone de migration pour restaurer le même groupe d'administration dans Kaspersky Security Center Cloud Console.

Ce groupe doit contenir les appareils administrés d'un seul système d'exploitation. Si votre réseau comprend les appareils de différents systèmes d'exploitation ou distributifs Linux, répartissez-les dans différents groupes d'administration et effectuez la migration de chaque groupe séparément.

Une fois la migration terminée, tous les Agents d'administration dans la zone de migration sont mis à niveau et administrés par Kaspersky Security Center Cloud Console.

Les étapes indiquées dans cette section couvrent le processus de migration effectué lorsqu'il n'existe aucune hiérarchie des Serveurs d'administration, c'est-à-dire qu'aucune connexion n'a été établie entre Kaspersky Security Center Cloud Console et Kaspersky Security Center Web Console fonctionnant sur site.

Prérequis

Avant de commencer, procédez comme suit :

- Mise à niveau du Serveur d'administration fonctionnant sur site vers la version 14.2 ou version ultérieure.
- Installez Kaspersky Security Center Web Console de version 12.1 ou ultérieure.
- Mettez à jour l'Agent d'administration sur les appareils administrés vers la version 12 ou ultérieure.
- Sur les appareils Windows, utilisez l'Agent d'administration sans mot de passe de désinstallation.

  Si le mot de passe a déjà été défini, effectuez l'une des opérations suivantes dans Kaspersky Security Center Web Console :

  - Désactivez l'option **Utiliser un mot de passe de désinstallation** dans les paramètres de stratégie de l'Agent d'administration.
  - Désinstallez l'Agent d'administration à distance en utilisant la tâche *Désinstallation à distance d'une application*. Dans le champ **Application à désinstaller** de la tâche, puis sélectionnez **Agent d'administration de Kaspersky Security Center**. N'oubliez pas de saisir le mot de passe de désinstallation.
- Mettez à jour les applications administrées vers des versions prises en charge par Kaspersky Security Center Cloud Console.
- Assurez-vous que vous disposez de stratégies pour les dernières versions des applications administrées. Si vous utilisez des stratégies obsolètes, créez-en de nouvelles pour les versions des applications prises en charge par Kaspersky Security Center Cloud Console.
- Pour utiliser les stratégies actuelles, mettez à jour les plug-ins Internet pour les applications que vous avez l'intention d'administrer via Kaspersky Security Center Cloud Console.
- Désinstallez les applications Kaspersky à partir des appareils administrés si ces applications ne sont pas prises en charge par Kaspersky Security Center Cloud Console.

- Déchiffrer toutes les données (au niveau du disque ou au niveau du fichier) qui ont été chiffrées par Kaspersky Endpoint Security for Windows sur les appareils administrés exécutant le système d'exploitation Windows, et désactiver la fonction de chiffrement sur les appareils administrés via la stratégie d'application ou localement. Pour plus d'informations, consulter l'Aide de Kaspersky Endpoint Security for Windows.

  Si un appareil Windows conserve encore des fichiers ou des dossiers chiffrés via Kaspersky Endpoint Security for Windows, la mise à niveau de l'Agent d'administration sera annulée pendant le processus de migration. Une notification vous invitera à déchiffrer toutes les données sur l'appareil et à désactiver la fonctionnalité de chiffrement.

Kaspersky Security Center Cloud Console autorise un maximum de 25 000 appareils administrés par Serveur d'administration.

Étapes de migration

La migration vers Kaspersky Security Center Cloud Console comprend les étapes suivantes :

1. **Planification de la zone de migration et vérification des préaccessoires**

   Estimez la zone d'action du processus de migration, c'est-à-dire, examinez le groupe d'administration à exporter, et évaluez le nombre d'appareils administrés qu'il contient. Assurez-vous également que toutes les activités répertoriées comme conditions indispensables à la migration ont été exécutées avec succès.

2. **Exportation d'appareils administrés, d'objets et de paramètres à partir de Kaspersky Security Center Web Console**

   Utilisez l'assistant de migration de Kaspersky Security Center Web Console fonctionnant sur site pour exporter vos appareils administrés avec leurs objets.

   La taille maximale du fichier d'exportation est de 4 Go.

3. **Importation du fichier d'exportation Kaspersky Security Center Cloud Console**

   Transférez les informations sur vos appareils et objets administrés vers Kaspersky Security Center Cloud Console. Pour cela, utilisez l'assistant de migration de Kaspersky Security Center Cloud Console pour importer le fichier d'exportation et créer un paquet d'installation autonome de l'Agent d'administration.

4. **Réinstallation de l'Agent d'administration sur les appareils administrés**

   Revenez à l'assistant de migration dans Kaspersky Security Center Web Console exécuté sur site pour créer une tâche d'installation à distance. Vous pourrez utiliser cette tâche (immédiatement ou ultérieurement) pour réinstaller l'Agent d'administration sur vos appareils administrés et terminer le processus de migration.

Résultats

Une fois la migration terminée, vous pouvez vous assurer que la migration a réussi de la manière suivante :

- L'Agent d'administration est réinstallé sur tous les appareils administrés.
- Tous les appareils sont administrés via Kaspersky Security Center Cloud Console.
- Tous les paramètres des objets qui étaient en vigueur avant la migration sont conservés.

Assistant de migration

Cette section fournit des informations à propos de l'assistant de migration dans Kaspersky Security Center Cloud Console et dans la version 12 de Kaspersky Security Center Web Console ou une version ultérieure.

Étape 1. Exportation d'appareils administrés, d'objets et de paramètres à partir de Kaspersky Security Center Web Console

La migration des appareils administrés de Kaspersky Security Center Web Console vers Kaspersky Security Center Cloud Console nécessite que vous créiez d'abord un fichier d'exportation contenant les informations sur la hiérarchie des groupes d'administration existant sur votre Serveur d'administration fonctionnant actuellement sur site. Le fichier d'exportation doit également contenir des informations sur les objets et leurs paramètres. Le fichier d'exportation sera utilisé pour une importation ultérieure dans Kaspersky Security Center Cloud Console.

La taille maximale du fichier d'exportation est de 4 Go.

Pour exporter des objets et leurs paramètres à partir de Kaspersky Security Center Web Console, procédez comme suit :

1. Dans le menu principal de Kaspersky Security Center Web Console, accédez à **Opérations** → **Migration**.
2. Sur la page d'accueil de l'assistant de migration, cliquez sur **Suivant**. La page **Appareils administrés à exporter** s'ouvre et affiche la hiérarchie complète des groupes d'administration du Serveur d'administration correspondant.
3. Sur la page **Appareils administrés à exporter**, cliquez sur l'icône en chevron (>) à côté du nom du groupe **Appareils administrés** pour développer la hiérarchie des groupes d'administration. Sélectionnez le groupe d'administration que vous souhaitez exporter.

   Après la migration de Kaspersky Security Center fonctionnant sur site vers Kaspersky Security Center Cloud Console réalisée pour deux groupes d'administration, les Tâches d'installation à distance de ces groupes s'affichent avec le même nom.

4. Sélectionnez les applications administrées dont les stratégies et les tâches doivent être transférées vers Kaspersky Security Center Cloud Console avec les objets de groupe. Pour sélectionner les applications administrées dont les objets doivent être exportés, cochez les cases en regard de leurs noms dans la liste.

   Bien que le Serveur d'administration de Kaspersky Security Center figure dans la liste, le fait de cocher la case correspondante n'entraîne pas l'exportation de ses stratégies.

   Pour vous assurer que vos applications administrées sont prises en charge par Kaspersky Security Center Cloud Console, cliquez sur le lien correspondant. Il vous redirigera vers la rubrique d'aide en ligne contenant la liste des applications administrées par Kaspersky Security Center Cloud Console.

   Si vous sélectionnez des applications qui ne sont pas prises en charge par Kaspersky Security Center Cloud Console, les stratégies et les tâches de ces applications seront de toute façon exportées puis importées, mais vous ne pourrez pas les administrer dans Kaspersky Security Center Cloud Console en raison de l'indisponibilité de plug-ins dédiés.

5. Affichez la liste des objets de groupe exportés par défaut et spécifiez les objets non-groupe à exporter avec le groupe d'administration sélectionné, si nécessaire. Configurez la zone d'exportation en incluant ou en excluant divers objets, tels que les tâches globales, les sélections d'appareils personnalisées, les rapports, les rôles personnalisés, les utilisateurs internes et les groupes de sécurité et les catégories d'applications personnalisées. Cette page comprend les sections suivantes :

   - **Tâches globales**

     Liste des tâches globales des applications administrées ainsi que des tâches globales de l'Agent d'administration.

     Si une tâche globale que vous avez sélectionnée s'applique à une sélection d'objets spécifiques, cette sélection sera également exportée.

     Bien que les tâches globales du Serveur d'administration soient présentes dans la liste, vous ne pouvez pas les exporter ; la sélection de ces tâches n'affecte pas la portée de l'exportation. Les tâches d'installation à distance restent également en dehors de la portée d'exportation, car leurs paquets d'installation respectifs ne peuvent pas être exportés.

   - **Sélections d'appareils**

     La liste des sélections d'appareils personnalisées.

   - **Rapports**

     La liste modifiable des instances de rapport à exporter.

     Si un rapport que vous avez sélectionné s'applique à une sélection d'objets spécifiques, cette sélection sera également exportée.

     Kaspersky Security Center Cloud Console contient le même ensemble de modèles de rapport que Kaspersky Security Center Web Console, vous pouvez donc sélectionner pour l'exportation uniquement les rapports que vous avez créés manuellement ou reconfigurés.

   - **Objets de groupe**

La liste des objets de groupe à exporter par défaut. Les objets suivants liés au groupe d'administration sélectionné seront exportés dans leur intégralité par défaut :

- Structure du groupe d'administration, c'est-à-dire tous les sous-groupes du groupe d'administration sélectionné.
- Appareils inclus dans les groupes d'administration à exporter.
- Balises affectées aux appareils à exporter.

  Si une balise a été créée dans Kaspersky Security Center Web Console, mais qu'elle n'a jamais été attribuée à un appareil, elle ne sera pas exportée. Les règles d'attribution automatique de tags ne seront pas non plus exportées.

- Stratégies de groupe des applications administrées sélectionnées.

  Les stratégies du Serveur d'administration et les stratégies de l'Agent d'administration ne sont pas exportées.

- Tâches de groupe des applications administrées sélectionnées et tâches de groupe de l'Agent d'administration.

  Les tâches du Serveur d'administration ne sont pas exportées.

Vous pouvez également empêcher certains types d'objets non-groupe d'être exportés :

- Pour annuler l'exportation des rôles personnalisés (c'est-à-dire ceux créés par l'utilisateur uniquement), cochez la case **Exclure les rôles personnalisés de l'exportation**.
- Pour annuler l'exportation pour les utilisateurs internes et les groupes de sécurité, cochez la case **Exclure les utilisateurs internes et les groupes de sécurité de l'exportation**.
- Pour annuler l'exportation des catégories d'applications personnalisées avec du contenu ajouté manuellement, cochez la case **Exclure les catégories d'applications personnalisées de l'exportation**.

Si vous transférez des appareils de divers systèmes d'exploitation vers Kaspersky Security Center Cloud Console, les objets non-groupe doivent uniquement être migrés une fois.

L'Assistant de migration vérifie le nombre total d'appareils administrés inclus dans le groupe d'administration sélectionné. Si ce nombre dépasse 10 000, le message d'erreur s'affiche. Le bouton **Suivant** restera inactif (grisé) jusqu'à ce que le nombre d'appareils administrés dans le groupe d'administration sélectionné se situe dans la limite.

6. Après avoir défini la zone de migration, cliquez sur **Suivant** pour démarrer le processus d'exportation. La page **Création du fichier d'exportation** s'ouvre. Sur celle-ci, vous pouvez afficher la progression de l'exportation pour chaque type d'objet que vous avez inclus dans la zone de migration. Attendez que les icônes de rafraîchissement (🔄) à côté de tous les éléments de la liste des objets soient remplacées par des coches vertes (✓). Le processus d'exportation se termine et le fichier d'exportation est automatiquement téléchargé

vers l'emplacement de téléchargement par défaut défini dans les paramètres de votre navigateur. Le nom du fichier d'exportation s'affiche dans la partie inférieure de la fenêtre du navigateur.

7. Lorsque la page **Exportation réussie** s'affiche, passez à l'étape suivante effectuée dans Kaspersky Security Center Cloud Console.

> Si vous utilisez Kaspersky Security Center Web Console et Kaspersky Security Center Cloud Console sur différents appareils, vous devrez copier le fichier d'exportation sur un disque amovible ou choisir d'autres moyens de transférer le fichier.

Étape 2. Importation du fichier d'exportation Kaspersky Security Center Cloud Console

Pour transférer des informations relatives aux appareils administrés, aux objets et à leurs paramètres que vous avez exportés à partir de Kaspersky Security Center Web Console, vous devez importer celles-ci dans Kaspersky Security Center Cloud Console déployée dans votre espace de travail. Cela vous permet de créer un paquet d'installation autonome et de l'utiliser pour la réinstallation de l'Agent d'administration sur vos appareils administrés.

> Avant de démarrer l'assistant de migration dans Kaspersky Security Center Cloud Console, assurez-vous que sa langue de localisation actuelle est la même que la langue de Kaspersky Security Center Web Console pendant le processus d'exportation. Changez de langue, si nécessaire.

> Si vous avez précédemment terminé l'assistant de démarrage rapide de l'application dans votre espace de travail Kaspersky Security Center Cloud Console, le groupe **Appareils administrés** comprend les stratégies et les tâches créées avec les paramètres par défaut. Supprimez ces stratégies et tâches avant d'importer celles que vous avez exportées à partir de Kaspersky Security Center Web Console.

Pour importer le fichier d'exportation dans Kaspersky Security Center Cloud Console, procédez comme suit :

1. Dans le menu principal de Kaspersky Security Center Cloud Console, accédez à **Opérations** → **Migration**.

2. Sur la page d'accueil de l'assistant de migration, cliquez sur **Importer**. Dans la fenêtre de l'Explorateur de fichiers qui s'ouvre, sélectionnez le fichier d'exportation en accédant au dossier où il a été enregistré, puis cliquez sur **Ouvrir**. Attendez que l'icône de rafraîchissement (🔄) à côté de l'état de chargement du fichier soit remplacée par une coche verte (✓).

3. Cliquez sur **Suivant**. La page suivante s'ouvre et affiche la hiérarchie complète des groupes d'administration du Serveur d'administration dans Kaspersky Security Center Cloud Console.

4. Cochez la case en regard du groupe d'administration cible dans lequel les objets de groupe doivent être restaurés, puis cliquez sur **Suivant**. L'Assistant de migration affiche une liste des paquets d'installation de l'Agent d'administration disponibles dans Kaspersky Security Center Cloud Console.

5. Sélectionnez le paquet d'installation contenant la version et la localisation correspondante de l'Agent d'administration, puis cliquez sur **Suivant**.

Sélectionnez le paquet d'installation de Kaspersky Network Agent for Windows uniquement si vous avez déjà terminé l'assistant de démarrage rapide de l'application dans votre espace de travail Kaspersky Security Center Cloud Console et si vous effectuez la migration des appareils Windows.

Attendez que l'assistant de migration crée un paquet d'installation autonome. La taille de fichier maximale du paquet d'installation autonome pour l'Agent d'administration est de 200 Mo.

Le fichier est décompressé et téléchargé automatiquement à l'emplacement de téléchargement par défaut défini dans les paramètres de votre navigateur. Les objets de non-groupe et les objets de groupe sont restaurés dans le groupe d'administration cible.

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 vous avez importé l'intégralité du groupe **Appareils administrés**, nous vous recommandons de renommer le sous-groupe nouvellement importé pour éviter toute confusion :

a. Passez à la section **Hiérarchie des groupes**.

b. Cliquez sur le nom du sous-groupe dans l'arborescence des groupes.

c. Dans la fenêtre des propriétés qui s'ouvre, dans le champ **Nom**, saisissez un autre nom (par exemple, " Appareils migrés ").

Nous vous recommandons de vérifier si les objets (stratégies, tâches et appareils administrés) inclus dans la portée de l'exportation ont bien été importés dans Kaspersky Security Center Cloud Console. Pour ce faire, accédez à la section **Ressources (Appareils)** et vérifiez si les objets importés apparaissent sur les listes dans les sous-sections **Stratégies et profils**, **Tâches** et **Appareils administrés**.

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. Après cela, les appareils commencent à passer à Kaspersky Security Center Cloud Console.

6. Cliquez sur **Terminer** pour fermer la fenêtre de l'assistant de migration.

7. Si vous souhaitez rechercher et télécharger à nouveau le paquet d'installation autonome, accédez à **Découverte et déploiement → Déploiement et attribution → Paquets d'installation** et cliquez sur le bouton **Consulter la liste des paquets autonomes**. Dans la liste qui s'ouvre, sélectionnez le paquet d'installation autonome que vous avez créé et cliquez sur le bouton **Télécharger**.

Si vous utilisez Kaspersky Security Center Web Console et Kaspersky Security Center Cloud Console sur différents appareils, vous devez copier le paquet d'installation autonome sur un disque amovible ou choisir d'autres moyens de transférer le fichier.

Étape 3. Réinstallez l'Agent d'administration sur les appareils administrés par Kaspersky Security Center Cloud Console

Après avoir créé le paquet d'installation autonome de l'Agent d'administration, vous pouvez procéder à la création d'une tâche d'installation à distance. L'exécution de cette tâche vous permet de réinstaller l'Agent d'administration sur tous les appareils administrés afin que ces appareils passent sous l'administration de Kaspersky Security Center Cloud Console.

Pour réduire le risque de perte de données, nous vous recommandons d'effectuer d'abord les actions pour un petit groupe d'administration comptant jusqu'à 20 appareils administrés, situés dans le réseau d'entreprise et ne comprenant aucun serveur physique. Après avoir effectué ces actions, vérifiez si la réinstallation s'est terminée correctement et passez à la portée complète de la réinstallation.

Pour créer une tâche d'installation à distance et réinstaller l'Agent d'administration, procédez comme suit :

1. Revenez à l'assistant de migration dans Kaspersky Security Center Web Console fonctionnant sur site.

   Nous vous recommandons d'utiliser l'assistant de migration pour créer une tâche d'installation à distance pour réinstaller l'Agent d'administration comme décrit ci-dessous. S'il est nécessaire d'utiliser une tâche d'installation à distance personnalisée, vous devez d'abord créer manuellement un paquet d'installation personnalisé à partir du paquet d'installation autonome de l'Agent d'administration. Veuillez noter que lors de la création d'un paquet d'installation personnalisé, vous devez spécifier la clé " -s " dans la ligne de commande du fichier exécutable. Sinon, la réinstallation de l'Agent d'administration à partir de ce paquet d'installation personnalisé se termine par une erreur.

   Selon l'état actuel de l'assistant de migration, vous pouvez effectuer l'une des opérations suivantes :

   - Si vous n'avez pas fermé l'assistant de migration après l'exportation et que votre session n'a pas expiré, cliquez sur le bouton **Passer à l'étape 3 de l'Assistant de migration**. Cochez la case **Charger un paquet d'installation autonome**, puis cliquez sur le bouton **Sélectionner un paquet d'installation autonome**. Dans la fenêtre du navigateur qui s'ouvre, spécifiez le paquet d'installation autonome de l'Agent d'administration.

   - Si vous devez redémarrer l'assistant de migration pour une raison quelconque, cochez la case **Charger un paquet d'installation autonome**, puis cliquez sur le bouton **Sélectionner un paquet d'installation autonome**. Dans la fenêtre du navigateur qui s'ouvre, spécifiez le paquet d'installation autonome de l'Agent d'administration. Après cela, l'assistant de migration affiche à nouveau la hiérarchie des groupes d'administration de ce Serveur d'administration. Sélectionnez le même groupe pour lequel vous avez créé le fichier d'exportation, puis cliquez sur **Suivant**.

     L'Assistant de migration vérifie de nouveau le nombre total d'appareils administrés inclus dans le groupe d'administration sélectionné. Si ce nombre dépasse 10 000, le message d'erreur s'affiche. Le bouton **Suivant** restera inactif (grisé) jusqu'à ce que le nombre d'appareils administrés dans le groupe d'administration sélectionné se situe dans la limite.

2. Attendez que le paquet d'installation autonome soit chargé, puis cliquez sur **Suivant**. L'Assistant de migration crée un paquet d'installation personnalisé et une tâche d'installation à distance pour celui-ci. La zone d'action de la tâche comprendra le groupe d'administration que vous avez sélectionné sur la page **Appareils administrés à exporter** ; la planification du lancement de la tâche sera par défaut définie sur **Mode manuel**. L'Assistant de migration affiche la progression de la création. Attendez que les icônes de rafraîchissement (🔄) soient remplacées par des coches vertes (✓), puis cliquez sur **Suivant**.

3. Si nécessaire, cochez la case **Exécuter la tâche d'installation à distance nouvellement créée** (décochée par défaut) pour les appareils du groupe d'administration sélectionné du Serveur d'administration fonctionnant sur site et de tous ses sous-groupes. Dans ce cas, les appareils passeront sous l'administration de Kaspersky Security Center Cloud Console, mais uniquement après la fin de l'installation de l'Agent d'administration. Le chemin d'accès complet sera affiché pour le groupe d'administration dans lequel la tâche sera exécutée.

La tâche ne doit être lancée qu'après la fin de l'importation dans Kaspersky Security Center Cloud Console. Sinon, les noms des appareils peuvent être dupliqués dans la liste.

4. Cliquez sur **Terminer** pour fermer l'assistant de migration et démarrer la tâche d'installation à distance pour les fins suivantes :

   - Mise à niveau des instances de l'Agent d'administration
   - Passage des instances de l'Agent d'administration sous l'administration de Kaspersky Security Center Cloud Console

   Si vous avez laissé la case **Exécuter la tâche d'installation à distance nouvellement créée** décochée, vous pouvez démarrer la tâche plus tard manuellement, si nécessaire.

Vous pouvez vérifier que vous pouvez désormais administrer les instances de l'Agent d'administration migrées via Kaspersky Security Center Cloud Console. Pour ce faire, accédez à **Ressources (Appareils)** → **Appareils administrés**. Assurez-vous que les appareils administrés migrés ont l'icône de confirmation (✓) dans les colonnes **Visible**, **L'Agent d'administration est installé** et **L'Agent d'administration est en cours d'exécution**. Assurez-vous également que ces appareils n'ont pas la description d'état *Non connecté depuis longtemps*.

Migration avec une hiérarchie de Serveurs d'administration

Cette section décrit la migration des appareils administrés et des objets associés de Kaspersky Security Center Web Console fonctionnant sur site vers Kaspersky Security Center Cloud Console. Le processus implique la présence d'une hiérarchie : Kaspersky Security Center Web Console fonctionnant sur site agit comme le Serveur d'administration secondaire et Kaspersky Security Center Cloud Console agit comme le Serveur d'administration principal.

Chaque groupe d'administration que vous transférez vers Kaspersky Security Center Cloud Console doit contenir les appareils administrés d'un seul système d'exploitation. Si votre réseau comprend les appareils de différents systèmes d'exploitation, répartissez-les dans différents groupes d'administration, puis effectuez la migration de chaque groupe séparément.

Une fois la migration terminée, tous les Agents d'administration du groupe compris dans la zone de migration sont mis à niveau et administrés par Kaspersky Security Center Cloud Console.

Avant de commencer, procédez comme suit :

- Mise à niveau du Serveur d'administration fonctionnant sur site vers la version 14.2 ou version ultérieure.
- Installez Kaspersky Security Center Web Console de version 12.1 ou ultérieure.
- Mettez à jour l'Agent d'administration sur les appareils administrés vers la version 12 ou ultérieure.
- Sur les appareils Windows, utilisez l'Agent d'administration sans mot de passe de désinstallation.

  Si le mot de passe a déjà été défini, effectuez l'une des opérations suivantes dans Kaspersky Security Center Web Console :

  - Désactivez l'option **Utiliser un mot de passe de désinstallation** dans les paramètres de stratégie de l'Agent d'administration.

- Désinstallez l'Agent d'administration à distance en utilisant la tâche *Désinstallation à distance d'une application*. Dans le champ **Application à désinstaller** de la tâche, puis sélectionnez **Agent d'administration de Kaspersky Security Center**. N'oubliez pas de saisir le mot de passe de désinstallation.

- Mettez à jour les applications administrées vers des versions prises en charge par Kaspersky Security Center Cloud Console.

- Assurez-vous que vous disposez de stratégies pour les dernières versions des applications administrées. Si vous utilisez des stratégies obsolètes, créez-en de nouvelles pour les versions des applications prises en charge par Kaspersky Security Center Cloud Console.

- Pour utiliser les stratégies actuelles, mettez à jour les plug-ins Internet pour les applications que vous avez l'intention d'administrer via Kaspersky Security Center Cloud Console.

- Désinstallez les applications Kaspersky à partir des appareils administrés si ces applications ne sont pas prises en charge par Kaspersky Security Center Cloud Console.

- Déchiffrer toutes les données (au niveau du disque ou au niveau du fichier) qui ont été chiffrées par Kaspersky Endpoint Security for Windows sur les appareils administrés exécutant le système d'exploitation Windows, et désactiver la fonction de chiffrement sur les appareils administrés via la stratégie d'application ou localement. Pour plus d'informations, consulter l'Aide de Kaspersky Endpoint Security for Windows.

  Si un appareil Windows conserve encore des fichiers ou des dossiers chiffrés via Kaspersky Endpoint Security for Windows, la mise à niveau de l'Agent d'administration sera annulée pendant le processus de migration. Une notification vous invitera à déchiffrer toutes les données sur l'appareil et à désactiver la fonctionnalité de chiffrement.

Kaspersky Security Center Cloud Console autorise un maximum de 25 000 appareils administrés par Serveur d'administration.

Pour migrer vers Kaspersky Security Center Cloud Console, procédez comme suit :

1. Estimez la zone d'action du processus de migration, c'est-à-dire, examinez le groupe d'administration à exporter, et évaluez le nombre d'appareils administrés qu'il contient. Assurez-vous que toutes les activités répertoriées comme conditions indispensables à la migration ont été exécutées avec succès.

2. Dans Kaspersky Security Center Cloud Console, accédez au Serveur d'administration secondaire dont vous souhaitez migrer les appareils administrés.

3. Dans le menu principal, accédez à **Opérations** → **Migration**.

   La page d'accueil de l'assistant de migration s'ouvre.

4. Sur la page d'accueil, cliquez sur le bouton **Suivant**.

   La page **Appareils administrés à exporter** s'ouvre et affiche la hiérarchie complète des groupes d'administration du Serveur d'administration secondaire correspondant.

5. Sur la page **Appareils administrés à exporter**, cliquez sur l'icône en chevron (>) à côté du nom du groupe **Appareils administrés**, puis développez la hiérarchie des groupes d'administration. Sélectionnez le groupe d'administration que vous souhaitez exporter.

L'Assistant de migration vérifie le nombre total d'appareils administrés inclus dans le groupe d'administration sélectionné. Si ce nombre dépasse 10 000, le message d'erreur s'affiche. Le bouton **Suivant** restera inactif (grisé) jusqu'à ce que le nombre d'appareils administrés dans le groupe d'administration sélectionné se situe dans la limite.

6. Sélectionnez les applications administrées dont les stratégies et les tâches doivent être transférées vers Kaspersky Security Center Cloud Console avec les objets de groupe. Pour sélectionner les applications administrées dont les objets doivent être exportés, cochez les cases en regard de leurs noms dans la liste.

   Bien que le Serveur d'administration de Kaspersky Security Center figure dans la liste, le fait de cocher la case correspondante n'entraîne pas l'exportation de ses stratégies.

   Pour vous assurer que vos applications administrées sont prises en charge par Kaspersky Security Center Cloud Console, cliquez sur le lien correspondant. Il vous redirigera vers la rubrique d'aide en ligne contenant la liste des applications administrées par Kaspersky Security Center Cloud Console.

   Si vous sélectionnez des applications qui ne sont pas prises en charge par Kaspersky Security Center Cloud Console, les stratégies et les tâches de ces applications seront de toute façon migrées, mais vous ne pourrez pas les administrer dans Kaspersky Security Center Cloud Console en raison de l'indisponibilité des plug-ins dédiés.

7. Affichez la liste des objets de groupe exportés par défaut. Si nécessaire, vous pouvez également définir des objets non-groupe à exporter avec le groupe d'administration sélectionné, comme les tâches globales, les sélections d'appareils personnalisées, les rapports, les rôles personnalisés, les utilisateurs internes et les groupes de sécurité, et les catégories d'applications personnalisées dont le contenu est ajouté manuellement. Cette page comprend les sections suivantes :

   - **Tâches globales**

     Liste des tâches globales des applications administrées ainsi que des tâches globales de l'Agent d'administration.

     Si une tâche globale que vous avez sélectionnée s'applique à une sélection d'objets spécifiques, cette sélection sera également exportée.

     Bien que les tâches globales du Serveur d'administration soient présentes dans la liste, vous ne pouvez pas les exporter ; la sélection de ces tâches n'affecte pas la portée de l'exportation. Les tâches d'installation à distance restent également en dehors de la portée d'exportation, car leurs paquets d'installation respectifs ne peuvent pas être exportés.

   - **Sélections d'appareils**

     La liste des sélections d'appareils personnalisées.

   - **Rapports**

La liste modifiable des instances de rapport à exporter.

Si un rapport que vous avez sélectionné s'applique à une sélection d'objets spécifiques, cette sélection sera également exportée.

Kaspersky Security Center Cloud Console contient le même ensemble de modèles de rapport que Kaspersky Security Center Web Console, vous pouvez donc sélectionner pour l'exportation uniquement les rapports que vous avez créés manuellement ou reconfigurés.

- Objets de groupe

La liste des objets de groupe à exporter par défaut. Les objets suivants liés au groupe d'administration sélectionné seront exportés dans leur intégralité par défaut :

- Structure du groupe d'administration, c'est-à-dire tous les sous-groupes du groupe d'administration sélectionné.
- Appareils inclus dans les groupes d'administration à exporter.
- Balises affectées aux appareils à exporter.

  Si une balise a été créée dans Kaspersky Security Center Web Console, mais qu'elle n'a jamais été attribuée à un appareil, elle ne sera pas exportée. Les règles d'attribution automatique de tags ne seront pas non plus exportées.
- Stratégies de groupe des applications administrées sélectionnées.

  Les stratégies du Serveur d'administration et les stratégies de l'Agent d'administration ne sont pas exportées.
- Tâches de groupe des applications administrées sélectionnées et tâches de groupe de l'Agent d'administration.

  Les tâches du Serveur d'administration ne sont pas exportées.

Vous pouvez également empêcher certains types d'objets non-groupe d'être exportés :

- Pour annuler l'exportation des rôles personnalisés (c'est-à-dire ceux créés par l'utilisateur uniquement), cochez la case **Exclure les rôles personnalisés de l'exportation**.
- Pour annuler l'exportation pour les utilisateurs internes et les groupes de sécurité, cochez la case **Exclure les utilisateurs internes et les groupes de sécurité de l'exportation**.
- Pour annuler l'exportation des catégories d'applications personnalisées avec du contenu ajouté manuellement, cochez la case **Exclure les catégories d'applications personnalisées de l'exportation**.

Si vous transférez des appareils de divers systèmes d'exploitation vers Kaspersky Security Center Cloud Console, les objets non-groupe doivent uniquement être migrés une fois.

8. Après avoir défini la zone de migration, cliquez sur **Suivant** pour démarrer le processus d'exportation. La page **Création du fichier d'exportation** s'ouvre. Sur celle-ci, vous pouvez afficher la progression de l'exportation pour chaque type d'objet que vous avez inclus dans la zone de migration. Attendez que chaque icône de rafraîchissement (🔄) à côté de tous les éléments de la liste des objets soit remplacée par une coche verte (✓). L'exportation se termine et le fichier d'exportation est automatiquement enregistré dans un dossier temporaire. La page suivante s'ouvre, affichant la hiérarchie complète des groupes d'administration dans Kaspersky Security Center Cloud Console, qui fait office de Serveur d'administration principal.

9. Cochez la case en regard du groupe d'administration dans lequel les objets de groupe doivent être importés, puis cliquez sur **Suivant**. Le fichier est décompressé, et les objets non-groupe et les objets groupe sont restaurés dans le groupe d'administration cible.

   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.

   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. Les objets non-groupe sont également importés.

   Il est impossible de réduire l'assistant de migration et d'effectuer des opérations simultanées lors de l'importation. Attendez que chaque icône de rafraîchissement (🔄) à côté de tous les éléments de la liste des objets soit remplacée par une coche verte (✓) et que l'importation soit terminée. Après cela, les appareils commencent à passer à Kaspersky Security Center Cloud Console.

10. Après la fin de l'importation, l'assistant de migration affiche une liste des paquets d'installation de l'Agent d'administration disponibles dans Kaspersky Security Center Cloud Console pour un système d'exploitation approprié. Sélectionnez le paquet d'installation contenant la version et la localisation correspondante de l'Agent d'administration.

    Sélectionnez le paquet d'installation de Kaspersky Network Agent for Windows uniquement si vous avez déjà terminé l'assistant de démarrage rapide de l'application dans votre espace de travail Kaspersky Security Center Cloud Console et si vous effectuez la migration des appareils Windows.

11. Cliquez sur **Suivant**.

    L'Assistant de migration crée un paquet d'installation autonome (ou utilise un paquet existant) et un paquet d'installation personnalisé fondé sur celui-ci ainsi que la tâche d'installation à distance correspondante. La zone d'action de la tâche comprend le groupe d'administration que vous avez sélectionné sur la page **Appareils administrés à exporter**. La planification du lancement de la tâche est définie à **Mode manuel** par défaut. L'Assistant de migration affiche la progression de la création.

12. Attendez que chaque icône de rafraîchissement (🔄) soit remplacée par une coche verte (✓), puis cliquez sur **Suivant**.

13. Si nécessaire, cochez la case **Exécuter la tâche d'installation à distance nouvellement créée** (décochée par défaut) pour les appareils du groupe d'administration sélectionné de l'instance de Kaspersky Security Center Web Console fonctionnant sur site et de tous ses sous-groupes. Une fois l'installation de l'Agent d'administration terminée, vous pouvez administrer les appareils sélectionnés via Kaspersky Security Center Cloud Console. Le chemin d'accès complet est affiché pour le groupe d'administration dans lequel la tâche doit être exécutée.

La tâche d'installation à distance ne doit être lancée qu'après la fin de l'importation dans Kaspersky Security Center Cloud Console. Dans le cas contraire, il se peut que les appareils soient dupliqués.

14. Cliquez sur **Terminer** pour fermer l'assistant de migration et démarrer la tâche d'installation à distance pour les fins suivantes :

    - Mise à niveau des instances de l'Agent d'administration
    - Administration des instances de l'Agent d'administration via Kaspersky Security Center Cloud Console

    Si vous avez laissé la case **Exécuter la tâche d'installation à distance** décochée, vous pouvez démarrer la tâche plus tard manuellement, si nécessaire.

Vous pouvez vérifier que vous pouvez désormais administrer les instances de l'Agent d'administration migrées via Kaspersky Security Center Cloud Console. Pour ce faire, accédez à **Ressources (Appareils)** → **Appareils administrés**. Assurez-vous que les appareils administrés migrés ont l'icône de confirmation (✓) dans les colonnes **Visible**, **L'Agent d'administration est installé** et **L'Agent d'administration est en cours d'exécution**. Assurez-vous également que ces appareils n'ont pas la description d'état *Non connecté depuis longtemps*.

Scénario : migration d'appareils exécutant des systèmes d'exploitation Linux ou macOS

Cette section décrit la migration des appareils fonctionnant sous les systèmes d'exploitation Linux ou macOS à partir de Kaspersky Security Center Web Console fonctionnant sur site vers Kaspersky Security Center Cloud Console. Les scénarios de base de la migration sans hiérarchie de Serveurs d'administration et la migration avec une telle hiérarchie permet de transférer tous les appareils et les objets associés vers Kaspersky Security Center Cloud Console. Cependant, si votre réseau comprend des appareils fonctionnant non seulement sous Windows, mais également sous Linux ou macOS, vous devez transférer séparément les appareils de chaque type de système d'exploitation. Par conséquent, vous devez effectuer la migration plusieurs fois.

Prérequis

Avant de commencer, procédez comme suit :

- Mettez à jour le Serveur d'administration fonctionnant sur site vers la version 12 Correctif A ou version ultérieure.
- Installez Kaspersky Security Center Web Console de version 12.1 ou ultérieure.
- Mettez à jour l'Agent d'administration sur les appareils administrés vers la version 12 ou ultérieure.
- Mettez à jour les applications administrées vers des versions prises en charge par Kaspersky Security Center Cloud Console.
- Assurez-vous que vous disposez de stratégies pour les dernières versions des applications administrées. Si vous utilisez des stratégies obsolètes, créez-en de nouvelles pour les versions des applications prises en charge par Kaspersky Security Center Cloud Console.

- Pour utiliser les stratégies actuelles, mettez à jour les plug-ins Internet pour les applications que vous avez l'intention d'administrer via Kaspersky Security Center Cloud Console.
- Désinstallez les applications Kaspersky des appareils administrés, si ces applications ne sont pas prises en charge par Kaspersky Security Center Cloud Console, puis remplacez les applications désinstallées par des applications prises en charge.

Kaspersky Security Center Cloud Console autorise un maximum de 25 000 appareils administrés par Serveur d'administration.

Étapes de migration

La migration vers Kaspersky Security Center Cloud Console comprend les étapes suivantes :

1. **Regroupement des appareils administrés par leurs systèmes d'exploitation**

   Si votre réseau comprend des appareils exécutant différents systèmes d'exploitation (Windows, Linux ou macOS), placez les appareils de chaque système d'exploitation dans des groupes d'administration séparés dans Kaspersky Security Center Web Console. Créez aussi un groupe d'administration pour chaque distribution Linux. Par exemple, si vous avez des appareils Debian et Red Hat Linux, répartissez-les dans différents groupes d'administration. Cela vous permettra de réussir la migration car différents paquets d'installation de l'Agent d'administration sont requis pour divers systèmes d'exploitation.

2. **Effectuer séparément la migration de chaque groupe d'administration et de ses objets d'application**

   Les appareils administrés de chaque système d'exploitation doivent migrer séparément pour inclure leurs stratégies et tâches. Par exemple, si vous possédez des appareils Windows, macOS, Ubuntu et CentOS, commencez par transférer les appareils exécutant le système d'exploitation Windows vers Kaspersky Security Center Cloud Console, puis macOS, puis Ubuntu et enfin CentOS. Vous pouvez transférer les appareils administrés dans n'importe quel ordre.

   Pour cela, effectuez la migration sans la hiérarchie des Serveurs d'administration ou la migration avec une telle hiérarchie, selon que votre réseau inclut ou non des Serveurs d'administration secondaires. Lors de la migration, utilisez le paquet d'installation de l'Agent d'administration correspondant au système d'exploitation des appareils transférés. Par exemple, sélectionnez l'Agent d'administration de Kaspersky Security Center 13.2 for Linux pour réussir la migration.

   Notez que les objets non groupés, tels que les tâches globales, les sélections d'appareils personnalisées ou les rapports, n'ont besoin d'être migrés qu'une seule fois.

Résultats

Une fois la migration terminée, vous pouvez vous assurer que la migration a réussi de la manière suivante :

- La version adéquate de l'Agent d'administration est réinstallée sur chaque appareil administré fonctionnant sous le système d'exploitation Linux ou macOS.
- Tous les appareils Linux ou macOS sont administrés par Kaspersky Security Center Cloud Console.
- Tous les paramètres des objets qui étaient en vigueur avant la migration sont conservés.

Scénario : migration inverse de Kaspersky Security Center Cloud Console vers Kaspersky Security Center

Vous souhaiterez peut-être migrer les appareils administrés de Kaspersky Security Center Cloud Console vers le Serveur d'administration de Kaspersky Security Center. Par exemple, ce processus peut être utilisé pour annuler la migration vers Kaspersky Security Center Cloud Console.

Prérequis

Avant de commencer, assurez-vous que les conditions préalables suivantes sont remplies :

- Kaspersky Security Center Cloud Console est disponible et des appareils administrés y sont connectés.
- Le Serveur d'administration de Kaspersky Security Center 14.2 (ou suivant) est disponible et dispose de la version 13 ou d'une version ultérieure d'un paquet d'installation de l'Agent d'administration.

Étapes de la migration inverse

La migration inverse comprend les étapes suivantes :

1. **Création d'un paquet d'installation autonome de l'Agent d'administration dans le Serveur d'administration de Kaspersky Security Center fonctionnant sur site**

   Dans le Serveur d'administration de Kaspersky Security Center fonctionnant sur site, créez un paquet d'installation autonome de l'Agent d'administration.

   Pendant le processus de création, vous pouvez sélectionner l'option **Déplacer les appareils non définis dans ce groupe** pour spécifier un groupe d'administration vers lequel vous souhaitez déplacer les Agents d'administration après l'installation. Si vous avez spécifié le groupe d'administration, une règle de déplacement automatique est créée, qui déplacera vers le groupe d'administration cible tous les Agents d'administration avec ce paquet d'installation autonome.

   > Pour assurer une migration inverse correcte, assurez-vous de sélectionner la version de l'Agent d'administration égale ou ultérieure à la version utilisée dans Kaspersky Security Center Cloud Console.

2. **Création d'un paquet d'installation personnalisé dans Kaspersky Security Center Cloud Console**

   Dans Kaspersky Security Center Cloud Console, créez un paquet d'installation personnalisé sur la base du paquet d'installation autonome que vous avez créé et enregistré à partir du Serveur d'administration de Kaspersky Security Center fonctionnant sur site.

   Pour activer l'installation des paquets en mode silencieux, spécifiez la clé `-s` dans le champ **Ligne de commande du fichier exécutable**.

3. **Création d'une tâche d'installation à distance**

   Dans Kaspersky Security Center Cloud Console, créez une tâche d'installation à distance à l'aide du paquet d'installation personnalisé que vous avez créé.

4. **Exécution de la tâche d'installation à distance**

Démarrez la tâche d'installation à distance que vous avez créée. La tâche lance la réinstallation de tous les Agents d'administration du groupe d'administration spécifié. Elle fait passer également les Agents d'administration sous l'administration d'une instance du Serveur d'administration de Kaspersky Security Center fonctionnant sur site en modifiant l'adresse et d'autres paramètres de connexion.

Si vous n'avez spécifié aucun groupe d'administration cible lors de la création du paquet d'installation autonome, tous les appareils sont déplacés vers le groupe **Appareils non définis**.

Résultats

Une fois la migration terminée, vous pouvez vous assurer que la migration a réussi de la manière suivante :

- Tous les appareils dans la zone d'action de la tâche d'installation à distance qui étaient auparavant administrés par Kaspersky Security Center Cloud Console sont désormais administrés par le Serveur d'administration de Kaspersky Security Center fonctionnant sur site.
- Les appareils sont automatiquement déplacés vers le groupe d'administration spécifié dans les paramètres du paquet d'installation.

La tâche d'installation à distance dans Kaspersky Security Center Cloud Console ne peut pas être terminée : il n'y a plus d'appareils cibles, car tous leurs paramètres de connexion ont été modifiés. Vous devez arrêter la tâche manuellement après vous être assuré que l'icône d'erreur (!) s'est affichée dans la colonne **Visible** de la liste des appareils administrés pour tous les appareils de la zone de migration.

Migration avec des Serveurs d'administration virtuels

Si vous disposez de Serveurs d'administration virtuels dans votre infrastructure Kaspersky Security Center sur site, il est impossible d'effectuer une migration à partir de Kaspersky Security Center sur site vers Kaspersky Security Center Cloud Console à l'aide de l'assistant de migration. De plus, vous ne pourrez migrer que les appareils de vos clients. Vous devrez créer des stratégies, des tâches et des rapports manuellement.

Vous pouvez effectuer l'un des scénarios de migration suivants :

- En déplaçant les appareils de vos clients des Serveurs d'administration virtuels vers un Serveur d'administration principal.
- En effectuant une migration manuelle à partir de Serveurs d'administration virtuels.

Scénario : migration avec des Serveurs d'administration virtuels en déplaçant des appareils

Pour effectuer la migration de Kaspersky Security Center Web Console exécuté sur site vers Kaspersky Security Center Cloud Console, vous pouvez déplacer vos appareils des Serveurs d'administration virtuels vers un Serveur d'administration principal.

Prérequis

Avant la migration, vous devez effectuer un certain nombre d'actions, y compris la mise à niveau du Serveur d'administration fonctionnant sur site vers la version 12 ou ultérieures et la mise à niveau des applications administrées vers des versions prises en charge par Kaspersky Security Center Cloud Console.

Scénario de migration

Le scénario se déroule par étapes :

1. **Création d'un groupe d'administration pour chacun de vos Serveurs d'administration virtuels**

   Vous créez le groupe dans votre instance de Kaspersky Security Center fonctionnant sur site.

2. **Déplacement des appareils de vos clients**

   Dans Kaspersky Security Center fonctionnant sur site, déplacez les appareils de vos clients de chaque Serveur d'administration virtuel vers le groupe d'administration respectif créé à l'étape précédente.

3. **Migration**

   Effectuez la migration comme décrit pour le réseau sans hiérarchie de Serveurs d'administration.

4. **Déplacement des appareils pris en charge par des serveurs d'administration virtuels (étape facultative)**

   Si vous souhaitez gérer vos clients via des serveurs d'administration virtuels, déplacez les appareils des groupes d'administration pris en charge par des serveurs d'administration virtuels.

5. **Créez des stratégies, des tâches et des rapports**

   Créez des stratégies, des tâches et des rapports selon les besoins.

Résultats

Une fois la migration terminée, vous pouvez vous assurer que la migration a réussi de la manière suivante :

- L'Agent d'administration est réinstallé sur tous les appareils administrés.
- Tous les appareils sont administrés via Kaspersky Security Center Cloud Console.
- Tous les paramètres des objets qui étaient en vigueur avant la migration sont conservés.

Scénario : migration manuelle avec des Serveurs d'administration virtuels

Vous pouvez effectuer une migration manuelle à partir de Kaspersky Security Center Web Console exécuté sur site vers Kaspersky Security Center Cloud Console.

Prérequis

Avant la migration, vous devez effectuer un certain nombre d'actions, y compris la mise à niveau du Serveur d'administration fonctionnant sur site vers la version 12 ou ultérieures et la mise à niveau des applications administrées vers des versions prises en charge par Kaspersky Security Center Cloud Console.

Scénario de migration

Le scénario se déroule par étapes :

1. **Création d'un groupe d'administration pour chacun de vos Serveurs d'administration virtuels**

   Dans Kaspersky Security Center Cloud Console, créez un groupe d'administration qui correspond à chacun de vos Serveurs d'administration virtuels.

2. **Création d'un paquet d'installation autonome pour l'Agent d'administration**

   Créez un paquet d'installation autonome pour l'Agent d'administration. Lors de la création, indiquez le groupe d'administration que vous avez créé à l'étape précédente. Cela signifie que vous devez créer un paquet d'installation autonome individuel pour chaque groupe d'administration.

   Cette étape se produit dans Kaspersky Security Center Cloud Console.

3. **Téléchargez les paquets d'installation autonomes**

   Téléchargez les paquets d'installation autonomes que vous avez créés à l'étape précédente. Cette étape se produit dans Kaspersky Security Center Cloud Console.

4. **Création d'une archive avec chaque paquet d'installation autonome**

   Les types d'archives disponibles sont les suivantes : ZIP, CAB, TAR ou TAR.GZ.

5. **Création de paquets d'installation personnalisés pour l'Agent d'administration**

   Créez des paquets d'installation personnalisés pour l'Agent d'administration. Lors de la création, utilisez les archives que vous avez créées à l'étape précédente.

   Cette étape se produit dans votre instance de Kaspersky Security Center fonctionnant sur site.

6. **Création de tâches d'installation à distance**

   Créez des tâches d'installation à distance pour installer l'Agent d'administration à partir des paquets d'installation personnalisés créés.

   Lors de la création d'une tâche, définissez un groupe d'administration correspondant.

   Cette étape se produit dans votre instance de Kaspersky Security Center fonctionnant sur site.

7. **Exécution des tâches d'installation à distance créées**

   Les Agents d'administration sont mis à jour. Le Serveur d'administration de Kaspersky Security Center Cloud Console se charge de leur gestion.

   Tous les appareils sont migrés vers Kaspersky Security Center Cloud Console et placés dans des groupes d'administration qui ont été définis lors de la création des paquets d'installation autonomes pour l'Agent d'administration.

8. **Déplacement des appareils pris en charge par des serveurs d'administration virtuels (étape facultative)**

   Si vous souhaitez gérer vos clients via des serveurs d'administration virtuels, déplacez les appareils des groupes d'administration pris en charge par des serveurs d'administration virtuels.

9. **Créez des stratégies, des tâches et des rapports**

   Créez des stratégies, des tâches et des rapports selon les besoins.

Résultats

Une fois la migration terminée, vous pouvez vous assurer que la migration a réussi de la manière suivante :

- L'Agent d'administration est réinstallé sur tous les appareils administrés.

- Tous les appareils sont administrés via Kaspersky Security Center Cloud Console.

  Tous les paramètres des objets qui étaient en vigueur avant la migration sont conservés.

Scénario : déplacement d'appareils à partir de groupes d'administration sous la gestion de Serveurs virtuels

Vous souhaiterez peut-être gérer vos clients via des serveurs d'administration virtuels. Si vous avez migré des appareils et d'autres éléments de Kaspersky Security Center sur site vers Kaspersky Security Center Cloud Console, ces appareils se trouvent dans des groupes d'administration. Pour gérer les appareils des clients via des Serveurs d'administration virtuels, vous devez déplacer les appareils des groupes d'administration pris en charge par les Serveurs d'administration virtuels.

Prérequis

Vous avez créé un serveur d'administration virtuel pour chacun de vos clients.

Tous les appareils de chaque client sont situés dans un groupe d'administration individuel.

Étapes

Le scénario se déroule par étapes :

1. **Création d'un paquet d'installation autonome pour l'Agent d'administration**

   Basculez vers chacun des Serveurs d'administration virtuels créés, puis créer un paquet d'installation autonome pour l'Agent d'administration. Vous pouvez changer de Serveur d'administration dans le menu principal en cliquant sur l'icône en forme de chevron (›) à droite du nom actuel du Serveur d'administration, puis en sélectionnant le Serveur d'administration voulu.

2. **Téléchargez les paquets d'installation autonomes**

   Téléchargez les paquets d'installation autonomes que vous avez créés à l'étape précédente.

3. **Créez une archive avec chaque paquet d'installation autonome.**

   Les types d'archives disponibles sont les suivantes : ZIP, CAB, TAR ou TAR.GZ.

4. **Création de paquets d'installation personnalisés pour l'Agent d'administration**

   Créez des paquets d'installation personnalisés pour l'Agent d'administration. Lors de la création, utilisez les archives que vous avez créées à l'étape précédente.

   Cette étape intervient sur le Serveur d'administration principal.

5. **Création de tâches d'installation à distance**

   Créez des tâches d'installation à distance pour installer l'Agent d'administration à partir des paquets d'installation personnalisés créés.

   Lors de la création d'une tâche, définissez un groupe d'administration correspondant.

   Cette étape intervient sur le Serveur d'administration principal.

6. **Lancez les tâches d'installation à distance créées.**

Les Agents d'administration sont mis à jour. Les appareils sont déplacés dans le cadre de leur prise en charge par les Serveurs d'administration virtuels.

7. **Créez des stratégies, des tâches et des rapports**

   Créez des stratégies, des tâches et des rapports selon les besoins.

Résultats

Vous pouvez désormais gérer les appareils des clients migrés à l'aide de Serveurs d'administration virtuels.

À propos de la migration depuis Kaspersky Endpoint Security Cloud

Vous pouvez migrer votre espace de travail de Kaspersky Endpoint Security Cloud vers Kaspersky Security Center Cloud Console.

Pour obtenir la description détaillée de la procédure de migration, consultez l'aide de Kaspersky Endpoint Security Cloud.

Une fois que la migration est terminée, un nouvel espace de travail est créé dans Kaspersky Security Center Cloud Console, et vous recevez une notification correspondante par email. Le nouvel espace de travail porte le même nom que l'espace de travail dans Kaspersky Endpoint Security Cloud.

Accédez au nouvel espace de travail et assurez-vous que les objets sont transférés :

- La licence Kaspersky Next s'affiche dans la section **Licence** et dans la fenêtre des propriétés du Serveur d'administration.
- Dans le menu principal, accédez à **Ressources (Appareils)** → **Appareils administrés**.

  Tous les appareils exécutant Windows et macOS sont affichés dans la liste des appareils administrés.

  > Les appareils transférés sont automatiquement connectés à l'espace de travail créé dans Kaspersky Security Center Cloud Console. Cette opération peut prendre un certain temps.

- Dans le menu principal, accédez à **Ressources (Appareils)** → **Stratégies et profils**.

  Dans la liste des stratégies, la stratégie de l'Agent d'administration s'affiche, et la protection par mot de passe est configurée.

Assistant de démarrage rapide de l'application

Cette tâche est créée automatiquement par l'assistant de démarrage rapide de l'application Kaspersky Security Center Cloud Console.

À propos de l'assistant de démarrage rapide de l'application

L'Assistant de démarrage rapide de l'application de Kaspersky Security Center Cloud Console vous permet de créer un ensemble minimal de tâches et de stratégies nécessaires, d'ajuster un minimum de paramètres et de commencer à créer des paquets d'installation d'applications Kaspersky. À l'aide de l'assistant, vous pouvez apporter les modifications suivantes à Kaspersky Security Center Cloud Console :

- Lancer le téléchargement des paquets d'installation pour les applications Kaspersky administrées.
- Créer un paquet d'installation autonome de l'Agent d'administration pour les appareils fonctionnant sous Windows, Linux ou macOS.
- Créer la stratégie de l'Agent d'administration de Kaspersky Security Center.
- Créez la tâche *Téléchargement des mises à jour sur les stockages des points de distribution*.
- Créez des stratégies et des tâches pour les applications Kaspersky administrées.
- Configurer l'interaction avec Kaspersky Security Network (KSN).

Une fois que l'assistant de démarrage rapide de l'application a terminé, des paquets d'installation pour l'Agent d'administration et les applications Kaspersky s'affichent dans la liste **Découverte et déploiement → Déploiement et attribution → Paquets d'installation**.

L'Assistant de démarrage rapide de l'application crée des stratégies pour les applications administrées, telles que Kaspersky Endpoint Security for Windows, à moins que ces stratégies ne soient créées pour le groupe d'appareils administrés. L'Assistant de démarrage rapide de l'application crée des tâches si les tâches portant le même nom n'existent pas pour le groupe d'appareils administrés.

Une fois que vous avez créé un espace de travail de l'entreprise et que vous avez lancé Kaspersky Security Center Cloud Console, l'application vous invite automatiquement à exécuter l'assistant de démarrage rapide de l'application. Vous pouvez aussi lancer l'assistant de démarrage rapide de l'application manuellement à tout moment.

Lancement de l'assistant de démarrage rapide de l'application

Une fois que vous avez créé un espace de travail de l'entreprise et que vous avez lancé Kaspersky Security Center Cloud Console, l'application vous invite automatiquement à exécuter l'assistant de démarrage rapide de l'application. Vous pouvez aussi lancer l'assistant de démarrage rapide de l'application manuellement à tout moment.

Si vous redémarrez l'assistant de démarrage rapide de l'application, les tâches et stratégies créées lors de l'exécution précédente de l'assistant ne sont pas recréées.

Pour lancer manuellement l'assistant de démarrage rapide de l'application, procédez comme suit :

1. Dans le menu principal, cliquez sur l'icône des paramètres ( ) à côté du nom du Serveur d'administration.

La fenêtre des propriétés du Serveur d'administration s'ouvre.

2. Sous l'onglet **Général**, sélectionnez la section **Général**.

3. Cliquez sur **Démarrer l'Assistant de configuration initiale de l'application**.

Vous pouvez également démarrer l'assistant de démarrage rapide de l'application en sélectionnant **Découverte et déploiement → Déploiement et attribution → Assistant de démarrage rapide de l'application**.

L'Assistant vous invite à réaliser la configuration initiale de Kaspersky Security Center Cloud Console. Suivez les instructions de l'assistant. Parcourez les étapes de l'assistant à l'aide du bouton **Suivant**. Utilisez le bouton **Précédent** pour revenir à l'étape précédente de l'assistant.

Étape 1. Sélection des paquets d'installation à télécharger

Dans la liste, sélectionnez les applications Kaspersky à installer sur les appareils clients. Kaspersky Security Center Cloud Console crée des paquets d'installation pour les applications sélectionnées. Ensuite, vous utiliserez les paquets d'installation créés pour installer les applications.

Lors de la sélection d'un paquet d'installation à télécharger, faites attention à la langue : les paquets d'installation sont disponibles dans différentes langues.

Sélectionnez les applications suivantes :

- Agent d'administration de Kaspersky Security Center

  Lors de la sélection des paquets d'installation de l'Agent d'administration, tenez compte des éléments suivants :

  - L'Agent d'administration doit être installé sur chaque appareil client. Par conséquent, sélectionnez un Agent d'administration approprié pour chaque système d'exploitation fonctionnant sur les appareils clients.

  - L'Agent d'administration doit être installé manuellement par un paquet d'installation autonome sur un appareil que vous sélectionnez comme point de distribution. Les points de distribution sont nécessaires pour effectuer un sondage du réseau et une installation à distance des applications de sécurité de Kaspersky sur les appareils clients. Par conséquent, vous devez sélectionner au moins un paquet d'installation de l'Agent d'administration. Pendant que vous passez aux étapes suivantes de l'assistant, Kaspersky Security Center Cloud Console crée le paquet d'installation autonome de l'Agent d'administration.

    Par rapport aux points de distribution basés sur Windows, les points de distribution basés sur Linux et macOS présentent des fonctionnalités limitées. Il est fortement recommandé de sélectionner des ordinateurs Windows comme points de distribution.

    Vous pouvez sélectionner des Agents d'administration pour Windows, Linux et macOS. Si vous sélectionnez un Agent d'administration uniquement pour un système d'exploitation, par exemple macOS, un paquet d'installation autonome sera créé pour le système d'exploitation sélectionné. Si vous sélectionnez un Agent d'administration pour plusieurs systèmes d'exploitation, Kaspersky Security Center Cloud Console crée un seul paquet d'installation autonome en fonction des priorités suivantes : Windows est la plus grande priorité, puis Linux, et enfin macOS. Par exemple, si vous sélectionnez un Agent d'administration pour Linux et macOS, Kaspersky Security Center Cloud Console crée un paquet d'installation autonome pour l'Agent d'administration pour Linux. Vous pouvez créer un paquet d'installation autonome de l'Agent d'administration pour n'importe lequel de ces systèmes d'exploitation manuellement à tout moment.

- Applications de sécurité Kaspersky

  Sélectionnez les paquets d'installation adaptés aux systèmes d'exploitation installés sur les appareils clients de votre organisation.

Étape 2. Configuration des paramètres du serveur proxy

Si votre organisation utilise un serveur proxy pour se connecter à Internet, vous devez indiquer les paramètres du serveur proxy à cette étape de l'assistant. Ces paramètres sont ajoutés au paquet d'installation de l'Agent d'administration. Après l'installation, l'Agent d'administration utilise automatiquement ces paramètres sur chaque appareil client.

Configurez les paramètres suivants de connexion au serveur proxy :

- **Utiliser un serveur proxy**
- **Adresse**
- **Numéro de port**
- **Authentification du serveur proxy**

  Si cette option est activée, les champs de saisie permettent d'indiquer les identifiants pour l'authentification sur le serveur proxy.

  Nous vous recommandons de spécifier les informations d'identification d'un compte disposant des privilèges minimaux requis uniquement pour l'authentification sur le serveur proxy.

  Cette option est Inactif par défaut.

- **Nom d'utilisateur**

  Le nom d'utilisateur du compte à partir duquel la connexion au serveur proxy est effectuée.

  Nous vous recommandons de spécifier les informations d'identification d'un compte disposant des privilèges minimaux requis uniquement pour l'authentification sur le serveur proxy.

- **Mot de passe**

  Le mot de passe du compte à partir duquel la connexion au serveur proxy est effectuée.

  Nous vous recommandons de spécifier les informations d'identification d'un compte disposant des privilèges minimaux requis uniquement pour l'authentification sur le serveur proxy.

Étape 3. Configuration de Kaspersky Security Network

Si, à l'étape précédente de l'assistant, vous avez téléchargé le paquet d'installation de Kaspersky Endpoint Security for Windows, le texte de la Déclaration KSN pour les applications suivantes s'affiche :

- Kaspersky Endpoint Security for Windows
- Kaspersky Security Center installé sur les appareils locaux
- Kaspersky Security Center Cloud Console installé dans l'environnement cloud

Si vous n'avez pas téléchargé le paquet d'installation de Kaspersky Endpoint Security for Windows, la Déclaration KSN de cette application ne s'affiche pas.

En mode d'évaluation, seule la Déclaration KSN pour Kaspersky Endpoint Security for Windows s'affiche.

Lisez attentivement la Déclaration de Kaspersky Security Network. Sélectionnez l'une des options ci-dessous :

- **J'accepte les termes du Kaspersky Security Network**

  Kaspersky Security Center Cloud Console 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 Cloud Console 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.

L'utilisation de KSN est désactivée par défaut. Plus tard, si vous changez d'avis sur l'utilisation de KSN, vous pouvez activer (ou désactiver) l'option correspondante dans la fenêtre des propriétés du Serveur d'administration, dans la section **Paramètres KSN**.

Étape 4. Configuration des paramètres d'administration des mises à jour tierces

Cette étape ne s'affiche pas si la tâche *Recherche de vulnérabilités et de mises à jour requises* existe déjà.

Si vous souhaitez obtenir une liste des mises à jour des applications installées sur les appareils administrés, et une liste des vulnérabilités trouvées et des correctifs recommandés pour celles-ci, activez l'option **Rechercher des mises à jour de logiciels tiers et des correctifs de vulnérabilité**. Si cette option est activée, Kaspersky Security Center Cloud Console crée la tâche *Recherche de vulnérabilités et de mises à jour requises*.

Étape 5. Création de la configuration de base de la protection d'un réseau

À cette étape de l'assistant, cliquez sur le bouton **Créer** pour créer les objets nécessaires à la protection initiale de vos appareils clients.

Kaspersky Security Center Cloud Console effectue deux opérations :

- Création de stratégies et de tâches de base avec des paramètres par défaut

  Les stratégies suivantes sont créées :

  - Stratégie de l'Agent d'administration de Kaspersky Security Center

- Stratégies pour les applications Kaspersky administrées

Les tâches suivantes sont créées :

- Tâche de *Téléchargement des mises à jour sur les stockages des points de distribution*
- Tâche *Recherche de vulnérabilités et de mises à jour requises*

  Cette tâche n'est créée que si vous avez activé l'option **Rechercher des mises à jour de logiciels tiers et des correctifs de vulnérabilité** à l'étape précédente de l'assistant.
- Tâches pour les applications Kaspersky administrées

- Création d'un paquet d'installation autonome pour l'Agent d'administration

  Vous utiliserez ce paquet pour installer l'Agent d'administration sur les points de distribution. Kaspersky Security Center Cloud Console crée le paquet d'installation autonome sur la base du paquet d'installation de l'Agent d'administration que vous avez sélectionné à l'étape précédente de l'assistant. Lors de la création du paquet, vous devez lire et accepter les conditions du CLUF relatif à l'Agent d'administration. Lorsque le paquet d'installation autonome est créé, vous êtes invité à le télécharger sur l'appareil que vous utilisez actuellement.

  La création du paquet d'installation autonome de l'Agent d'administration peut prendre un certain temps. Vous pouvez passer à l'étape suivante de l'assistant. Le processus se poursuivra en mode arrière-plan. Si nécessaire, vous pouvez suivre l'état de téléchargement du paquet d'installation dans la colonne **État du paquet** (**Découverte et déploiement** → **Déploiement et attribution** → **Paquets d'installation**).

  Pour des raisons d'authentification, chaque paquet d'installation autonome est signé à l'aide d'un certificat. Le certificat est réémis de temps en temps. Après chaque procédure de réémission de certificat, Kaspersky Security Center Cloud Console met automatiquement à jour les signatures de tous les paquets d'installation autonomes créés. Une mise à jour de signature automatique ne peut pas être effectuée pour des paquets d'installation autonomes téléchargés. Par conséquent, le certificat expire et une erreur de certificat peut se produire lors de l'installation d'une application à partir d'un paquet d'installation autonome. Dans ce cas, téléchargez à nouveau le paquet d'installation autonome.

Étape 6. Fin de l'assistant de démarrage rapide de l'application

Sur la page de fin de l'assistant de démarrage rapide de l'application, apprenez-en plus sur les opérations supplémentaires que vous devez effectuer pour déployer les applications de sécurité de Kaspersky sur les appareils clients. Suivez les étapes fournies dans le scénario de déploiement initial des applications de Kaspersky.

Déploiement initial des applications Kaspersky

Cette section décrit le déploiement initial des applications Kaspersky sur les appareils clients de votre organisation.

Scénario : Déploiement initial des applications Kaspersky

Ce scénario explique comment installer des applications Kaspersky sur des appareils client dans Kaspersky Security Center Cloud Console. Tout d'abord, vous devez déployer des points de distribution sur votre réseau. À l'aide des points de distribution, vous devez ensuite effectuer un sondage du réseau et détecter les appareils sur votre réseau. Vous pouvez ensuite déployer des applications Kaspersky sur des appareils en réseau.

Une fois le scénario terminé, les applications Kaspersky sont déployées sur les appareils client sélectionnés sur le réseau de votre organisation. Vous pouvez gérer tous les appareils sur lesquels des applications Kaspersky sont installées.

Prérequis

Avant de commencer, assurez-vous que les conditions préalables suivantes sont remplies :

- L'Assistant de démarrage rapide de l'application est terminé.
- Les paquets d'installation de l'Agent d'administration et des applications de sécurité ont été créés.
- L'adresse https://aes.s.kaspersky-labs.com/endpoints/ est incluse dans les exceptions de pare-feu de l'appareil administré.
- Vous disposez d'informations sur les paramètres Internet des appareils clients de votre organisation, ainsi que sur les paramètres de passerelle et de serveur proxy.
- Les appareils clients de votre organisation ne sont pas chiffrés.

Étapes

Le déploiement initial des applications Kaspersky se déroule par étapes :

1. **Sélection d'un appareil qui va jouer le rôle de point de distribution**

   Dans Kaspersky Security Center Cloud Console, un point de distribution est destiné :

   - au sondage réseau et à la recherche d'appareils
   - à l'installation à distance de l'Agent d'administration sur les appareils client
   - à la connexion des appareils clients au Serveur d'administration (lorsqu'un point de distribution agit en tant que passerelle de connexion)

   Sur le réseau de votre organisation, sélectionnez un appareil en tant que point de distribution pour un groupe d'administration. L'appareil sélectionné doit répondre aux exigences d'un point de distribution. En fonction de la quantité d'appareils client dans le réseau de votre organisation, sélectionnez le nombre approprié d'appareils à utiliser comme points de distribution.

2. **Création d'un paquet d'installation autonome pour l'Agent d'administration**

   Créez un paquet d'installation autonome pour que l'Agent d'administration l'installe sur le point de distribution.

   Si vos appareils clients ne disposent pas d'un accès Internet direct pour se connecter au Serveur d'administration, configurez les paramètres du paquet d'installation de l'Agent d'administration, configurez la passerelle de connexion et le serveur proxy.

3. **Installation de l'Agent d'administration sur l'appareil sélectionné pour qu'il serve de point de distribution**

   Fournissez le paquet d'installation autonome pour l'Agent d'administration à l'appareil sélectionné par n'importe quelle méthode. Vous pouvez par exemple copier le paquet d'installation autonome sur un disque amovible (tel qu'un disque flash) ou le placer dans un dossier partagé.

   Dans la fenêtre **Propriétés** du fichier de paquet d'installation autonome, vérifiez que le paquet d'installation autonome de l'Agent d'administration est signé par Kaspersky.

   Exécutez le paquet d'installation autonome pour l'Agent d'administration sur l'appareil sélectionné. L'Agent d'administration est maintenant installé conformément aux paramètres du paquet d'installation de l'Agent d'administration et connecté au Serveur d'administration. L'appareil avec l'Agent d'administration est placé dans le groupe d'administration spécifié lors de la création du paquet d'installation autonome pour l'Agent d'administration.

   > Si vous installez l'Agent d'administration à l'aide d'un paquet d'installation autonome sur un appareil fonctionnant sous Microsoft Windows XP Professional for Embedded Systems 32 bits, l'installation échoue. Pour résoudre ce problème, installez tout d'abord la mise à jour KB2868626 pour Windows XP à partir du site Internet de Microsoft : https://www.catalog.update.microsoft.com/Search.aspx?q=KB2868626.

4. **Affectation de l'appareil avec l'Agent d'administration installé en tant que point de distribution**

   Affectation de l'appareil avec l'Agent d'administration installé en tant que point de distribution.

5. **Configuration et exécution d'un sondage réseau pour le point de distribution**

   Configurez l'interrogation réseau pour le point de distribution avec l'Agent d'administration installé. Vous pouvez aussi configurer le sondage réseau dans la stratégie de l'Agent d'administration.

   Une fois le sondage réseau terminé, les appareils client connectés au réseau de votre organisation sont détectés et placés dans le groupe **Appareils non définis**.

6. **Création de paquets d'installation pour l'Agent d'administration et les applications Kaspersky administrées**

   Si vous n'avez pas lancé l'assistant de démarrage rapide de l'application ou si vous avez ignoré l'étape de création des paquets d'installation, créez des paquets d'installation pour les applications Kaspersky. Vous devez créer des paquets d'installation (aussi bien pour l'Agent d'administration que pour les applications Kaspersky administrées) adaptés au système d'exploitation installé sur les appareils clients du réseau de votre entreprise.

7. **Remplacement des applications de sécurité d'éditeurs tiers**

   Si des applications de sécurité tierces sont installées sur les appareils clients du réseau de votre entreprise, supprimez-les avant l'installation de l'application Kaspersky.

8. **Installation d'applications Kaspersky sur des appareils clients**

   Créez des tâches afin d'installer l'Agent d'administration et les applications Kaspersky administrées sur les appareils clients du réseau de votre entreprise. Lors de la création des tâches, utilisez le type de tâche **Installation à distance d'une application**. Pour la tâche d'installation de l'Agent d'administration, utilisez l'option **En utilisant les ressources du système d'exploitation via les points de distribution**. Pour installer des applications Kaspersky administrées, utilisez l'option **Utilisation de l'Agent d'administration**. Une fois les tâches créées, vous pouvez configurer leurs paramètres. Assurez-vous que la programmation pour chaque tâche répond à vos exigences. Tout d'abord, la tâche pour installer l'Agent d'administration doit être exécutée. Une fois l'Agent d'administration installé sur les appareils clients, vous devez exécuter la tâche d'installation des applications Kaspersky administrées.

En option, vous pouvez créer une tâche d'installation à distance pour installer l'Agent d'administration et les applications Kaspersky administrées sur les appareils clients du réseau de votre entreprise. Dans ce cas, dans le bloc **Paquets d'installation**, utilisez l'option **Sélectionnez le paquet d'installation** et l'option **Sélectionnez l'Agent d'administration** ; dans le bloc **Forcer le téléchargement du paquet d'installation**, utilisez l'option **En utilisant les ressources du système d'exploitation via les points de distribution**.

Vous pouvez également créer plusieurs tâches d'installation à distance pour installer des applications Kaspersky administrées pour différents groupes d'administration ou différentes sélections d'appareils.

Si vous avez des appareils client avec un point de distribution en dehors du réseau, par exemple des ordinateurs portables d'utilisateurs à distance, vous devez créer et fournir le paquet d'installation autonome de l'Agent d'administration à ces appareils client par n'importe quelle méthode. Installez le paquet d'installation autonome de l'Agent d'administration en local sur ces appareils client. Vous pouvez ensuite installer des applications Kaspersky administrées sur les appareils de ces utilisateurs distants en suivant les mêmes instructions que pour les autres appareils détectés par le point de distribution.

Lancez les tâches d'installation à distance.

En option, pour installer les applications Kaspersky, vous pouvez lancer l'Assistant de déploiement de la protection.

9. **Installation de Kaspersky Security for Mobile**

   Si vous prévoyez d'administrer des appareils mobiles d'entreprise, suivez les instructions fournies dans l'aide de Kaspersky Security for Mobile pour obtenir plus d'informations sur le déploiement de Kaspersky Endpoint Security for Android.

10. **Vérification du déploiement initial des applications Kaspersky**

    Générez et affichez le **Rapport sur les versions de l'application Kaspersky**. Assurez-vous que les applications Kaspersky administrées sont installées sur tous les appareils clients de votre organisation.

Pour le chiffrement du disque, Kaspersky Security Center Cloud Console prend en charge BitLocker uniquement.

Création de paquets d'installation pour les applications Kaspersky

Pour déployer les applications Kaspersky sur les appareils en réseau de votre organisation, vous devez créer des paquets d'installation des applications Kaspersky dans Kaspersky Security Center Cloud Console.

Pour créer un paquet d'installation personnalisé Kaspersky :

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 dans la liste des notifications à l'écran. Si des notifications sur un nouveau paquet sont présentes, vous pouvez cliquer sur le lien en regard de la notification et accéder à la liste des paquets d'installation disponibles.

   Une liste des paquets d'installation disponibles sur le Serveur d'administration s'affiche.

2. Cliquez sur **Ajouter**.

L'Assistant de création du paquet d'installation se lance. Parcourez les étapes de l'assistant à l'aide du bouton **Suivant**.

3. Sélectionnez **Générer un paquet d'installation pour une application Kaspersky**.

   Une liste des paquets de distribution disponibles sur les serveurs Web de Kaspersky apparaît.

4. Cliquez sur le nom d'un paquet de distribution, par exemple, **Kaspersky Endpoint Security for Windows (<numéro de version>)**.

   Une fenêtre contenant des informations sur le paquet de distribution s'ouvre.

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 automatiquement en un paquet d'installation, le bouton **Télécharger le paquet de distribution** s'affiche à la place du bouton **Télécharger et créer le paquet d'installation**. Dans ce cas, téléchargez le paquet de distribution, puis utilisez le fichier téléchargé pour créer un paquet d'installation personnalisé.

   Le téléchargement du paquet d'installation se lance. 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, puis passez à l'étape 6 de l'instruction. Par défaut, les Paquets d'installation avec les statuts **En cours** et **Accepter le CLUF** sont placés au début de la liste.

   Si vous prévoyez d'effectuer la migration de Kaspersky Security Center Web Console vers Kaspersky Security Center Cloud Console et que les règles de sécurité de votre organisation exigent l'utilisation d'un proxy lors de l'accès au réseau d'entreprise, le processus de migration peut être affecté. Après avoir créé un paquet d'installation de l'Agent d'administration, vous devez spécifier les paramètres de proxy pour assurer la connexion entre les instances de l'Agent d'administration sur les appareils administrés et votre espace de travail Kaspersky Security Center Cloud Console :

   a. Cliquez sur le nom du paquet d'installation.

   b. Dans la fenêtre des propriétés du paquet d'installation qui s'ouvre, accédez à l'onglet **Paramètres**.

   c. Ouvrez la section **Connexion**.

   d. Sélectionnez l'option **Utiliser un serveur proxy** et remplissez les champs **Adresse du serveur proxy** et **Port du serveur proxy**.

6. Pour certaines applications de Kaspersky, le bouton **Afficher le CLUF** s'affiche pendant le téléchargement. Si c'est le cas, procédez comme suit :

   a. Cliquez sur le bouton **Afficher le CLUF** pour lire le contrat de licence utilisateur final (CLUF).

   b. Lisez le CLUF affiché à l'écran, puis cliquez de nouveau sur le bouton **Accepter**.

      L'installation se poursuit après que vous avez accepté le CLUF. Si vous cliquez sur **Refuser**, le téléchargement cesse.

7. Une fois le téléchargement terminé, cliquez sur le bouton **Fermer** (×) pour fermer la fenêtre contenant les informations sur le paquet de distribution.

Le paquet d'installation est créé. Le paquet d'installation apparaît dans la liste des paquets d'installation.

Vous ne pouvez pas ajouter plusieurs fois un paquet d'installation avec la même langue de localisation. Par exemple, si vous avez déjà ajouté le paquet d'installation de Kaspersky Endpoint Security for Windows (anglais), vous pouvez ajouter des paquets d'installation de Kaspersky Endpoint Security for Windows localisés dans d'autres langues, à l'exception de l'anglais.

Propagation des paquets d'installation sur les Serveurs d'administration secondaires

Pour propager les paquets d'installation sur les Serveurs d'administration secondaires, procédez comme suit :

1. Connectez-vous au Serveur d'administration qui gère les Serveurs d'administration secondaires nécessaires.
2. Lancez la création de la tâche de propagation du paquet d'installation sur les Serveurs d'administration secondaires à l'aide d'un des moyens suivants :
   - Si vous voulez former la tâche pour les Serveurs secondaires du groupe d'administration sélectionné, lancez la création de la tâche de groupe pour ce groupe.
   - Si vous voulez créer une tâche pour un ensemble de Serveurs d'administration secondaires, lancez la création d'une tâche pour un ensemble d'appareils.

   Ceci permet de lancer l'assistant de création d'une tâche. Suivez les instructions de l'assistant.

   Dans la fenêtre **Nouvelle tâche** de l'assistant de création d'une tâche, dans le champ **Type de tâche**, sélectionnez **Diffusion du paquet d'installation**. Vous pouvez également modifier le nom par défaut de la tâche dans le champ **Nom de la tâche**.

   À l'étape suivante, indiquez les Serveurs d'administration secondaires pour la zone d'action de la tâche et suivez les instructions de l'assistant de création d'une tâche. Lorsque vous aurez terminé, l'assistant de création d'une tâche créera la tâche de propagation des paquets d'installation sélectionnés sur les Serveurs d'administration secondaires.

   Lorsque vous créez la tâche Diffusion du paquet d'installation pour les Serveurs d'administration secondaires fonctionnant sur site, la zone d'action de la distribution, à l'exception des paquets d'installation personnalisés, inclut uniquement les paquets d'installation des applications Kaspersky prises en charge par l'instance de Kaspersky Security Center Web Console fonctionnant sur site, quelle que soit l'option de distribution sélectionnée (**Tous les paquets d'installation** ou **Paquets d'installation sélectionnés**).
3. Lancez la tâche manuellement ou attendez son lancement conformément à la planification que vous avez indiquée dans les paramètres de la tâche.

Suite à l'exécution de la tâche, les paquets d'installation sélectionnés seront copiés sur les Serveurs d'administration secondaires.

Création des paquets d'installation autonome pour l'Agent d'administration

Vous et les autres utilisateurs d'appareils dans votre organisation pouvez utiliser des paquets d'installation autonomes pour installer l'Agent d'administration en local sur des appareils. Des paquets d'installation autonomes peuvent être créés pour les appareils fonctionnant sous Windows, Linux ou macOS.

Dans Kaspersky Security Center Cloud Console, vous pouvez créer des paquets d'installation autonomes uniquement pour l'Agent d'administration.

Le paquet d'installation autonome est un fichier exécutable qui peut être envoyé par email 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'Agent d'administration sans l'intervention de Kaspersky Security Center Cloud Console.

Pour l'Agent d'administration pour Linux et pour macOS, le paquet d'installation autonome est un fichier script dont l'extension est .sh. Quand vous exécutez ce fichier, le script décompresse l'archive jointe contenant le paquet d'installation et ses paramètres, puis lance l'installation.

Si vous installez l'Agent d'administration à l'aide d'un paquet d'installation autonome sur un appareil fonctionnant sous Microsoft Windows XP Professional for Embedded Systems 32 bits, l'installation échoue. Pour résoudre ce problème, installez tout d'abord la mise à jour KB2868626 pour Windows XP à partir du site Internet de Microsoft : https://www.catalog.update.microsoft.com/Search.aspx?q=KB2868626.

Pour des raisons d'authentification, chaque paquet d'installation autonome est signé à l'aide d'un certificat. Le certificat est réémis de temps en temps. Après chaque procédure de réémission de certificat, Kaspersky Security Center Cloud Console met automatiquement à jour les signatures de tous les paquets d'installation autonomes créés. Une mise à jour de signature automatique ne peut pas être effectuée pour des paquets d'installation autonomes téléchargés. Par conséquent, le certificat expire et une erreur de certificat peut se produire lors de l'installation d'une application à partir d'un paquet d'installation autonome. Dans ce cas, téléchargez à nouveau le paquet d'installation autonome.

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 s'affiche. Si le paquet d'installation de l'Agent d'administration ne figure pas dans la liste, créez-le manuellement.

2. Dans la liste des paquets d'installation, 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'affiche.

3. Configurez les paramètres du paquet d'installation de l'Agent d'administration si nécessaire, puis fermez la fenêtre de propriétés du paquet d'installation de l'Agent d'administration.

4. 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**.

5. 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**.

6. Assurez-vous que l'option **Installer l'Agent d'administration avec cette application** est activée si vous souhaitez installer l'Agent d'administration avec l'application sélectionnée.

Cette option est activée par défaut. Il est recommandé d'activer cette option si vous n'êtes pas sûr que l'Agent d'administration est installé sur l'appareil. Si l'Agent d'administration est déjà installé sur l'appareil, après l'installation du paquet d'installation autonome avec l'Agent d'administration, l'Agent d'administration est mis à jour vers la version la plus récente.

Si vous désactivez cette option, l'Agent d'administration n'est pas installé sur l'appareil et l'appareil n'est pas administré.

Si un paquet d'installation autonome pour l'application sélectionnée existe déjà sur le Serveur d'administration, l'assistant vous en informe. Dans ce cas, vous devez sélectionner l'une des actions suivantes :

- **Créer un paquet d'installation autonome**. Sélectionnez cette option, par exemple, si vous souhaitez créer un paquet d'installation autonome pour une nouvelle version d'application et que vous souhaitez également conserver un paquet d'installation autonome que vous avez créé pour une version d'application précédente. Le nouveau paquet d'installation autonome est placé dans un autre dossier.

- **Utiliser le paquet d'installation autonome existant**. Sélectionnez cette option si vous souhaitez utiliser un paquet d'installation autonome existant. Le processus de création du paquet n'est pas démarré.

- **Reconstruire le paquet d'installation autonome existant**. Sélectionnez cette option si vous souhaitez créer de nouveau un paquet d'installation autonome pour la même application. Le paquet d'installation autonome est placé dans le même dossier.

7. À l'étape **Déplacement dans la liste des appareils administrés**, l'option **Ne pas déplacer les appareils** est sélectionnée par défaut. Si vous ne souhaitez pas déplacer l'appareil client vers un groupe d'administration après l'installation de l'Agent d'administration, ne modifiez pas l'option.

   Si vous souhaitez déplacer les appareils clients vers un groupe d'administration après l'installation de l'Agent d'administration, sélectionnez l'option **Déplacer les appareils non définis dans ce groupe**, et spécifiez un groupe d'administration vers lequel vous souhaitez déplacer l'appareil client. Par défaut, l'appareil est déplacé vers le groupe **Appareils administrés**.

8. Sélectionnez l'option **Ouvrir la liste des paquets autonomes** si vous souhaitez que la liste des paquets d'installation autonomes soit affichée après la fermeture de l'assistant.

9. Cliquez sur le bouton **Terminer**.

   L'Assistant de création du paquet d'installation autonome se ferme.

Le paquet d'installation autonome de l'Agent d'administration est créé. Le paquet d'installation autonome créé s'affiche alors dans la liste des paquets d'installation autonomes disponibles.

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 :

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 s'affiche.

2. Au-dessus de la liste, cliquez sur le bouton **Consulter la liste des paquets autonomes**.

Une liste des paquets d'installation autonome s'affiche.

Dans la liste des paquets d'installation autonomes, les propriétés de ceux-ci sont affichées comme suit :

- **Nom de l'archive**. Le nom du paquet d'installation autonome formé automatiquement sous le nom de l'application inclus dans le paquet et la version de l'application.
- **Nom du paquet d'installation de l'Agent d'administration**.
- **Version de l'Agent d'administration**.
- **Taille**. Taille du fichier en mégaoctets (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.
- **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.

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 :

- Télécharger un paquet d'installation autonome sur votre appareil en cliquant sur le bouton **Télécharger**.

  Pour des raisons d'authentification, chaque paquet d'installation autonome est signé à l'aide d'un certificat. Le certificat est réémis de temps en temps. Après chaque procédure de réémission de certificat, Kaspersky Security Center Cloud Console met automatiquement à jour les signatures de tous les paquets d'installation autonomes créés. Une mise à jour de signature automatique ne peut pas être effectuée pour des paquets d'installation autonomes téléchargés. Par conséquent, le certificat expire et une erreur de certificat peut se produire lors de l'installation d'une application à partir d'un paquet d'installation autonome. Dans ce cas, téléchargez à nouveau le paquet d'installation autonome.

- Supprimer un paquet d'installation autonome en cliquant sur le bouton **Supprimer**.

Génération des paquets d'installation personnalisés

Vous pouvez utiliser des paquets d'installation personnalisés pour effectuer les opérations suivantes :

- Pour installer n'importe quelle application (comme un éditeur de texte) sur un appareil client utilisant Kaspersky Security Center Cloud Console, 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, dont un fichier exécutable. Un fichier archive est une source permettant de créer un paquet d'installation personnalisé. Le fichier archive contient le ou les fichiers à inclure dans le paquet d'installation personnalisé. En créant un paquet d'installation personnalisé, vous pouvez définir des options de ligne de commande pour installer l'application en mode silencieux par exemple.

Vous ne pouvez pas créer de paquets d'installation personnalisés dans le mode d'essai de Kaspersky Security Center Cloud Console.

Pour créer le paquet d'installation personnalisé :

1. Exécutez une des actions suivantes :

   - Dans le menu principal, accédez à **Découverte et déploiement → Déploiement et attribution → Paquets d'installation**.
   - Dans le menu principal, accédez à **Opérations → Stockages → Paquets d'installation**.

   Une liste des paquets d'installation disponibles sur le Serveur d'administration s'affiche.

2. Cliquez sur **Ajouter**.

   L'Assistant de création du paquet d'installation se lance. Parcourez les étapes de l'assistant à l'aide du bouton **Suivant**.

3. Sélectionnez l'option **Générer un paquet d'installation à partir d'un fichier**.

4. Définissez le nom du paquet d'installation et cliquez sur le bouton **Parcourir**.

   Une fenêtre **Ouvrir** standard permet de choisir un fichier d'archive pour créer le paquet d'installation.

5. Sélectionnez un fichier d'archive situé sur les disques disponibles.

   Vous pouvez charger un fichier d'archive ZIP, CAB, TAR ou TAR.GZ. Il est impossible de créer un paquet d'installation à partir d'un fichier SFX (archive auto-extractible).

   Les fichiers sont téléchargés sur le Serveur d'administration de Kaspersky Security Center Cloud Console.

   Si le Serveur d'administration détecte que l'archive inclut l'application Kaspersky, un message d'erreur s'affiche. Vous pouvez télécharger des paquets d'installation pour les applications Kaspersky à partir des Serveurs Web Kaspersky. Cette opération est disponible en sélectionnant **Opérations → Applications Kaspersky → Versions actuelles des applications**.

6. Si le fichier d'archive sélectionné contient plusieurs fichiers exécutables, sélectionnez un fichier exécutable à exécuter pour installer l'application à l'aide du paquet d'installation créé.

7. Si vous le souhaitez, spécifiez les paramètres de la ligne de commande d'un fichier exécutable.

   Vous pouvez spécifier des paramètres de ligne de commande pour installer l'application à partir du paquet d'installation en mode silencieux par exemple. Reportez-vous à la documentation du fournisseur de l'application pour plus de détails sur les paramètres de ligne de commande.

   La création du paquet d'installation est lancée.

   L'Assistant vous informe lorsque le processus est terminé.

   Si le paquet d'installation n'est pas créé, un message d'erreur s'affiche.

Dans Kaspersky Security Center Cloud Console, la taille totale de l'ensemble des paquets d'installation sur le Serveur d'administration est limitée à 500 Mo. Si la limite de taille totale est dépassée au cours du processus de création d'un paquet d'installation, supprimez les paquets d'installation créés précédemment. La taille du paquet d'installation est indiquée dans ses propriétés.

8. Cliquez sur le bouton **Terminer** pour fermer l'assistant.

Le paquet d'installation personnalisé que vous venez de créer est alors téléchargé sur le 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, vous pouvez afficher les propriétés suivantes d'un paquet d'installation personnalisé :

- **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 personnalisé.
- **Système d'exploitation**. Système d'exploitation pour lequel le paquet d'installation personnalisé est créé.
- **Date de création**. Date de création du paquet d'installation.
- **Date de modification**. Date de modification du paquet d'installation.
- **Type**. Application Kaspersky ou application tierce.

Dans la liste des paquets d'installation, en cliquant sur le lien portant le nom d'un paquet d'installation personnalisé, vous pouvez modifier les paramètres de ligne de commande et le nom du paquet d'installation personnalisé.

Exigences d'un point de distribution

Pour pouvoir traiter un maximum de 10 000 appareils clients, un point de distribution doit répondre à la configuration suivante (une configuration pour banc d'essai est fournie) :

- Processeur : Intel® Core™ i7-7700 CPU, 3,60 GHz 4 noyaux.
- Mémoire vive : 8 Go.
- Espace de stockage disponible : 120 Go.

Par ailleurs, un point de distribution doit disposer d'un accès à Internet et toujours être allumé.

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.

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 lien portant 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 informations de la fenêtre sont regroupées sous forme d'onglets et de sections.

Général

La section **Général** affiche des informations générales sur le paquet d'installation :

- Nom du paquet d'installation
- Nom et version de l'application pour laquelle un paquet d'installation est créé
- Volume du paquet d'installation
- Date de création du paquet d'installation
- Chemin d'accès au dossier de placement du paquet d'installation

Paramètres

Cette section permet de configurer les paramètres nécessaires afin de garantir le fonctionnement de l'Agent d'administration tout de suite après son installation. Les paramètres de cette section sont disponibles uniquement sur les appareils qui tournent sous Windows.

Dans le groupe des paramètres **Dossier de destination**, vous pouvez sélectionner le dossier de l'appareil client où l'Agent d'administration sera installé.

- Installer dans le dossier par défaut

Si cette option a été sélectionnée, l'Agent d'administration sera installé dans le dossier <Drive>:\Program Files\Kaspersky Lab\NetworkAgent. Si ce dossier n'existe pas, alors il sera créé automatiquement.

Cette option est sélectionnée par défaut.

- Installer dans un dossier défini

  Si cette option a été sélectionnée, l'Agent d'administration sera installé dans le dossier indiqué dans le champ de saisie.

Le groupe des paramètres du bas permet de définir le mot de passe pour la tâche d'installation à distance de l'Agent d'administration.

- Utiliser un mot de passe de désinstallation

  Si cette option est activée, cliquez sur le bouton **Modifier** pour saisir le mot de passe de désinstallation de l'application (accessible uniquement pour l'Agent d'administration sur les appareils tournant sous des systèmes d'exploitation Windows).

  Cette option est Inactif par défaut.

- **État**

- 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 cette case est cochée, toutes les mises à jour et correctifs téléchargés pour l'Agent d'administration seront installés automatiquement.

  Si la case est décochée, les mises à jour et les correctifs téléchargés sont installés uniquement après que vous leur avez attribué l'état *Approuvée*. Les mises à jour et les correctifs avec l'état *Non défini* ne sont pas installés.

  Par défaut, la case est cochée.

Connexion

Cette section permet de configurer les paramètres de connexion de l'Agent d'administration au Serveur d'administration :

- **Utiliser un port UDP**

  Port UDP

Dans ce champ, vous pouvez spécifier le port pour connecter le Serveur d'administration à l'Agent d'administration en utilisant le protocole UDP.

Le numéro de port UDP est de 15000 par défaut.

- &Ouvrir les ports de l'Agent d'administration dans le pare-feu Microsoft Windows

  Quand l'option est activée, les ports utilisés par l'Agent d'administration sont ajoutés à la liste des exclusions du Pare-feu Microsoft Windows.

  Cette option est activée par défaut.

- **Ne pas utiliser de serveur proxy**
- **Utiliser un serveur proxy**

  Adresse du serveur proxy

  Port du serveur proxy

- Authentification du serveur proxy

  Si cette option est activée, les champs de saisie permettent d'indiquer les identifiants pour l'authentification sur le serveur proxy.

  Nous vous recommandons de spécifier les informations d'identification d'un compte disposant des privilèges minimaux requis uniquement pour l'authentification sur le serveur proxy.

  Cette option est Inactif par défaut.

  Nom d'utilisateur

  Le nom d'utilisateur du compte à partir duquel la connexion au serveur proxy est effectuée.

  Nous vous recommandons de spécifier les informations d'identification d'un compte disposant des privilèges minimaux requis uniquement pour l'authentification sur le serveur proxy.

  Mot de passe

  Le mot de passe du compte à partir duquel la connexion au serveur proxy est effectuée.

  Nous vous recommandons de spécifier les informations d'identification d'un compte disposant des privilèges minimaux requis uniquement pour l'authentification sur le serveur proxy.

Pour des raisons de compatibilité, il est déconseillé d'indiquer les paramètres de connexion par proxy dans les paramètres du paquet d'installation de l'Agent d'administration.

Avancé

Dans cette section, vous pouvez configurer l'utilisation de la passerelle de connexion et de la machine virtuelle, ainsi que l'enregistrement ou non d'un utilisateur en tant que propriétaire de l'appareil :

- **Se connecter au Serveur d'administration au moyen d'une passerelle de connexion**
- **Adresse de la passerelle**

- **Activer le mode dynamique pour VDI**

  Si cette option est activée, pour l'Agent d'administration installé sur la machine virtuelle, le mode dynamique pour Virtual Desktop Infrastructure (VDI) sera activé.

  Cette option est Inactif par défaut.

- **Optimiser les paramètres pour VDI**

  Si cette option est activée, les fonctionnalités suivantes sont désactivées dans les paramètres de l'Agent d'administration :

  - Réception d'informations sur les logiciels installés
  - Réception d'informations sur la configuration matérielle
  - Réception d'informations sur la présence de vulnérabilités
  - Réception d'informations sur les mises à jour nécessaires

  Cette option est Inactif par défaut.

- **Autoriser l'exécution de l'utilitaire d'enregistrement des utilisateurs après l'installation de l'Agent d'administration**

  Si cette option est activée, l'enregistrement de l'utilisateur en tant que propriétaire de l'appareil sera lancé après l'installation de l'Agent d'administration. Cette option est Inactif par défaut.

Modules complémentaires

Cette section permet de sélectionner les modules complémentaires pour l'installation collective avec l'Agent d'administration.

Tags

La section **Tags** affiche la liste des mots clés (tags) qui peuvent être ajoutés aux appareils clients après l'installation de l'Agent d'administration. Vous pouvez ajouter des tags à la liste, en supprimer ou les renommer.

Si la case en regard d'un tag est cochée, ce tag sera ajouté automatiquement aux appareils administrés lors de l'installation de l'Agent d'administration sur ces derniers.

Si la case en regard d'un tag est décochée, ce tag ne sera pas ajouté automatiquement aux appareils administrés lors de l'installation de l'Agent d'administration sur ces derniers. Ce tag peut être ajouté manuellement aux appareils.

Quand un tag est supprimé de la liste, il est retiré automatiquement de tous les appareils auxquels il avait été ajouté.

Historique des révisions

Cette section vous permet de consulter l'historique des révisions du paquet d'installation. Vous pouvez comparer les révisions, consulter les révisions, enregistrer les révisions au fichier, ajouter et modifier des descriptions de révision.

Les paramètres de paquet d'installation de l'Agent d'administration disponibles pour un système d'exploitation particulier sont repris dans le tableau ci-dessous.

Paramètres du paquet d'installation de l'Agent d'administration

Section Propriété	Windows	Mac	Linux
Général	✓	✓	✓
Paramètres	✓	—	—
Connexion	✓	✓ * sauf la case à cocher **&Ouvrir les ports de l'Agent d'administration dans le pare-feu Microsoft Windows**	✓ * sauf la case à cocher **&Ouvrir les ports de l'Agent d'administration dans le pare-feu Microsoft Windows**
Avancé	✓	✓	✓
Modules complémentaires	✓	✓	✓
Tags	✓	✓ * sauf les règles d'attribution des tags automatique	✓ * sauf les règles d'attribution des tags automatique
Historique des révisions	✓	✓	✓

Infrastructure virtuelle

Kaspersky Security Center Cloud Console prend en charge les machines virtuelles. Pour protéger votre infrastructure virtuelle, vous devez installer l'Agent d'administration sur chaque machine virtuelle.

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 Cloud Console qui ne sont pas très utiles aux machines virtuelles.

Lors de l'installation de l'Agent d'administration sur une machine virtuelle ou sur un modèle qui servira plus tard à créer des machines virtuelles, nous recommandons de réaliser les opérations suivantes :

- En cas d'installation à distance, sélectionnez l'option **Optimiser les paramètres pour VDI** dans la fenêtre des propriétés du paquet d'installation de l'Agent d'administration, dans la section **Avancé**.
- En cas d'installation interactive à l'aide de l'assistant, sélectionnez l'option **Optimiser les paramètres de l'Agent d'administration pour l'infrastructure virtuelle** dans la fenêtre de l'assistant.

En sélectionnant ces options, vous modifiez les paramètres de l'Agent d'administration afin que les fonctions suivantes soient désactivées par défaut (avant l'application d'une stratégie) :

- Réception d'informations sur les logiciels installés
- Réception d'informations sur la configuration matérielle
- Réception d'informations sur la présence de vulnérabilités
- Réception d'informations sur les mises à jour nécessaires

En général, les fonctions énumérées ne sont pas nécessaires sur les machines virtuelles dans la mesure où le logiciel et la configuration matérielle virtuelle sont homogènes.

Les fonctions peuvent être réactivées. Si n'importe laquelle des fonctions désactivées est malgré tout requise, elle peut être activée à l'aide d'une stratégie de l'Agent d'administration ou dans les paramètres locaux de l'Agent d'administration. Les paramètres locaux de l'Agent d'administration sont accessibles via le menu contextuel de l'appareil concerné dans la Console d'administration.

Prise en charge des machines virtuelles dynamiques

Kaspersky Security Center Cloud Console 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. La machine virtuelle sur laquelle l'Agent d'administration est installé est également ajoutée à la base de données du Serveur d'administration. Une fois que cette machine virtuelle a été désactivée, son enregistrement doit également être supprimé de la base de données du Serveur d'administration.

Pour garantir le fonctionnement de la suppression automatique des enregistrements relatifs aux machines virtuelles, sélectionnez l'option **Activer le mode dynamique pour VDI** lors de l'installation de l'Agent d'administration sur le modèle qui va servir à la création des machines virtuelles dynamiques :

- En cas d'installation à distance : dans la fenêtre des propriétés du paquet d'installation de l'Agent d'administration (section **Avancé**)
- En cas d'installation interactive – dans l'assistant d'installation de l'Agent d'administration

Évitez de sélectionner l'option **Activer le mode dynamique pour VDI** lors de l'installation de l'Agent d'administration sur des appareils physiques.

Si les événements sur les machines virtuelles dynamiques doivent être conservés un certain temps sur le Serveur d'administration après la suppression des machines virtuelles, vous devez sélectionner l'option **Conserver les événements après la suppression des appareils** dans la section **Stockage d'événements** de la fenêtre des propriétés du Serveur d'administration, puis indiquer la durée de conservation maximale des événements en jours.

Prise en charge de la copie des machines virtuelles

Kaspersky Security Center Cloud Console prend en charge la copie d'une machine virtuelle sur laquelle l'Agent d'administration est installé ou la création d'une machine virtuelle à partir d'un modèle avec l'Agent d'administration installé.

L'Agent d'administration peut détecter automatiquement la copie de machines virtuelles dans les cas suivants :

- 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.

Utilisation de l'Agent d'administration pour Windows, Linux et macOS : comparaison

L'Agent d'administration pour macOS et Linux présente plusieurs limitations fonctionnelles par rapport à l'Agent d'administration pour Windows. Les paramètres de la stratégie de l'Agent d'administration et du paquet d'installation varient également en fonction du système d'exploitation. Le tableau ci-dessous compare les fonctionnalités de l'Agent d'administration et les scénarios d'utilisation disponibles pour les systèmes d'exploitation Windows, macOS et Linux.

Comparaison entre fonctionnalités de l'Agent d'administration

Fonctionnalité de l'Agent d'administration	Windows	Linux	macOS
Installation			
Installation automatique des mises à jour et des correctifs pour l'Agent d'administration	✓	—	—
Diffusion automatique de la clé	✓	✓	✓
Programme d'installation Manuellement, en lançant les programmes d'installation sur les appareils	✓	✓	✓
Synchronisation forcée	✓	✓	✓
Point de distribution			
Sondage réseau	✓ • Sondage des plages IP • Sondage du réseau Windows • Sondage du contrôleur de domaine (Microsoft Active Directory)	✓ • Sondage des plages IP • Sondage du contrôleur de domaine (Microsoft Active Directory, Samba en tant qu'Active Directory)	—
Activer le service KSN proxy côté point de distribution	✓	✓	—
Téléchargement des mises à jour via les serveurs de mise à jour de Kaspersky dans les stockages des points de distribution qui diffusent les mises à jour sur les appareils administrés	✓	✓	— Les appareils de points de distribution exécutant macOS ne peuvent pas télécharger les mises à jour à partir des serveurs de mises à jour de Kaspersky.

			Si un ou plusieurs appareils exécutant macOS sont inclus dans la zone d'action de la tâche *Télécharger les mises à jour sur les stockages des points de distribution*, la tâche reçoit l'état *Échec*, même si elle s'est terminée avec succès sur tous les appareils Windows.
Installation push des applications	✓	Restreint : il n'est pas possible d'effectuer une installation push sur les appareils Windows à l'aide de points de distribution Linux.	Restreint : il n'est pas possible d'effectuer une installation push sur les appareils Windows à l'aide des points de distribution macOS.
Gestion des applications tierces			
Installation à distance des applications sur les appareils	✓	—	—
Mises à jour du logiciel	✓	—	—
Configuration des mises à jour du système d'exploitation dans une stratégie d'Agent d'administration	✓	—	—
Consultation des informations relatives aux vulnérabilités dans les applications	✓	—	—
Recherche de vulnérabilités dans les applications	✓	—	—
Inventaire du logiciel installé sur les appareils	✓	✓	—
Machines virtuelles			
Installation de l'Agent d'administration sur une machine virtuelle	✓	✓	✓
Optimiser les paramètres pour Virtual Desktop Infrastructure (VDI)	✓	✓	✓
Prise en charge des machines virtuelles dynamiques	✓	✓	✓
Autres			
Audit des opérations sur un appareil client distant à l'aide du Partage du bureau Windows	✓	—	—
Administration des redémarrages d'appareils	✓	—	—
Gestionnaire de connexion	✓	✓	✓
Connexion à distance au bureau de l'appareil client	✓	—	—

Les sections suivantes sont affichées dans les propriétés du point de distribution, mais les fonctionnalités correspondantes ne sont pas prises en charge par l'Agent d'administration pour macOS :

- Source des mises à jour
- Serveur proxy KSN
- Domaines Windows
- Active Directory

- Plages IP
- Avancé
- Statistiques

Spécification des paramètres pour l'installation à distance sur les appareils Unix

Lorsque vous installez une application sur un appareil Unix à l'aide d'une tâche d'installation à distance, vous pouvez spécifier les paramètres propres à Unix pour la tâche. Ces paramètres sont disponibles dans les propriétés de la tâche une fois la tâche créée.

Pour spécifier des paramètres propres à Unix pour une tâche d'installation à distance, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Tâches**.
2. Cliquez sur le nom de la tâche d'installation à distance pour laquelle vous souhaitez spécifier les paramètres propres à Unix.

   La fenêtre de propriétés de la tâche s'affiche.
3. Accédez à **Paramètres de l'application** → **Paramètres propres à Unix**.
4. Définissez les paramètres suivants :
   - **Définir un mot de passe pour le compte root (uniquement pour le déploiement via SSH)**

     Si la commande `sudo` ne peut pas être utilisée sur l'appareil cible sans indiquer le mot de passe, sélectionnez cette option, puis indiquez le mot de passe du compte root. Kaspersky Security Center Cloud Console 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 Cloud Console 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 Cloud Console 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.

Remplacement d'application de sécurité d'éditeurs tiers

L'installation des applications de sécurité de Kaspersky via Kaspersky Security Center Cloud Console peut nécessiter la suppression de logiciels tiers incompatibles avec l'application en cours d'installation.
Kaspersky Security Center Cloud Console propose plusieurs méthodes pour supprimer les applications tierces.

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. Vous pouvez trouver cette option dans l'assistant de déploiement de la protection. Si cette option est activée, Kaspersky Security Center Cloud Console 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 **Tâche de désinstallation à distance d'une application**. Il faut lancer la tâche sur les appareils avant la tâche d'installation de l'application de sécurité. Par exemple, vous pouvez choisir la programmation de type **A la fin d'une autre tâche** dans la tâche d'installation, où l'autre tâche est **Tâche de désinstallation à distance d'une application**.

Ce mode de suppression est recommandé si le programme d'installation de l'application de sécurité ne parvient pas à supprimer une des applications incompatibles.

Possibilités d'installation manuelle des applications

Vous pouvez installer l'Agent d'administration sur les appareils localement sans impliquer Kaspersky Security Center Cloud Console. Pour ce faire, créez un paquet d'installation autonome pour l'Agent d'administration comme décrit dans la section suivante : Création de paquets d'installation autonomes. Transférez le paquet sur votre appareil client et installez-le. Une fois l'installation de l'Agent d'administration terminée, vous pouvez utiliser l'appareil comme point de distribution.

Déploiement forcé à l'aide d'une tâche d'installation à distance des applications de Kaspersky Security Center Cloud Console

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 Cloud Console, à condition que chaque appareil dispose d'un ou plusieurs comptes utilisateurs avec des droits d'administrateur local.

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 des points de distribution.

Vous pouvez désigner un compte ayant accès au partage admin$ dans les paramètres de la tâche d'installation à distance.

Les appareils peuvent être désignés explicitement (via une liste) soit via la sélection du groupe d'administration de Kaspersky Security Center Cloud Console 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 Cloud Console chargée de l'interaction sur le réseau. Les conditions suivantes doivent être remplies :

- Les appareils cibles sont accessibles du côté 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 des points de distribution vers les appareils cibles.
- Les paramètres de sécurité de la stratégie de domaine Active Directory sont autorisés à assurer le fonctionnement du protocole NTLM lors du déploiement de l'Agent d'administration.
- Sur les appareils cibles exécutant Microsoft Windows XP, le mode Simple File Sharing est désactivé.
- Sur les appareils cibles, le modèle d'accès partagé et de sécurité est défini sur *Habituel – les utilisateurs locaux s'authentifient comme eux-mêmes*. Il ne peut en aucun cas être défini sur *Invité – les utilisateurs locaux s'authentifient en tant qu'invité*.
- Les appareils appartiennent au domaine ou des comptes utilisateurs unifiés avec privilèges d'administration sont créés au préalable sur les appareils.

Pour réussir le déploiement de l'Agent d'administration ou d'autres applications sur un appareil qui n'est pas joint à un domaine Active Directory Windows Server 2003 ou une version ultérieure, vous devez désactiver le contrôle de compte d'utilisateur à distance sur cet appareil. Le contrôle de compte d'utilisateur à distance est l'une des raisons qui empêche les comptes d'administration locaux d'accéder à admin$, ce qui est nécessaire pour le déploiement forcé de l'Agent d'administration ou d'autres applications. La désactivation du contrôle de compte d'utilisateur à distance n'affecte pas le contrôle de compte d'utilisateur local.

Lors de l'installation sur de nouveaux appareils qui ne figurent pas encore dans les groupe d'administration de Kaspersky Security Center Cloud Console, 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.

Les appareils jouant le rôle de points de distribution doivent répondre aux exigences applicables aux points de distribution. Vous devez garantir la présence de points de distribution dans chacun de ces réseaux isolés où se trouvent des appareils.

Il faut que l'espace disponible dans la section contenant le dossier %ALLUSERSPROFILE %\Application Data\KasperskyLab\adminkit soit plusieurs fois supérieur au volume total des paquets de distribution des applications à installer.

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**.

Étape 1. Démarrage de l'assistant de déploiement de la protection

Pour lancer manuellement l'assistant de déploiement de la protection, procédez comme suit

Dans le menu principal, accédez à **Découverte et déploiement → Déploiement et attribution → Assistant de déploiement de la protection**.

L'Assistant de déploiement de la protection démarre. Parcourez les étapes de l'assistant à l'aide du bouton **Suivant**.

Étape 1. Sélection du paquet d'installation

Sélectionnez la manière dont vous voulez installer le paquet d'installation sélectionné :

- **Installation à distance par Kaspersky Security Center**
- **Installation à distance par l'API Microsoft Azure**

Ensuite, sélectionnez le paquet d'installation de l'application que vous souhaitez installer.

Si le paquet d'installation de l'application en question ne figure pas dans la liste, cliquez sur le bouton **Ajouter**, puis sélectionnez l'application dans la liste.

Étape 2. Sélection de la version de l'Agent d'administration

Si vous avez sélectionné le paquet d'installation d'une application autre que l'agent d'administration, vous devez aussi installer l'agent d'administration qui connecte l'application au serveur d'administration de Kaspersky Security Center.

Sélectionnez la dernière version de l'agent d'administration.

Étape 3. 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.

Étape 4. Indiquez les paramètres de la tâche d'installation à distance

Dans la fenêtre **Paramètres de la tâche 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 l'option est activée, les paquets d'installation sont transmis sur les appareils clients via les outils du système d'exploitation par les points de distribution. Cette option peut être sélectionnée si au moins un point de distribution se trouve sur le réseau.

  Si l'option **À l'aide de l'Agent d'administration** est activée, les fichiers seront livrés via les outils du système d'exploitation uniquement dans le cas où il n'est pas possible d'utiliser les moyens de l'Agent d'administration.

  Par défaut, l'option est activée pour les tâches d'installation à distance créées sur le Serveur d'administration virtuel.

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.

Mot de passe pour désinstaller l'application Kaspersky actuelle

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**.

Saisissez le mot de passe dans le champ **Mot de passe pour désinstaller l'application Kaspersky actuelle** si vous migrez d'une application Kaspersky vers une autre et que votre application actuelle est protégée par un mot de passe. Notez que lors de la migration, votre application Kaspersky actuelle sera désinstallée.

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.

Étape 5. 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.

Étape 6. 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 Cloud Console 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 7. Déplacement des appareils vers Appareils administrés

Indiquez si les appareils doivent être déplacés vers un groupe d'administration après l'installation de l'agent d'administration.

- Ne pas déplacer les appareils

Les appareils demeurent dans les groupes où ils se trouvent. Les appareils qui n'ont été placés dans aucun groupe restent non définis.

- Déplacer les appareils non définis dans un groupe

  Les appareils sont déplacés vers le groupe d'administration que vous avez sélectionné.

L'option **Ne pas déplacer les appareils** est sélectionnée par défaut. Pour des raisons de sécurité, envisagez de déplacer les appareils manuellement.

Étape 8. 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 Cloud Console 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 Cloud Console. Pour créer une clé privée au format PEM pris en charge, ajoutez l'option -m PEM dans la commande ssh-keygen. Par exemple :

    ```
    ssh-keygen -m PEM -t rsa -b 4096 -C "<user email>"
    ```

Étape 9. 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.

Paramètres réseau pour l'interaction avec des services externes

Kaspersky Security Center Cloud Console utilise les paramètres réseau suivants pour interagir avec les services externes.

Paramètres réseau

Paramètres réseau	Adresse	Description
Port : 443 Protocole : HTTPS	activation-v2.kaspersky.com/activationservice/activationservice.svc	Activation des applications.
Port : 443 Protocole : HTTPS	https://s00.upd.kaspersky.com https://s01.upd.kaspersky.com https://s02.upd.kaspersky.com https://s03.upd.kaspersky.com https://s04.upd.kaspersky.com https://s05.upd.kaspersky.com https://s06.upd.kaspersky.com https://s07.upd.kaspersky.com https://s08.upd.kaspersky.com https://s09.upd.kaspersky.com https://s10.upd.kaspersky.com https://s11.upd.kaspersky.com https://s12.upd.kaspersky.com https://s13.upd.kaspersky.com https://s14.upd.kaspersky.com https://s15.upd.kaspersky.com https://s16.upd.kaspersky.com https://s17.upd.kaspersky.com https://s18.upd.kaspersky.com https://s19.upd.kaspersky.com https://cm.k.kaspersky-labs.com	Mise à jour des bases de données, des modules logiciels et des applications de Kaspersky.
Port : 443 Protocole : HTTPS	https://downloads.upd.kaspersky.com	• Mise à jour des bases de données, des modules logiciels et des applications de Kaspersky. • Vérification de l'accessibilité des serveurs de Kaspersky. Avant de télécharger les bases de données et les modules logiciels de Kaspersky, Kaspersky Security Center Cloud Console vérifie si les serveurs de Kaspersky sont accessibles. Si l'accès aux serveurs via le DNS système n'est pas possible, l'application utilise les serveurs DNS publics.
Port : 80 Protocole : HTTP	http://p00.upd.kaspersky.com http://p01.upd.kaspersky.com http://p02.upd.kaspersky.com	Mise à jour des bases de données, des modules logiciels et des applications de Kaspersky.

	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	
Port : 443 Protocole : HTTPS	ds.kaspersky.com	Utilisation de Kaspersky Security Network.
Port : 443, 1443 Protocole : HTTPS	ksn-a-stat-geo.kaspersky-labs.com ksn-file-geo.kaspersky-labs.com ksn-verdict-geo.kaspersky-labs.com ksn-url-geo.kaspersky-labs.com ksn-a-p2p-geo.kaspersky-labs.com ksn-info-geo.kaspersky-labs.com ksn-cinfo-geo.kaspersky-labs.com	Utilisation de Kaspersky Security Network.
Protocole : HTTPS	click.kaspersky.com redirect.kaspersky.com	En suivant les liens depuis l'interface.
Port : 80 Protocole : HTTP	http://crl.kaspersky.com http://ocsp.kaspersky.com	Infrastructure à clé publique (ICP).
Port : 443 Protocole : HTTPS	https://ipm-klca.kaspersky.com	Annonces marketing.

Préparation d'un appareil exécutant Astra Linux dans l'environnement logiciel fermé mode pour l'installation de l'Agent d'administration

Avant l'installation de l'Agent d'administration sur un appareil exécutant Astra Linux en mode environnement logiciel fermé, vous devez effectuer deux procédures de préparation : celle des instructions ci-dessous et les étapes générales de préparation pour tout appareil Linux.

Conditions préalables :

- Assurez-vous que l'appareil sur lequel vous voulez installer l'Agent d'administration pour Linux fonctionne sur une des distributions Linux supportées.
- Téléchargez le fichier d'installation nécessaire de l'Agent d'administration sur le site Internet de Kaspersky.

Exécutez les commandes fournies dans cette instruction sous un compte avec des privilèges root.

Pour préparer un appareil exécutant Astra Linux dans l'environnement logiciel fermé mode en vue de l'installation de l'Agent d'administration, procédez comme suit :

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

   ```
   DIGSIG_ELF_MODE=1
   ```

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

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

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

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

4. Placez la clé de l'application /opt/kaspersky/ksc64/share/kaspersky_astra_pub_key.gpg dans le répertoire créé à l'étape précédente :

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

   Si le kit de distribution Kaspersky Security Center Cloud Console n'inclut pas la clé de l'application kaspersky_astra_pub_key.gpg, vous pouvez la télécharger en cliquant sur le lien : https://media.kaspersky.com/utilities/CorporateUtilities/kaspersky_astra_pub_key.gpg.

5. Mettez à jour les disques RAM :

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

   Redémarrez le système.

6. Effectuez les étapes de préparation communes à tout appareil Linux.

L'appareil est préparé. Vous pouvez maintenant procéder à l'installation de l'Agent d'administration.

Préparation d'un appareil Linux et installation de l'Agent d'administration sur un appareil Linux à distance

L'installation de l'Agent d'administration comprend deux étapes :

- Préparation de l'appareil Linux
- Installation à distance de l'Agent d'administration

Préparation de l'appareil Linux

Pour préparer l'appareil fonctionnant sous le système d'exploitation Linux à l'installation à distance de l'Agent d'administration, procédez comme suit :

1. Assurez-vous que le logiciel suivant est installé sur l'appareil Linux cible :
   - Sudo (pour Ubuntu 10.04, version de Sudo 1.7.2p1 ou version ultérieure)
   - Interpréteur Perl version 5.10 ou ultérieure
2. Lancez l'analyse de la configuration de l'appareil :
   a. Vérifiez que la connexion à l'appareil à l'aide de l'application client SSH (par exemple, l'application PuTTY) est possible.

      Si vous ne pouvez pas vous connecter à l'appareil, ouvrez le fichier `/etc/ssh/sshd_config` et veillez à ce que les paramètres suivants aient les valeurs :

      ```
      PasswordAuthentication no
      ChallengeResponseAuthentication yes
      ```

      > Ne modifiez pas le fichier /etc/ssh/sshd_config si vous pouvez vous connecter à l'appareil sans problèmes ; dans le cas contraire, vous pouvez rencontrer un échec de l'authentification SSH lors de l'exécution d'une tâche d'installation à distance.

      Enregistrez le fichier (si besoin) et relancez le service SSH à l'aide de la commande `sudo service ssh restart`.

   b. Désactivez le mot de passe de la demande sudo pour le compte utilisateur utilisé pour la connexion à l'appareil.

   c. Utilisez la commande sudo `visudo` pour ouvrir le fichier de configuration sudoers.

      Dans le fichier que vous avez ouvert, ajoutez la ligne suivante à la fin du fichier : `<username> ALL = (ALL) NOPASSWD: ALL`. Dans ce cas, `< username >` est le compte utilisateur qui sera utilisé pour la connexion à l'appareil via le protocole SSH. Si vous utilisez le système d'exploitation Astra Linux, ajoutez dans le fichier /etc/sudoers la dernière ligne avec le texte suivant : `%astra-admin ALL=(ALL:ALL) NOPASSWD: ALL`

   d. Enregistrez le fichier sudoers et fermez-le.

   e. Connectez-vous à nouveau à l'appareil via SSH et vérifiez que le service Sudo ne requiert pas de mot de passe à l'aide de la commande `sudo whoami`.
3. Ouvrez le fichier `/etc/systemd/logind.conf`, puis effectuez l'une des opérations suivantes :
   - Spécifiez " non " comme valeur pour le paramètre KillUserProcesses : `KillUserProcesses=no`.
   - Pour le paramètre KillExcludeUsers, saisissez le nom d'utilisateur du compte sous lequel l'installation à distance doit être effectuée, par exemple, `KillExcludeUsers=root`.

Si la machine cible exécute Astra Linux, ajoutez la chaîne `export PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin` dans le fichier `/home/< username >/.bashrc`, où `< username >` est le compte à utiliser pour la connexion de l'appareil via SSH.

Si vous souhaitez installer l'Agent d'administration sur des appareils qui utilisent le système d'exploitation RED OS 7.3.4 ou une version ultérieure ou MSVSPHERE 9.2 ou une version ultérieure, installez le paquet libxcrypt-compat pour assurer le bon fonctionnement de l'Agent d'administration.

Pour appliquer le paramètre modifié, redémarrez l'appareil Linux ou exécutez la commande suivante :

```
$ sudo systemctl restart systemd-logind.service
```

4. Si vous souhaitez installer l'Agent d'administration sur des appareils dotés du système d'exploitation SUSE Linux Enterprise Server 15, installez le paquet insserv-compat en premier pour configurer l'Agent d'administration.

5. Si vous souhaitez installer l'Agent d'administration sur des appareils dotés du système d'exploitation Astra Linux à l'aide de l'environnement logiciel fermé, exécutez les étapes complémentaires de préparation des appareils Astra Linux.

Installation à distance de l'Agent d'administration

Pour installer l'Agent d'administration sur l'appareil localement, procédez comme suit :

1. Téléchargez et créez le paquet d'installation :

   a. Avant l'installation du paquet sur l'appareil, assurez-vous que les dépendances (les applications, les bibliothèques) liées au paquet en question sont installées.

   Vous pouvez indépendamment consulter les dépendances liées à chaque paquet en utilisant les utilitaires spécifiques à ce distributif Linux sur lequel le paquet sera installé. Vous pouvez consulter les informations relatives aux utilitaires dans la documentation de votre système d'exploitation.

   b. Téléchargez le paquet d'installation de l'Agent d'administration via l'interface de l'application ou depuis le site Internet de Kaspersky.

   c. Pour la création du paquet d'installation à distance, utilisez les fichiers :

   - klnagent.kpd
   - akinstall.sh
   - Paquet .deb ou .rpm de l'Agent d'administration

2. Créez la tâche d'installation à distance de l'application avec les paramètres :

   - Dans la page **Paramètres** de l'assistant de création d'une tâche, cochez la case **En utilisant les ressources du système d'exploitation via le Serveur d'administration**. Décochez toutes les autres cases.
   - Dans la page **Sélection du compte utilisateur pour exécuter la tâche**, définissez les paramètres du compte utilisateur servant à connecter l'appareil via SSH.

3. Lancez la tâche d'installation à distance de l'application. Utilisez l'option de la commande `su` pour préserver l'environnement : `-m, -p, --preserve-environment`.

Installation des applications à l'aide de la tâche d'installation à distance

Kaspersky Security Center Cloud Console permet d'installer à distance des applications sur les appareils à l'aide des tâches d'installation à distance. Ces tâches sont créées et attribuées à des appareils à l'aide d'un Assistant. Pour pouvoir attribuer une tâche plus vite et plus facilement, vous pouvez désigner les appareils (jusqu'à 1 000 appareils) dans la fenêtre de l'Assistant de la manière qui vous convient le plus :

- **Sélectionner les appareils détectés sur le réseau par le Serveur d'administration**. Dans ce cas la tâche est affectée à un ensemble d'appareils. L'ensemble d'appareils peut reprendre aussi bien des appareils de groupes d'administration que des appareils non définis.
- **Définir les adresses des appareils manuellement ou les importer à partir d'une liste**. Dans ce cas, 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.
- **Attribuer la tâche à un groupe d'administration**. Dans ce cas, la tâche est affectée aux appareils qui appartiennent à un groupe d'administration déjà créé.

Pour éviter les problèmes pouvant survenir lors de l'installation de l'application sur un appareil client sans Agent d'administration installé, il faut procéder comme décrit dans le déploiement forcé via la tâche d'installation à distance de Kaspersky Security Center Cloud Console.

Installation d'une application à distance

Cet article contient des informations sur l'installation à distance d'une application sur les appareils d'un groupe d'administration, les appareils avec des adresses spécifiques ou une sélection d'appareils.

Pour installer l'application sur les appareils spécifiques, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Tâches**.
2. Cliquez sur **Ajouter**.

   Ceci permet de lancer l'Assistant de création d'une tâche.
3. Dans le champ **Type de tâche**, sélectionnez **Installation à distance d'une application**.
4. Sélectionnez l'une des options ci-dessous :

   - Attribuer la tâche à un groupe d'administration

     La tâche est affectée aux appareils qui appartiennent à un groupe d'administration. Vous pouvez renseigner un des groupes existants ou en créer un.

     Par exemple, vous pourriez souhaiter utiliser cette option pour exécuter une tâche d'envoi de messages pour les utilisateurs si le message est particulier pour les appareils repris dans un groupe d'administration spécifique.

     Si une tâche est attribuée à un groupe d'administration, l'onglet **Sécurité** ne s'affiche pas dans la fenêtre des propriétés de la tâche, car les tâches de groupe sont soumises aux paramètres de sécurité des groupes auxquels elles s'appliquent.

   - Définir les adresses des appareils manuellement ou les importer à partir de la liste

Vous pouvez définir les noms NetBIOS, les noms DNS, les adresses IP, ainsi que les plages d'adresses IP auxquels il convient d'affecter la tâche.

Vous pourriez utiliser cette option pour exécuter une tâche pour un sous-réseau défini. Par exemple, vous pourriez souhaiter installer une certaine application sur les appareils des comptables ou analyser des appareils dans un sous-réseau qui est probablement infecté.

- **Attribuer la tâche à une sélection d'appareils**

  La tâche est affectée aux appareils qui appartiennent à une sélection d'appareils. Vous pouvez définir une des sélections existantes.

  Par exemple, vous pourriez souhaiter utiliser cette option pour exécuter une tâche sur des appareils dotés d'une version du système d'exploitation spécifique.

La tâche *Installer l'application à distance* est créée pour les appareils indiqués. Si vous avez sélectionné l'option **Attribuer la tâche à un groupe d'administration**, la tâche est de groupe.

5. À l'étape Zone d' **Zone 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 :

   - Sélectionnez la manière dont vous souhaitez installer l'application sélectionnée :

     - **Installation à distance par Kaspersky Security Center**

     - **Installation à distance par l'API Microsoft Azure**

       Pour en savoir plus sur l'installation d'applications sur les machines virtuelles Microsoft Azure, consultez la section Installation à distance d'applications sur les machines virtuelles Azure.

   - Dans le champ **Sélection du paquet d'installation**, sélectionnez le paquet d'installation d'une application que vous souhaitez installer.

   - Le groupe de paramètres **Forcer le téléchargement du paquet d'installation** permet de sélectionner le mode d'envoi des fichiers nécessaires pour l'installation de l'application sur les appareils clients :

     - **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 l'option est activée, les paquets d'installation sont transmis sur les appareils clients via les outils du système d'exploitation par les points de distribution. Cette option peut être sélectionnée si au moins un point de distribution se trouve sur le réseau.

Si l'option **À l'aide de l'Agent d'administration** est activée, les fichiers seront livrés via les outils du système d'exploitation uniquement dans le cas où il n'est pas possible d'utiliser les moyens de l'Agent d'administration.

Par défaut, l'option est activée pour les tâches d'installation à distance créées sur le Serveur d'administration virtuel.

- 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 Cloud Console 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**, puis relancez 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 applications 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 options 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 Cloud Console 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 Cloud Console ne transmet pas les fichiers et n'essaie pas d'installer l'application. Par exemple, pour installer une application quelconque sur les appareils d'un groupe d'administration qui comprend des appareils fonctionnant sous divers systèmes d'exploitation, vous pouvez attribuer la tâche d'installation au groupe d'administration, puis activer cette option pour ignorer les appareils qui fonctionnent sous un système d'exploitation autre que celui requis.

- **Demander aux utilisateurs de fermer les applications en cours d'exécution**

  Les applications en cours d'exécution peuvent empêcher le redémarrage de l'appareil client. Par exemple, si un document est en train d'être modifié dans un logiciel de traitement de texte et qu'il n'est pas enregistré, l'application n'autorise pas le redémarrage de l'appareil.

  Quand cette option est activée, l'arrêt forcé de ces applications sur un appareil verrouillé doit avoir lieu avant de pouvoir redémarrer l'appareil. Les utilisateurs pourraient perdre toute modification qui n'a pas été enregistrée à ce moment.

  Si cette option est désactivée, un appareil verrouillé n'est pas redémarré. L'état de la tâche sur cet appareil indique qu'il faut redémarrer l'appareil. Les utilisateurs doivent quitter manuellement toutes les applications en cours d'exécution sur les appareils verrouillés, puis redémarrer ces appareils.

  Cette option est Inactif par défaut.

- Sélectionnez les appareils sur lesquels vous souhaitez installer l'application :

  - **Installer sur tous les appareils**

    L'application est installée même sur les appareils administrés par d'autres Serveurs d'administration.

    Par défaut, cette option est sélectionnée. Vous n'avez pas à modifier ce paramètre si vous n'avez qu'un seul Serveur d'administration sur votre réseau.

  - **Installer uniquement sur les appareils administrés via &ce Serveur d'administration**

    L'application est installée uniquement sur les appareils administrés par ce Serveur d'administration. Sélectionnez cette option si vous avez plus d'un Serveur d'administration dans votre réseau et que vous souhaitez évitez les conflits entre eux.

- Spécifiez si les appareils doivent être déplacés vers un groupe d'administration après l'installation :

  - **Ne pas déplacer les appareils**

    Les appareils demeurent dans les groupes où ils se trouvent. Les appareils qui n'ont été placés dans aucun groupe restent non définis.

  - **Déplacer les appareils non définis vers le groupe sélectionné (seul un groupe unique peut être sélectionné)**

    Les appareils sont déplacés vers le groupe d'administration que vous avez sélectionné.

L'option **Ne pas déplacer les appareils** est sélectionnée par défaut. Pour des raisons de sécurité, envisagez de déplacer les appareils manuellement.

7. À cette étape de l'assistant, indiquez si les appareils doivent être redémarrés lors de l'installation des applications :

- **Ne pas redémarrer l'appareil**

  Si cette option a été sélectionnée, l'appareil ne sera pas redémarré après l'installation de l'application de sécurité.

- **Redémarrer l'appareil**

  Si cette option a été sélectionnée, l'appareil sera redémarré après l'installation de l'application de sécurité.

- **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.

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 Cloud Console 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 Cloud Console. Pour créer une clé privée au format PEM pris en charge, ajoutez l'option -m PEM dans la commande ssh-keygen. Par exemple :

    ```
    ssh-keygen -m PEM -t rsa -b 4096 -C "<user email>"
    ```

9. À l'étape **Fin de la création de la tâche**, cliquez sur le bouton **Terminer** pour créer la tâche et fermer l'Assistant.

   Si vous avez activé l'option **Ouvrir les détails de la tâche à la fin de la création**, la fenêtre des paramètres de la tâche s'ouvre. Dans cette fenêtre, vous pouvez vérifier les paramètres de la tâche, les modifier ou configurer une planification de lancement de la tâche, si nécessaire.

10. Dans la liste des tâches, sélectionnez la tâche que vous avez créée, puis cliquez sur **Démarrer**.

Vous pouvez également attendre que la tâche se lance conformément à la planification que vous avez spécifiée dans les paramètres de la tâche.

Une fois la tâche d'installation à distance terminée, l'application sélectionnée est installée sur les appareils indiqués.

Installation des applications sur les Serveurs d'administration secondaires

Pour installer l'application sur les Serveurs d'administration secondaires, procédez comme suit :

1. Connectez-vous au Serveur d'administration qui gère les Serveurs d'administration secondaires nécessaires.
2. Assurez-vous que le paquet d'installation correspondant à l'application à installer se trouve sur chaque Serveur d'administration secondaire sélectionné. Si vous ne trouvez pas le paquet d'installation sur l'un des Serveurs secondaires, distribuez-le. Pour ce faire, créez une tâche avec le type de tâche **Diffusion du paquet d'installation**
3. Créez une tâche pour l'installation à distance de l'application sur les Serveurs d'administration secondaires. Sélectionnez le type de tâche **Installer à distance l'application sur le Serveur d'administration secondaire**.

   L'Assistant de création d'une tâche crée une tâche d'installation à distance de l'application sélectionnée dans l'Assistant sur certains Serveurs d'administration secondaires.
4. Lancez la tâche manuellement ou attendez son lancement conformément à la planification que vous avez indiquée dans les paramètres de la tâche.

Une fois la tâche d'installation à distance terminée, l'application sélectionnée est installée sur les Serveurs d'administration secondaires.

Lancement et arrêt des applications Kaspersky.

Vous pouvez utiliser la tâche *Lancer ou arrêter une application* pour lancer et arrêter des applications de Kaspersky sur les appareils administrés.

Pour créer la tâche Lancer ou arrêter une application, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Tâches**.
2. Cliquez sur **Ajouter**.

   Ceci permet de lancer l'assistant de création d'une tâche. Parcourez les étapes de l'assistant à l'aide du bouton **Suivant**.
3. Dans la liste déroulante **Application**, sélectionnez l'application pour laquelle vous voulez créer une tâche.
4. À partir de la liste **Type de tâche**, sélectionnez la tâche **Activation de l'application**.
5. Dans le champ **Nom de la tâche**, indiquez le nom de la nouvelle tâche.

   Le nom de la tâche ne peut pas contenir plus de 100 symboles et contenir de symboles spéciaux ("*<>?\:|).
6. Sélectionnez les appareils auxquels les tâches seront affectées.
7. Dans la fenêtre **Applications**, réalisez les opérations suivantes :

- Cochez les cases en regard du nom des applications pour lesquelles vous souhaitez créer une tâche.
- Sélectionnez l'option **Lancer l'application** ou **Arrêter l'application**.

8. Si vous souhaitez modifier les paramètres de la tâche par défaut, activez l'option **Ouvrir les détails de la tâche à la fin de la création** à l'étape **Fin de la création de la tâche**. Si vous n'activez pas cette tâche, la tâche est créée selon les paramètres par défaut. Vous pourrez modifier ces paramètres par défaut plus tard, à tout moment.

9. Cliquez sur le bouton **Terminer**.

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

10. Cliquez sur le nom de la tâche créée pour ouvrir la fenêtre de propriétés de la tâche.

11. Dans la fenêtre des propriétés de la tâche, indiquez les paramètres généraux de la tâche en fonction de vos besoins, puis enregistrez les paramètres.

La tâche est créée et configurée.

Si vous souhaitez exécuter la tâche, sélectionnez-la dans la liste des tâches, puis cliquez sur le bouton **Démarrer**.

Administration des appareils mobiles

L'administration de la protection des appareils mobiles via la Kaspersky Security Center Cloud Console est confiée à la Fonction Administration des appareils mobiles. Si vous avez l'intention d'administrer les appareils mobiles qui appartiennent aux employés de votre organisation, activez et configurez l'Administration des appareils mobiles.

L'administration des appareils mobiles vous permet d'administrer les appareils Android des employés. La protection est assurée par l'application mobile Kaspersky Security for Mobile app installée sur les appareils. Cette application mobile assure la protection des appareils mobiles contre les menaces Web, les virus et les autres programmes qui présentent des menaces.

Appareils iOS

Kaspersky Device Management for iOS assure la protection et le contrôle des appareils mobiles connectés à Kaspersky Security Center Cloud Console.

L'application Kaspersky Security for iOS offre les fonctionnalités suivantes :

- **Protection Internet**. Ce module bloque les sites malveillants conçus pour diffuser du code malveillant. La Protection Internet bloque également les sites Internet de phishing qui servent à voler des données confidentielles des utilisateurs (mots de passe des banques en lignes ou des systèmes de paiement, par exemple) pour obtenir un accès à leurs comptes bancaires.

- **Détection de jailbreak**. Lorsque Kaspersky Security for iOS détecte un jailbreak, il affiche un message critique et vous informe du problème.

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.

Capacités de Detection and Response

Cette section contient des informations sur les solutions Kaspersky qui peuvent être intégrées à Kaspersky Security Center Cloud Console pour ajouter les capacités de Detection and Response à la console.

À propos des capacités de Detection and Response

Kaspersky Security Center Cloud Console peut intégrer des fonctionnalités d'autres solutions Kaspersky à l'interface de la console. Par exemple, vous pouvez ajouter les fonctionnalités de Detection and Response aux fonctionnalités de Kaspersky Security Center Cloud Console.

Les solutions de détection et de réponse sont conçues pour protéger l'infrastructure informatique d'une entreprise contre les cybermenaces complexes. La fonctionnalité de la solution combine la détection automatique des menaces avec la capacité de répondre à ces menaces pour résister aux attaques complexes, y compris les nouveaux exploits, les ransomwares, les attaques sans fichier et les méthodes qui utilisent des outils système légitimes.

Vous pouvez intégrer les solutions suivantes :

- Kaspersky Endpoint Detection and Response Optimum

  Lorsqu'une application Kaspersky Endpoint Protection Platform (également appelée EPP) détecte une menace, Kaspersky Security Center Cloud Console ajoute une nouvelle alerte à la liste d'alertes. Une alerte contient des informations détaillées sur la menace détectée et vous permet d'analyser et d'enquêter sur la menace. Vous pouvez également visualiser la menace en créant un graphique de la chaîne de développement des menaces. Le graphique décrit les étapes de déploiement de l'attaque détectée dans la durée.

  En tant qu'une réponse, vous pouvez sélectionner une des actions de réponse prédéfinies, par exemple, isoler un objet non approuvé, isoler un appareil compromis du réseau ou créer une règle de prévention d'exécution pour un objet non approuvé.

  Pour plus d'informations sur l'activation de la solution, consultez la documentation de Kaspersky Endpoint Detection and Response Optimum.

- Kaspersky Managed Detection and Response

  Lorsqu'une application Kaspersky EPP détecte une menace, Kaspersky Security Center Cloud Console ajoute un nouvel incident à la liste des incidents. Un incident contient des informations détaillées sur la menace détectée. Les analystes MDR Security Operation Center (SOC) de Kaspersky ou d'une entreprise tierce enquêtent sur les incidents et proposent des réponses pour résoudre les incidents. Vous pouvez accepter ou rejeter les mesures proposées manuellement, ou activer l'option d'acceptation automatique de toutes les réponses.

  Pour plus d'informations sur l'activation de la solution, consultez la documentation de Kaspersky Managed Detection and Response.

- Kaspersky Endpoint Detection and Response Expert

  Il s'agit d'une solution pour les organisations qui disposent d'une équipe d'analystes SOC. Les menaces détectées sont enregistrées sous forme d'alertes ou d'incidents qui peuvent être attribués aux analystes du SOC pour enquête. Kaspersky Endpoint Detection and Response Expert vous fournit des informations détaillées sur chaque alerte ou incident, ainsi que les outils d'administration des alertes et des incidents, la recherche des menaces et le développement de règles personnalisées. Les analystes SOC ou les responsables de la sécurité peuvent sélectionner manuellement les actions de réponse, ou les mesures de réponse automatisées prédéfinies peuvent être prises.

  Pour plus d'informations sur l'activation de la solution, consultez la documentation de Kaspersky Endpoint Detection and Response Expert.

Modifications d'interface après intégration des fonctionnalités de Detection and Response

Les solutions Kaspersky suivantes offrent des fonctionnalités de détection et de réponse qui peuvent être intégrées à l'interface de Kaspersky Security Center Cloud Console :

- Kaspersky Endpoint Detection and Response (EDR) Optimum
- Kaspersky Managed Detection and Response (MDR)
- Kaspersky Endpoint Detection and Response (EDR) Expert

Le tableau ci-dessous liste les modifications apportées par les solutions à l'interface de Kaspersky Security Center Cloud Console après l'intégration.

Modifications de l'interface apportées par les solutions Kaspersky intégrées

Solution	Modifications dans Kaspersky Security Center Cloud Console
Kaspersky EDR Optimum	Ajoute les éléments suivants : • Section **Alertes** (**Surveillance et rapports** → **Alertes**). Les alertes détectées par cette solution sont listées sous l'onglet **Optimum**. • Un widget sur le **Tableau de bord** (**Surveillance et rapports** → **Tableau de bord**).
Kaspersky MDR	Ajoute les éléments suivants : • Section **MDR** (**Surveillance et rapports** → **MDR**). • Option **Afficher les fonctionnalités MDR** (**Paramètres** → **Options d'interface** → **Afficher les fonctionnalités MDR**). • Un widget sur le **Tableau de bord** (**Surveillance et rapports** → **Tableau de bord**).
Kaspersky EDR Expert	Ajoute les éléments suivants : • Section **Alertes** (**Surveillance et rapports** → **Alertes**). Les alertes détectées par cette solution sont listées sous l'onglet **Expert**. • Section **Incidents** (**Surveillance et rapports** → **Incidents**). • Section **Recherche des menaces** (**Surveillance et rapports** → **Recherche des menaces**). • Section **Règles personnalisées** (**Surveillance et rapports** → **Règles personnalisées**). • Paramètres généraux de Kaspersky EDR Expert (**Paramètres** → **Intégration** → **Kaspersky EDR Expert**). • Un widget sur **Tableau de bord** (**Surveillance et rapports** → **Tableau de bord**).

Découverte des appareils en réseau et création de groupes d'administration

Cette section décrit la recherche et la découverte d'appareils en réseau, ainsi que la création groupes d'administration pour ces appareils.

Kaspersky Security Center Cloud Console permet de rechercher les appareils sur la base des critères définis. Vous pouvez enregistrer les résultats de la recherche dans un fichier texte.

La fonction de recherche permet de trouver les appareils suivants :

- les appareils administrés dans les groupes d'administration du Serveur d'administration de Kaspersky Security Center Cloud Console et ses Serveurs d'administration secondaires ;
- Les appareils non définis administrés par le Serveur d'administration de Kaspersky Security Center Cloud Console et ses Serveurs secondaires.

Scénario de recherche d'appareils en réseau

Vous devez effectuer une recherche d'appareils avant le déploiement initial 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.

Une fois que vous avez terminé le scénario, la recherche d'appareils est configurée et est exécutée conformément au calendrier spécifié.

Prérequis

Dans Kaspersky Security Center Cloud Console, la recherche d'appareils est effectuée par des points de distribution. Avant de commencer, procédez comme suit :

- Décidez quels appareils serviront de points de distribution.
- Installez les Agents d'administration sur les appareils que vous avez choisis.
- Désignez manuellement les appareils comme points de distribution.

Étapes

Le scénario se déroule par étapes :

1. **Choisir les types de recherche**

   Décidez quel(s) type(s) de découverte vous voulez utiliser régulièrement.

2. **Configuration des sondages**

   Dans les propriétés de chaque point de distribution, activez et configurez les types de sondages du réseau que vous avez choisis : sondage du réseau Windows, sondage du contrôleur de domaine ou sondage des plages IP. Assurez-vous que la programmation des sondages répond aux besoins de votre organisation.

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

3. **Configuration de règles pour l'ajout d'appareils découverts aux groupes d'administration (facultatif)**

   Si de nouveaux appareils apparaissent sur votre réseau, ils sont trouvés lors de sondages réguliers et sont automatiquement inclus dans le groupe **Appareils non définis**. Vous pouvez configurer des règles de déplacement automatique pour déplacer ces appareils vers le groupe **Appareils administrés**. Vous pouvez aussi définir des règles de conservation.

   Si vous ignorez cette étape de définition des règles, tous les appareils découverts sont placés dans le groupe **Appareils non définis** et y restent. Vous pouvez déplacer ces appareils vers le groupe des **Appareils administrés**. Si vous déplacez les appareils vers le groupe **Appareils administrés** manuellement, vous pouvez analyser les informations sur chaque appareil et décider si vous voulez le déplacer vers un groupe d'administration, et si oui, quel groupe.

Une fois l'opération de sondage réseau terminée, vérifiez que les appareils récemment détectés sont organisés en fonction des règles configurées. En l'absence de règles, ils restent dans le groupe **Appareils non définis**.

Sondage réseau

Les informations sur la structure du réseau et les appareils de ce réseau sont reçues par Kaspersky Security Center Cloud Console par le biais d'un sondage régulier du réseau Windows, des plages IP, du contrôleur de domaine Microsoft Active Directory et d'un contrôleur de domaine Samba. Pour un contrôleur de domaine Samba, Samba 4 est utilisé comme contrôleur de domaine Active Directory. Le sondage du réseau peut être lancé manuellement ou automatiquement selon une programmation.

En fonction des résultats de ce sondage, Kaspersky Security Center Cloud Console met à jour la liste des appareils non définis. Vous pouvez également configurer des règles pour que les derniers appareils découverts soient automatiquement déplacés vers des groupes d'administration.

Kaspersky Security Center Cloud Console utilise les méthodes suivantes pour le sondage du réseau :

- *Sondage des plages IP*. Kaspersky Security Center Cloud Console sonde les intervalles IP spécifiés à l'aide de paquets ICMP (Internet Control Message Protocol) et reçoit toutes les informations sur les appareils appartenant aux plages IP.

- *Sondage du réseau Windows*. Deux sondages différents sont disponibles : le sondage rapide et le sondage complet. Lors du sondage rapide, Kaspersky Security Center Cloud Console ne reçoit que les informations relatives à la liste des noms NetBIOS des appareils de tous les domaines et des groupes de travail du réseau. Pendant le sondage complet, les informations suivantes sont demandées pour chaque appareil : nom du système d'exploitation (SE), adresse IP, nom DNS et nom NetBIOS.

- *Sondage des contrôleurs de domaine*. Les informations sur la structure de l'unité Active Directory et sur les noms DNS des appareils des groupes Active Directory sont enregistrées dans la base de données de Kaspersky Security Center Cloud Console.

Les résultats du sondage sont affichés dans la section **Découverte et déploiement → Découverte** séparément pour les méthodes de sondage du *réseau Windows* et des *contrôleurs de domaine*.

Les résultats du sondage pour la méthode *de sondage de plage IP* sont affichés dans la section **Découverte et déploiement → Appareils non définis**.

Un appareil peut être affiché dans plusieurs zones de détection. Si un appareil est détecté dans le domaine HQ et que son adresse est 192.168.0.1, il s'affiche à la fois dans la section **Domaines Windows** et dans la section **Appareils non définis**. Vous pouvez modifier les paramètres de sondage réseau pour chaque méthode de sondage. Par exemple, il se peut que vous souhaitiez modifier la programmation du sondage ou décider de sonder l'ensemble de la forêt Active Directory ou uniquement un domaine en particulier.

Sondage du réseau Windows

À propos du sondage du réseau Windows

Lors du sondage rapide, le Serveur d'administration ne reçoit que les informations relatives à la liste des noms NetBIOS des appareils de tous les domaines et des groupes de travail du réseau. Au cours d'un sondage complet, les informations suivantes sont demandées à chaque appareil client :

- Nom du système d'exploitation
- Adresse IP
- Nom DNS
- Nom NetBIOS

Les sondages rapides et complets nécessitent les éléments suivants :

- Les ports UDP 137/138, TCP 139 doivent être disponibles sur le réseau.
- Le service Microsoft Computer Browser doit être utilisé et l'ordinateur du navigateur primaire doit être activé sur le point de distribution.
- Le service Microsoft Computer Browser doit être utilisé et l'ordinateur du navigateur primaire doit être activé sur les appareils clients :
  - Sur au moins un appareil, si le nombre d'appareils en réseau ne dépasse pas 32.
  - Sur au moins un appareil pour 32 appareils en réseau.

Le sondage complet ne peut s'exécuter que si le sondage rapide a été exécuté au moins une fois.

Affichage et modification des paramètres de sondage du réseau Windows

Pour modifier les paramètres du sondage du réseau Windows, procédez comme suit :

1. Dans le menu principal, cliquez sur l'icône des paramètres ( ) en regard du nom du Serveur d'administration requis.

   La fenêtre des propriétés du Serveur d'administration s'ouvre.

2. Sous l'onglet **Général**, sélectionnez la section **Points de distribution**.
3. Cliquez sur le nom du point de distribution que vous souhaitez utiliser pour sonder le réseau.

   La fenêtre Propriétés du point de distribution s'affiche.

4. Sélectionnez la section **Sondage des domaines Windows**.
5. Activez ou désactivez le sondage réseau Windows à l'aide du bouton à bascule **Autoriser le sondage du réseau**.

6. Configurez la programmation pour le sondage rapide et le sondage complet.

7. Cliquez sur le bouton **OK**.

Les propriétés sont enregistrées et appliquées à l'ensemble des domaines Windows et des groupes de travail.

Sondage du contrôleur de domaine

Kaspersky Security Center Cloud Console prend en charge le sondage d'un contrôleur de domaine Microsoft Active Directory et d'un contrôleur de domaine Samba uniquement en utilisant un point de distribution.

Kaspersky Security Center Cloud Console permet de sonder un contrôleur de domaine Samba uniquement à l'aide d'un point de distribution Linux. Pour un contrôleur de domaine Samba, Samba 4 est utilisé comme contrôleur de domaine Active Directory.

Lorsque vous interrogez un contrôleur de domaine, un point de distribution récupère des informations sur la structure du domaine, les comptes utilisateurs, les groupes de sécurité et les noms DNS des appareils inclus dans le domaine. Le sondage du contrôleur de domaine est exécuté selon la planification que vous avez définie.

Prérequis

Avant d'interroger un contrôleur de domaine, assurez-vous que les protocoles suivants sont activés :

- Couche d'authentification et de sécurité simple (SASL)
- Protocole d'accès léger à l'annuaire (LDAP)

Assurez-vous que les ports suivants sont disponibles sur l'appareil du contrôleur de domaine :

- 389 pour SASL
- 636 pour TLS

Sondage du contrôleur de domaine à l'aide d'un point de distribution

Vous pouvez également interroger un contrôleur de domaine à l'aide d'un point de distribution. Un appareil administré basé sur Windows ou Linux peut servir de point de distribution.

Pour un point de distribution Linux, le sondage d'un contrôleur de domaine Microsoft Active Directory et d'un contrôleur de domaine Samba est pris en charge.
Pour un point de distribution Windows, seule le sondage d'un contrôleur de domaine Microsoft Active Directory est pris en charge.
Le sondage avec un point de distribution Mac n'est pas pris en charge.

Pour configurer le sondage du contrôleur de domaine à l'aide du point de distribution :

1. Ouvrez les propriétés du point de distribution.

2. Sélectionnez la section **Sondage du contrôleur de domaine**.

3. Sélectionnez l'option **Activer le sondage du contrôleur de domaine**.

4. Sélectionnez le contrôleur de domaine que vous souhaitez interroger.

   Si vous utilisez un point de distribution Linux, dans la section **Sonder les domaines 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**

5. Cliquez sur le bouton **Planifier le sondage** pour spécifier les options de planification du sondage si nécessaire.

   Le sondage démarre uniquement selon le calendrier spécifié. Le démarrage manuel du sondage n'est pas disponible.

Une fois le sondage terminé, la structure du domaine sera affichée dans la section **Contrôleurs de domaine**.

Si vous configurez et activez les règles de déplacement de l'appareil, les appareils détectés sont automatiquement inclus dans le groupe **Appareils administrés**. Si aucune règle de déplacement n'est activée, les nouveaux appareils détectés sont automatiquement inclus dans le groupe **Appareils non définis**.

Les comptes utilisateurs découverts peuvent être utilisés pour l'authentification de domaine dans Kaspersky Security Center Cloud Console.

Affichage des résultats du sondage du contrôleur de domaine

Pour afficher les résultats du sondage du contrôleur de domaine :

1. Dans le menu principal, accédez à **Découverte et déploiement** → **Découverte** → **Contrôleurs de domaine**.

   La liste des unités organisationnelles découvertes s'affiche.

2. Sélectionnez une unité organisationnelle, puis cliquez sur le bouton **Appareils**.

   La liste des appareils de l'unité organisationnelle s'affiche.

Vous pouvez effectuer une recherche dans la liste et filtrer les résultats.

Sondage des plages IP

Kaspersky Security Center Cloud Console tente de réaliser une résolution de nom inverse pour chacune des adresses de la plage définie en un nom DNS à l'aide des requêtes DNS standard. Si cette opération réussit, le serveur envoie une `ICMP ECHO REQUEST` (idem qu'une commande ping) au nom reçu. Si l'appareil répond, les informations à son sujet sont ajoutées à la base de données de Kaspersky Security Center Cloud Console. La résolution de nom inverse est nécessaire pour exclure les appareils réseau qui ne peuvent avoir d'adresse IP mais qui ne sont pas des ordinateurs, par exemple, les imprimantes réseau ou les routeurs.

Cette méthode de sondage repose sur un service DNS local correctement configuré. Il doit avoir une zone de recherche inversée. Si cette zone n'est pas configurée, le sondage du sous-réseau IP ne donnera aucun résultat. Sur les réseaux qui utilisent Active Directory, cette zone est maintenue automatiquement. Mais sur ces réseaux, le sondage du sous-réseau IP n'offre pas plus d'informations que le sondage Active Directory. De plus, les administrateurs de petits réseaux configurent rarement la zone de recherche inversée car elle n'est pas indispensable au fonctionnement de nombreux services réseau. Pour toutes ces raisons, le sondage du sous-réseau IP est désactivé par défaut.

Kaspersky Security Center Cloud Console obtient d'abord les plages IP pour le sondage dans les paramètres réseau de l'appareil du point de distribution utilisé pour le sondage. 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 Cloud Console inclut automatiquement le réseau 192.168.0.0/24 dans la liste des adresses de sondage. Kaspersky Security Center Cloud Console sonde dans ce cas toutes les adresses entre 192.168.0.1 et 192.168.0.254.

Il n'est pas recommandé d'utiliser le sondage des plages IP si vous utilisez le sondage réseau Windows et/ou le sondage Active Directory.

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, cliquez sur l'icône des paramètres ( ) en regard du nom du Serveur d'administration requis.

   La fenêtre des propriétés du Serveur d'administration s'ouvre.

2. Sous l'onglet **Général**, sélectionnez la section **Points de distribution**.

3. Cliquez sur le nom du point de distribution que vous souhaitez utiliser pour sonder le réseau.

   La fenêtre Propriétés du point de distribution s'affiche.

4. Sélectionnez la section **Sondage des plages IP**.

5. Activez ou désactivez le sondage des plages IP à l'aide du commutateur **Autoriser le sondage des plages**.

6. Configuration de la programmation de l'interrogation. Par défaut, l'interrogation IP est exécutée toutes les 420 minutes (sept heures).

7. Si nécessaire, ajoutez ou modifiez des plages IP à sonder.

   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.

8. Cliquez sur le bouton **OK**.

Les propriétés sont enregistrées et appliquées à toutes les plages IP.

Configuration d'un contrôleur de domaine Samba

Kaspersky Security Center Cloud Console 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 Cloud Console et le contrôleur de domaine Samba.

Pour activer la compatibilité totale d'un contrôleur de domaine Samba avec un contrôleur de domaine Microsoft Active Directory :

1. Exécutez la commande suivante pour utiliser l'extension de schéma RFC2307 :

   ```
   samba-tool domain provision --use-rfc2307 --interactive
   ```

2. Activez la mise à jour du schéma dans un contrôleur de domaine Samba. Pour ce faire, ajoutez la ligne suivante au fichier /etc/samba/smb.conf :

   ```
   dsdb:schema update allowed = true
   ```

   Si la mise à jour du schéma aboutit à une erreur, vous devez effectuer une restauration complète du contrôleur de domaine qui fait office de maître de schéma.

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

Ajout et modification d'une plage IP

Kaspersky Security Center Cloud Console obtient d'abord les plages IP pour le sondage dans les paramètres réseau de l'appareil du point de distribution utilisé pour le sondage. 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 Cloud Console inclut automatiquement le réseau 192.168.0.0/24 dans la liste des adresses de sondage. Kaspersky Security Center Cloud Console 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.

Pour ajouter une nouvelle plage IP, procédez comme suit :

1. Dans le menu principal, cliquez sur l'icône des paramètres ( ) en regard du nom du Serveur d'administration requis.

   La fenêtre des propriétés du Serveur d'administration s'ouvre.

2. Sous l'onglet **Général**, sélectionnez la section **Points de distribution**.

3. Cliquez sur le nom du point de distribution que vous souhaitez utiliser pour sonder le réseau.

   La fenêtre Propriétés du point de distribution s'affiche.

4. Sélectionnez la section **Sondage des plages IP**.

5. Pour ajouter une nouvelle plage IP, cliquez sur le bouton **Ajouter**.

6. Dans la fenêtre qui s'ouvre, configurez les paramètres suivants :

- **Nom**

  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 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.

- **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.

7. Cliquez sur le bouton **OK**.

La nouvelle plage IP est ajoutée à la liste des plages IP.

Une fois l'interrogation terminée, vous pouvez consulter la liste des appareils à l'aide du bouton **Appareils**. Par défaut, la durée de vie des résultats du sondage est de 24 heures, et est égale au réglage de la durée de vie de l'adresse IP.

Réglage des points de distribution et des passerelles de connexion

Une structure de groupes d'administration de Kaspersky Security Center Cloud Console remplit les fonctions suivantes :

- Désignation de la zone d'action des stratégies

  Il existe une autre méthode d'application des paramètres nécessaires sur les appareils : le recours aux *profils de stratégie*. Dans ce cas, la zone d'action des stratégies est définie à l'aide de tags, de l'emplacement des appareils dans les sous-divisions Active Directory, de l'appartenance aux groupes de sécurité Active Directory, etc.

- 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.

- Définit les privilèges d'accès aux appareils et aux Serveurs d'administration secondaires.

- 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.

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. Utilisez les tableaux ci-dessous pour calculer le nombre de points de distribution requis pour votre réseau.

Assurez-vous que les appareils que vous souhaitez utiliser comme points de distribution disposent de suffisamment d'espace libre sur le disque, qu'ils ne sont pas régulièrement éteints et que le " mode veille " est désactivé.

Nombre de points de distribution exclusivement attribués sur un réseau qui contient un segment unique, sur la base du nombre d'appareils en réseau

Nombre d'appareils clients administrés dans le segment du réseau	Nombre des points de distribution
Moins de 300	0 (ne pas assigner de points de distribution)
Plus de 300	Acceptable : (N/10 000 + 1), recommandé : (N/5 000 + 2), où N représente le nombre d'appareils sur le réseau

Nombre de points de distribution exclusivement attribués sur un réseau qui contient plusieurs segments, sur la base du nombre d'appareils en réseau

Nombre d'appareils clients par segment de réseau	Nombre des points de distribution
Moins de 10	0 (ne pas assigner de points de distribution)
10... 100	1
Plus de 100	Acceptable : (N/10 000 + 1), recommandé : (N/5 000 + 2), où N représente le nombre d'appareils sur le réseau

Utilisation d'appareils clients standard (postes de travail) en tant que points de distribution

Si vous avez l'intention d'utiliser des appareils clients standard (à savoir, des postes de travail) en tant que points de distribution, nous vous conseillons de les désigner comme dans les tableaux ci-dessous afin d'éviter une charge excessive des canaux de communication et du Serveur d'administration :

Nombre de postes de travail servant de points de distribution sur un réseau qui contient un segment unique, sur la base du nombre d'appareils en réseau

Nombre d'appareils clients administrés dans le segment du réseau	Nombre des points de distribution
Moins de 300	0 (ne pas assigner de points de distribution)
Plus de 300	(N/300 +1), où N est le nombre des appareils sur le réseau ; il doit y avoir au moins 3 points de distribution

Nombre de postes de travail servant de points de distribution sur un réseau qui contient plusieurs segments, sur la base du nombre d'appareils en réseau

Nombre d'appareils clients par segment de réseau	Nombre des points de distribution
Moins de 10	0 (ne pas assigner de points de distribution)
10... 30	1

31… 300	2
Plus de 300	(N/300 +1), où N est le nombre des appareils sur le réseau ; il doit y avoir au moins 3 points de distribution

Si aucun point de distribution n'est disponible, mettez à jour les bases de données, les modules logiciels et les applications de Kaspersky manuellement ou directement à partir des serveurs de mise à jour de Kaspersky.

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 :

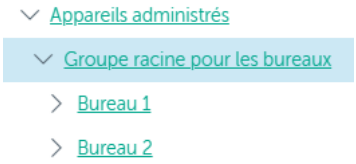
- Construction de la structure des groupes d'administration en tenant compte de la topologie du réseau. La structure des groupes d'administration ne doit pas obligatoirement refléter exactement la topologie du réseau. Il suffit que quelques groupes d'administration correspondent à des parties du réseau mises en évidence.

- Construction de la structure des groupes d'administration qui ne reflète pas la topologie du réseau. Dans ce cas, il faut désigner dans chaque partie du réseau mise en évidence un ou plusieurs appareils en tant que points de distribution sur le groupe d'administration racine, par exemple, sur le groupe **Appareils administrés**. Tous les points de distribution se trouvent au même niveau et possèdent la même zone d'action, à savoir " tous les appareils du réseau de l'entreprise ". Chaque Agent d'administration se connecte dans ce cas au point de distribution qui possède l'itinéraire le plus court. L'utilitaire tracert permet de définir l'itinéraire d'accès au point de distribution.

Configuration typique des points de distribution : plusieurs petits bureaux isolés

Cette configuration typique correspond à plusieurs petits bureaux distants, potentiellement connectés au siège principal via Internet. Chacun de ces bureaux distants se trouve au-delà du NAT. Autrement dit, la connexion d'un bureau distant à un autre est impossible. Ils sont isolés.

La configuration doit absolument se refléter dans la structure des groupes d'administration : pour chacun des bureaux distants. il faut créer un groupe d'administration distinct (les groupes **Bureau 1**, **Bureau 2** sur l'illustration ci-après).



Bureaux distants affichés dans la structure des groupes d'administration

Sur chaque groupe d'administration correspondant à un bureau, il faut désigner un ou plusieurs points de distribution. Les points de distribution doivent être des appareils du bureau distant dotés d'espace suffisant sur le disque. Ainsi, les appareils qui se trouvent par exemple dans le groupe **Bureau 1** vont contacter les points de distribution assignés au groupe d'administration **Bureau 1**.

Si certains utilisateurs se déplacent d'un bureau à l'autre avec des ordinateurs portables, il faut sélectionner dans chaque bureau distant, en plus des points de distribution cités ci-dessus, deux ou plusieurs appareils et les assigner comme points de distribution pour le groupe d'administration de niveau supérieur (le groupe **Groupe racine pour les bureaux** dans l'illustration ci-dessus).

Exemple : Par exemple, voici un ordinateur portable qui se trouve dans le groupe d'administration **Bureau 1**, mais qui est déplacé physiquement dans le bureau qui correspond au groupe **Bureau 2**. Après le déplacement, l'Agent d'administration sur l'ordinateur portable tente de contacter les points de distribution assignés au groupe **Bureau 1**, mais ceux-ci ne sont pas accessibles. Alors l'Agent d'administration commence à contacter les points de distribution désignés pour le groupe **Groupe racine pour les bureaux**. Étant donné que les bureaux distants sont isolés les uns des autres, seules les requêtes d'accès aux points de distribution assignés au groupe d'administration **Groupe racine pour les bureaux** aboutissent lorsque l'Agent d'administration tente d'accéder aux points de distribution dans le groupe **Bureau 2**. Autrement dit, l'ordinateur portable demeure dans le groupe d'administration qui correspond à son bureau d'origine, mais il utilise malgré tout le point de distribution du bureau où il se trouve physiquement à l'heure actuelle.

Assignation manuelle des points de distribution

Kaspersky Security Center Cloud Console permet de désigner manuellement des appareils comme points de distribution. Nous vous recommandons de calculer le nombre et la configuration de points de distribution nécessaires pour votre réseau.

Les appareils de points de distribution exécutant macOS ne peuvent pas télécharger les mises à jour à partir des serveurs de mises à jour de Kaspersky.

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

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

Pour désigner manuellement un appareil comme point de distribution :

1. Dans le menu principal, cliquez sur l'icône des paramètres ( ) en regard du nom du Serveur d'administration requis.

   La fenêtre des propriétés du Serveur d'administration s'ouvre.

2. Sous l'onglet **Général**, sélectionnez la section **Points de distribution**.

3. Cliquez sur le bouton **Désigner**.

4. 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.

5. Sélectionnez le groupe d'administration que vous voulez inclure dans le champ du point de distribution sélectionné.

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

   Le point de distribution que vous avez ajouté sera affiché dans la liste des points de distribution, dans la section **Points de distribution**.

7. Sélectionnez le nouveau point de distribution dans la liste pour ouvrir la fenêtre de ses propriétés.

8. Configurez le point de distribution dans la fenêtre des propriétés :

- Dans la section **Général**, indiquez les paramètres d'interaction entre le point de distribution et les appareils clients :

  - **Port SSL**

    Le numéro du port SSL utilisé pour la connexion sécurisée des appareils clients au point de distribution via le protocole SSL.

    Le numéro de port est de 13000 par défaut.

  - **Utiliser la multidiffusion**

    Si cette option est activée, la multidiffusion pour la diffusion automatique des paquets d'installation sur les appareils clients du groupe sera utilisée.

    La diffusion IP multidiffusion réduit le temps nécessaire à l'installation d'une application à partir d'un paquet d'installation sur un groupe d'appareils clients, mais prolonge le temps d'installation lorsque vous installez une application sur un seul appareil client.

  - **Adresse IP de multidiffusion**

    Adresse IP sur laquelle est exécuté l'envoi diffusion multiadresse. L'adresse IP peut être indiquée dans l'intervalle 224.0.0.0 – 239.255.255.255

    Par défaut, Kaspersky Security Center Cloud Console attribue automatiquement une adresse IP de multidiffusion unique dans la plage donnée.

  - **Numéro du port IP de multidiffusion**

    Numéro du port de diffusion multiadresse.

    Le numéro de port est de 15001 par défaut. Dans le cas où le point de distribution tourne sur un appareil sur lequel est également installé un Serveur d'administration, le numéro de port par défaut pour la connexion SSL est 13001.

  - **Déployer les mises à jour**

    Les mises à jour sont distribuées aux appareils administrés à partir des sources suivantes :

    - Ce point de distribution si cette option est activée.
    - Autres points de distribution, Serveur d'administration ou serveurs de mise à jour Kaspersky si cette option est désactivée.

    Si vous utilisez des points de distribution pour déployer des mises à jour, vous pouvez économiser du trafic parce que vous réduisez le nombre de téléchargements. Vous pouvez aussi alléger la charge sur le Serveur d'administration et répartir la charge entre les points de distribution. Vous pouvez calculer le nombre de points de distribution de votre réseau pour optimiser le trafic et la charge.

    Si vous désactivez cette option, le nombre de téléchargements de mises à jour et de charges sur le Serveur d'administration peut augmenter. Cette option est activée par défaut.

  - **Déployer les paquets d'installation**

Les paquets d'installation sont distribuées aux appareils administrés à partir des sources suivantes :

- Ce point de distribution si cette option est activée.
- Autres points de distribution, Serveur d'administration ou serveurs de mise à jour Kaspersky si cette option est désactivée.

Si vous utilisez des points de distribution pour déployer des paquets d'installation, vous pouvez économiser du trafic parce que vous réduisez le nombre de téléchargements. Vous pouvez aussi alléger la charge sur le Serveur d'administration et répartir la charge entre les points de distribution. Vous pouvez calculer le nombre de points de distribution de votre réseau pour optimiser le trafic et la charge.

Si vous désactivez cette option, le nombre de téléchargements de paquets d'installation et de charges sur le Serveur d'administration peut augmenter. Cette option est activée par défaut.

- **Exécuter le serveur push**

  Dans Kaspersky Security Center Cloud Console, un point de distribution peut fonctionner comme un serveur push pour les appareils Windows et Linux administrés par l'Agent d'administration. Un serveur push a la même portée d'appareils administrés que le point de distribution sur lequel le serveur push est activé. Si plusieurs points de distribution sont affectés au même groupe d'administration, vous pouvez activer le serveur push sur chacun des points de distribution. Dans ce cas, le Serveur d'administration équilibre la charge entre les points de distribution.

- **Port du serveur push**

  Le numéro de port pour le serveur push. Vous pouvez préciser le numéro de tout port inoccupé.

- Dans la section **Zone d'action**, indiquez la zone dans laquelle le point de distribution va distribuer des mises à jour (groupes d'administration et/ou emplacement réseau).

  Seuls les appareils administrés sous Windows peuvent définir l'emplacement réseau. La définition de l'emplacement réseau est inaccessible pour les appareils administrés sous d'autres systèmes d'exploitation.

- 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.

Cette fonctionnalité n'est pas prise en charge par les appareils de point de distribution exécutant Linux ou macOS.

Le point de distribution envoie les statistiques KSN, lesquelles sont répertoriées dans la Déclaration de Kaspersky Security Network, à Kaspersky. Par défaut, la Déclaration KSN se trouve dans %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\ksneula.

Cette option est Inactif par défaut. L'activation de cette option prend effet uniquement si l'option **J'accepte les termes du Kaspersky Security Network** est activée 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.

- Configurez les paramètres de sondage par le point de distribution des domaines Windows, du contrôleur de domaine et des plages IP :

  - Sondage des domaines Windows

    Vous pouvez autoriser la recherche d'appareils pour les domaines Windows et programmer la recherche.

  - Sondage du contrôleur de domaine

    Vous pouvez autoriser le sondage du réseau pour Active Directory et programmer le sondage.

    Si vous utilisez un point de distribution Windows, vous pouvez sélectionner une des options suivantes :

    - **Sonder le domaine actuel Active Directory**.
    - **Sonder la forêt de domaines Active Directory**.
    - **Sonder les domaines indiqués Active Directory**. Si vous choisissez cette option, ajoutez un ou plusieurs domaines Active Directory à la liste.

    Si vous utilisez un point de distribution Linux avec l'Agent d'administration version 15 installé, vous ne pouvez interroger que les domaines Active Directory dont vous spécifiez l'adresse et les informations d'identification de l'utilisateur. Les sondages du domaine Active Directory actuel et de la forêt de domaines Active Directory ne sont pas disponibles.

Vous pouvez activer la découverte d'appareils pour les contrôleurs de domaine.

Si vous sélectionnez l'option **Activer le sondage du contrôleur de domaine**, vous pouvez sélectionner des contrôleurs de domaine pour le sondage et également spécifier le calendrier de sondage pour eux.

Si vous utilisez un point de distribution Linux, dans la section **Sonder les domaines 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**

- 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 indiqué

    Lors du choix de cette option, il est possible d'indiquer dans le champ situé ci-dessous le chemin d'accès au dossier. Le dossier peut être local sur le point de distribution ou distant, sur n'importe lequel des appareils faisant partie du réseau de l'entreprise.

    Le compte utilisateur, sous lequel l'Agent d'administration est lancé sur le point de distribution, doit posséder l'accès au dossier indiqué pour lecture et écriture.

9. Cliquez sur le bouton **OK**.

Les appareils sélectionnés sont comme des points de distribution.

Modifier la liste des points de distribution pour un groupe d'administration

Vous pouvez voir la liste des points de distribution assignés à un groupe d'administration spécifique et y ajouter ou en éliminer des points de distribution.

Pour voir et modifier la liste des points de distribution assignés à un groupe d'administration :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Groupes**.
2. Dans la structure du groupe d'administration, sélectionnez le groupe d'administration dont vous voulez voir les points de distribution assignés.
3. Cliquez sur l'onglet **Points de distribution**.
4. Ajoutez de nouveaux points de distribution pour le groupe d'administration à l'aide du bouton **Désigner** ou supprimez les points de distribution assignés à l'aide du 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.

Utilisation d'un point de distribution en tant que serveur push

Dans Kaspersky Security Center Cloud Console, un point de distribution peut fonctionner comme un serveur push pour les appareils Windows et Linux administrés par l'Agent 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 pouvez utiliser des points de distribution comme serveurs push pour garantir une connectivité continue 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'envoyer de paquets sur le port UDP de l'Agent d'administration.

Pour utiliser un point de distribution en tant que serveur push :

1. Dans le menu principal, cliquez sur l'icône des paramètres ( ) en regard du nom du Serveur d'administration requis.

   La fenêtre des propriétés du Serveur d'administration s'ouvre.
2. Sous l'onglet **Général**, sélectionnez la section **Points de distribution**.
3. Cliquez sur le point de distribution que vous souhaitez utiliser comme serveur push.
4. Dans la liste des propriétés du point de distribution sélectionné, accédez à la section **Général**, puis activez l'option **Exécuter le serveur push**.

   Le champ de saisie **Port du serveur push** est disponible.
5. Dans le champ de saisie **Port du serveur push**, spécifiez le port sur le point de distribution que les appareils clients utiliseront pour la connexion. Le numéro du port est de 13295 par défaut.

Pour établir une connexion entre le point de distribution agissant comme un serveur push et un appareil administré, vous devez ajouter manuellement le port de serveur push spécifié à la liste des exclusions du Pare-feu Microsoft Windows.

6. Cliquez sur **OK** pour quitter la fenêtre des propriétés du point de distribution, puis cliquez sur **Enregistrer** pour appliquer les modifications.

   Après avoir activé l'option **Exécuter le serveur push**, l'option **Maintenir la connexion au Serveur d'administration** est automatiquement activée sur le point de distribution qui agit comme un serveur push. Cette option permet d'établir une connexion anticipée entre l'Agent d'administration et le Serveur d'administration.

7. Ouvrez la fenêtre des propriétés de stratégie de l'Agent d'administration.

8. Accédez à **Connectivité** → **Réseau**, puis activez l'option **Utiliser le point de distribution pour forcer la connexion au Serveur d'administration**. Fermez le cadenas pour cette option.

9. Toujours dans la sous-section **Réseau**, vous pouvez désactiver l'option **Utiliser un port UDP**. Le serveur push configuré assure une connexion permanente entre l'appareil administré et le Serveur d'administration au lieu d'envoyer des paquets via le port UDP.

10. Cliquez sur le bouton **OK** pour quitter la fenêtre.

Le point de distribution commence à agir comme un serveur push. Il peut désormais envoyer des notifications push aux appareils client.

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 Cloud Console ne fournit pas de connexion permanente entre les appareils administrés et le Serveur d'administration. Les agents d'administration sur les appareils administrés établissent périodiquement une connexion et se synchronisent avec le Serveur d'administration. L'intervalle entre ces sessions de synchronisation est défini dans une stratégie de l'Agent d'administration. Si une synchronisation s'impose plus tôt, le Serveur d'administration (ou un point de distribution, s'il est en cours d'utilisation) envoie un paquet réseau signé sur un réseau IPv4 ou IPv6 vers le port UDP de l'Agent d'administration. Le numéro de port est de 15000 par défaut. Si aucune connexion via UDP entre le Serveur d'administration et l'appareil administré n'est possible, la synchronisation se déroulera lors de la prochaine connexion ordinaire de l'Agent d'administration au Serveur d'administration pendant l'intervalle de synchronisation.

Certaines opérations ne peuvent pas être exécutées sans connexion anticipée de l'Agent d'administration au Serveur d'administration, telles que le lancement et l'arrêt des tâches locales, la réception des statistiques de l'application administrée ou la création d'un tunnel. Pour résoudre ce problème, si vous n'utilisez pas de serveurs push, vous pouvez utiliser l'option **Maintenir la connexion au Serveur d'administration** pour assurer 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. Exécutez une des actions suivantes :

   - Si l'appareil administré accède au Serveur d'administration directement (c'est-à-dire pas via un point de distribution) :

a. Dans le menu principal, accédez à **Appareils** → **Appareils administrés**.

b. Cliquez sur le nom de l'appareil avec lequel vous souhaitez assurer une connexion permanente.

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

- Si l'appareil administré accède au Serveur d'administration via un point de distribution fonctionnant en mode passerelle, pas directement :

a. Dans le menu principal, cliquez sur l'icône des paramètres ( ) en regard du nom du Serveur d'administration requis.

La fenêtre des propriétés du Serveur d'administration s'ouvre.

b. Sous l'onglet **Général**, sélectionnez la section **Points de distribution**.

c. Dans la liste des points de distribution, cliquez sur le nom du point de distribution requis.

La fenêtre des propriétés du point de distribution sélectionné s'ouvre.

2. Dans la section **Général** de la fenêtre de propriétés ouverte, sélectionnez l'option **Maintenir la connexion au Serveur &d'administration**.

La connexion permanente est établie entre l'appareil administré et le Serveur d'administration.

Le total des appareils pour lesquels l'option **Maintenir la connexion au Serveur &d'administration** a été sélectionnée ne peut être supérieur à 300.

Création des groupes d'administration

Initialement, la hiérarchie des groupes d'administration contient le seul groupe d'administration intitulé **Appareils administrés**. Lors de la création d'une hiérarchie de groupes d'administration, vous pouvez ajouter des appareils et des machines virtuelles au groupe **Appareils administrés**, ainsi que des sous-groupes. La fenêtre des propriétés de chacun des groupes d'administration contient des informations sur les stratégies, les tâches et les appareils associés au groupe.

Pour créer un groupe d'administration, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Hiérarchie des groupes**.
2. Cochez la case en regard du groupe d'administration pour lequel vous souhaitez créer un sous-groupe.
3. Cliquez sur le bouton **Ajouter**.
4. Tapez un nom pour le nouveau groupe d'administration.
5. Cliquez sur le bouton **Ajouter**.

Un nouveau groupe d'administration portant le nom spécifié apparaît dans la structure hiérarchique du groupe d'administration.

L'application permet de créer une hiérarchie de groupes d'administration sur la base de la structure d'Active Directory ou de la structure du réseau de domaine. Vous pouvez aussi créer une structure de groupes du fichier texte.

Pour créer une structure de groupes d'administration, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Hiérarchie des groupes**.
2. Cliquez sur le bouton **Importer**.

   Finalement, l'assistant de création de la structure des groupes d'administration se lance. Suivez les instructions de l'assistant.

Création des règles de déplacement des appareils

Vous pouvez configurer les règles de déplacement des appareils qui attribuent automatiquement des appareils à des groupes d'administration.

Pour créer une règle de déplacement, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Règles de déplacement**.
2. Cliquez sur **Ajouter**.
3. Dans la fenêtre qui s'ouvre, précisez les informations suivantes sous l'onglet **Général** :

   - **Nom de la règle**

     Saisissez un nom pour la nouvelle règle.

     Si vous copiez une règle, la nouvelle règle obtient le même nom que la règle de source, mais un index au format () est ajouté au nom, par exemple : (1).

   - **Groupe d'administration**

     Sélectionnez le groupe d'administration dans lequel les appareils seront déplacés automatiquement.

   - **Règle active**

     Si cette option est activée, la règle est activée et commence à s'applique après avoir été enregistrée.

     Si cette option est désactivée, la règle est créée mais pas activée. Elle ne fonctionnera pas jusqu'à ce que vous activiez cette option.

   - **Déplacer uniquement les appareils non inclus dans un groupe d'administration**

     Si cette option est activée, seuls les appareils non définis sont déplacés dans le groupe sélectionné.

     Si cette option est désactivée, les appareils qui appartiennent déjà à d'autres groupes d'administration ainsi que les appareils non définis seront déplacés dans le groupe sélectionné.

- Exécution de la règle

  Vous avez le choix parmi les options suivantes :

  - **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 augmenter ou diminuer la priorité d'une règle en mouvement, déplacez la règle vers le haut ou vers le bas dans la liste, respectivement, à l'aide de la souris.

Si l'option **Appliquer la règle en continu** est sélectionnée, la règle de déplacement est appliquée quels que soient les paramètres de priorité. Ces règles sont appliquées selon la planification que le Serveur d'administration configure automatiquement.

Si les attributs de l'appareil satisfont directement à plusieurs règles, l'appareil est placé dans le groupe cible de la règle qui affiche la priorité la plus élevée (la règle qui figure plus haut dans la liste).

Copie des règles de déplacement des appareils

Vous pouvez copier les règles de déplacement par exemple si vous souhaitez avoir plusieurs règles identiques pour différents groupes d'administration cibles.

Pour copier une règle de déplacement existante, procédez comme suit :

1. Exécutez une des actions suivantes :

   - Dans le menu principal, accédez à **Ressources (Appareils)** → **Règles de déplacement**.

   - Dans le menu principal, accédez à **Découverte et déploiement** → **Déploiement et attribution** → **Règles de déplacement**.

La liste des règles de déplacement s'affiche.

2. Cochez la case en regard de la règle que vous souhaitez copier.

3. Cliquez sur **Copier**.

4. Dans la fenêtre qui s'ouvre, modifiez les informations suivantes sous l'onglet **Général** ou ne changez rien si vous souhaitez uniquement copier la règle sans modifier ses paramètres :

   - **Nom de la règle**

     Saisissez un nom pour la nouvelle règle.

     Si vous copiez une règle, la nouvelle règle obtient le même nom que la règle de source, mais un index au format () est ajouté au nom, par exemple : (1).

   - **Groupe d'administration**

     Sélectionnez le groupe d'administration dans lequel les appareils seront déplacés automatiquement.

   - **Règle active**

     Si cette option est activée, la règle est activée et commence à s'applique après avoir été enregistrée.

     Si cette option est désactivée, la règle est créée mais pas activée. Elle ne fonctionnera pas jusqu'à ce que vous activiez cette option.

   - **Déplacer uniquement les appareils non inclus dans un groupe d'administration**

     Si cette option est activée, seuls les appareils non définis sont déplacés dans le groupe sélectionné.

     Si cette option est désactivée, les appareils qui appartiennent déjà à d'autres groupes d'administration ainsi que les appareils non définis seront déplacés dans le groupe sélectionné.

   - **Exécution de la règle**

     Vous avez le choix parmi les options suivantes :

     - **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.
- Les applications administrées installées sur les appareils clients, par exemple, l'Agent d'administration ou le Serveur d'administration.
- Les machines virtuelles, qui sont les appareils clients.
- Informations sur l'unité d'organisation (OU) Active Directory avec les appareils clients.
- Informations sur un segment dans le Cloud avec les appareils clients.

Vous trouverez ci-dessous la description de la manière de spécifier ces informations dans une règle de déplacement des appareils.

Si vous spécifiez plusieurs conditions dans la règle, l'opérateur logique ET fonctionne et toutes les conditions s'appliquent en même temps. Si vous ne sélectionnez aucune option ou si vous laissez certains champs vides, ces conditions ne s'appliquent pas.

Onglet Tags

Sur cet onglet, vous pouvez configurer une règle de déplacement de l'appareil basée sur les tags de l'appareil qui ont été précédemment ajoutés aux descriptions des appareils clients. Pour ce faire, sélectionnez les balises requises. Vous pouvez également activer les options suivantes :

- **Appliquer aux appareils sans les tags sélectionnés**

  Si cette option est activée, tous les appareils avec les tags indiqués sont exclus de la règle de déplacement des appareils. Si cette option est désactivée, la règle de déplacement des appareils s'applique aux appareils avec tous les tags sélectionnés.

  Cette option est Inactif par défaut.

- **Appliquer si au moins un tag sélectionné coïncide**

  Si cette option est activée, une règle de déplacement des appareils s'applique aux appareils clients avec au moins une des balises sélectionnées. Si cette option est désactivée, la règle de déplacement des appareils s'applique aux appareils avec tous les tags sélectionnés.

  Cette option est Inactif par défaut.

Onglet Réseau

Sous cet onglet, vous pouvez spécifier les données réseau des appareils pris en compte par une règle de déplacement des appareils :

- **Nom de l'appareil sur le réseau Windows**

  Nom de réseau Windows (nom NetBIOS) de l'appareil ou adresse IPv4 ou IPv6.

- **Domaine Windows**

  Une règle de déplacement des appareils s'applique à tous les appareils inclus dans le domaine Windows indiqué.

- **Nom 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 Cloud Console, 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 appartient à la plage IP**

  Si cette option est activée, vous pouvez sélectionner une plage IP que vous avez précédemment ajoutée dans la section **Plages IP**. Les appareils concernés doivent être inclus dans la plage IP sélectionnée.

  Cette option est Inactif par défaut.

- Profil de connexion modifié

  Sélectionnez l'une des valeurs ci-dessous :

  - **Oui**. Une règle de déplacement des appareils s'applique uniquement aux appareils clients dont le profil de connexion a été modifié.
  - **Non**. La règle de déplacement des appareils s'applique uniquement aux appareils clients dont le profil de connexion n'a pas changé.
  - **La valeur n'est pas sélectionnée**. La condition ne s'applique pas.

- Administrés par un autre Serveur d'administration

  Sélectionnez l'une des valeurs ci-dessous :

  - **Oui**. Une règle de déplacement des appareils s'applique uniquement aux appareils clients administrés par d'autres Serveurs d'administration. Ces Serveurs sont différents du Serveur sur lequel vous configurez la règle de déplacement des appareils.
  - **Non**. La règle de déplacement des appareils s'applique uniquement aux appareils clients administrés par le Serveur d'administration actuel.
  - **La valeur n'est pas sélectionnée**. La condition ne s'applique pas.

Onglet Applications

Cet onglet permet de configurer une règle de déplacement des appareils en fonction des applications administrées et des systèmes d'exploitation installés sur les appareils clients :

- L'Agent d'administration est installé

  Sélectionnez l'une des valeurs ci-dessous :

  - **Oui**. Une règle de déplacement des appareils s'applique uniquement aux appareils clients sur lesquels l'Agent d'administration est installé.
  - **Non**. La règle de déplacement des appareils s'applique uniquement aux appareils clients sur lesquels l'Agent d'administration n'est pas installé.
  - **La valeur n'est pas sélectionnée**. La condition ne s'applique pas.

- Applications

  Spécifiez les applications administrées qui doivent être installées sur les appareils clients, de sorte qu'une règle de déplacement des appareils s'applique à ces appareils. Par exemple, vous pouvez sélectionner **Agent d'administration de Kaspersky Security Center 15.3** ou **Serveur d'administration de Kaspersky Security Center 15.3**.

  Si vous ne sélectionnez aucune application administrée, la condition ne s'applique pas.

- Version du système d'exploitation

Vous pouvez supprimer les appareils clients en fonction de la version du système d'exploitation. Pour ce faire, indiquez les systèmes d'exploitation qui doivent être installés sur les appareils clients. Par conséquent, une règle de déplacement des appareils s'applique aux appareils clients avec les systèmes d'exploitation sélectionnés.

Si vous n'activez pas cette option, la condition ne s'applique pas. L'option est désactivée par défaut.

- Capacité du système d'exploitation

  Vous pouvez sélectionner les appareils clients en fonction de la taille des bits du système d'exploitation. Dans le champ **Capacité du système d'exploitation**, vous pouvez sélectionner une des valeurs suivantes :

  - **Inconnu**
  - **x86**
  - **AMD64**
  - **IA64**

  Pour vérifier la taille en bits du système d'exploitation des appareils clients, procédez comme suit :

  1. Dans le menu principal, accédez à la section **Ressources (Appareils)** → **Appareils administrés**.
  2. Cliquez sur le bouton **Paramètres des colonnes** ( ) à droite.
  3. Sélectionnez l'option **Capacité du système d'exploitation**, puis cliquez sur le bouton **Enregistrer**.

     Ensuite, la taille en bits du système d'exploitation s'affiche pour chaque appareil administré.

- Version du paquet de mise à jour 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.

- Version du système d'exploitation

Ce paramètre concerne uniquement les systèmes d'exploitation Windows.

Vous pouvez indiquer si le système d'exploitation sélectionné doit avoir un numéro de version égal, antérieur ou supérieur. Vous pouvez aussi configurer une règle de déplacement de l'appareil pour tous les numéros de version, à l'exception du numéro indiqué.

- Numéro de version du système d'exploitation

  Ce paramètre concerne uniquement les systèmes d'exploitation Windows.

  Vous pouvez indiquer si le système d'exploitation sélectionné doit avoir un numéro de version égal, antérieur ou supérieur. Vous pouvez également configurer une règle de déplacement des appareils pour tous les numéros de version, à l'exception de celui indiqué.

Onglet Machines virtuelles

Sous cet onglet, vous pouvez configurer une règle de déplacement des appareils selon que les appareils clients sont des machines virtuelles ou font partie d'une infrastructure de bureau virtuel (VDI) :

- Est une machine virtuelle

  Dans la liste déroulante, vous pouvez sélectionner une des options suivantes :
  - **N/A**. La condition ne s'applique pas.
  - **Non**. Déplacez les appareils qui ne sont pas des machines virtuelles.
  - **Oui**. Déplacez les appareils qui sont des machines virtuelles.

- **Type 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'appareils s'applique aux appareils de l'unité d'organisation Active Directory indiquée 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 Active Directory.

  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'appareils s'applique aux appareils du groupe Active Directory indiqué dans la liste sous l'option.

  Cette option est Inactif par défaut.

Onglets Segments dans le Cloud

Cet onglet vous permet d'indiquer qu'il est nécessaire de déplacer les appareils qui appartiennent à certains segments dans le Cloud :

- L'appareil se trouve dans 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.

  L'option est désactivée par défaut.

- Objets enfants inclus

  Si vous sélectionnez cette option, une règle de déplacement d'appareils s'applique non seulement au segment dans le Cloud sélectionné, mais également aux objets enfants de ce segment.

  L'option est désactivée par défaut.

- **Déplacer les appareils des objets enfants vers les sous-groupes correspondants**
- **Créer 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

La liste déroulante permet de choisir s'vous pouvez détecter un appareil à l'aide des outils de l'API :

- **AWS**. L'appareil est détecté via l'utilisation de l'API AWS, autrement dit, l'appareil est bel et bien dans l'environnement cloud AWS.
- **Azure**. L'appareil est détecté via l'utilisation de l'API Azure, autrement dit, l'appareil est bel et bien dans l'environnement cloud Azure.
- **Google Cloud.** L'appareil est détecté via l'utilisation de l'API Google, autrement dit, l'appareil est bel et bien dans le cloud Google.
- **Non**. L'appareil n'est pas détecté à l'aide de l'API AWS, Azure ou Google, c'est-à-dire qu'il se trouve soit en dehors de l'environnement Cloud, soit dans l'environnement Cloud, mais il ne peut pas être détecté à l'aide d'une API.
- **Pas de valeur**. Cette condition ne s'applique pas.

Ajout manuel d'appareils à un groupe d'administration

Vous pouvez déplacer des appareils vers des groupes d'administration automatiquement en créant des règles de déplacement d'appareils ou manuellement en déplaçant des appareils d'un groupe d'administration vers un autre ou en ajoutant des appareils à un groupe d'administration sélectionné. Cette section décrit comment ajouter manuellement des appareils à un groupe d'administration.

Pour ajouter manuellement un ou plusieurs appareils à un groupe d'administration sélectionné, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Appareils administrés**.
2. 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 :

     Cliquez sur le bouton **Modifier la portée** 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.
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.
  - Indiquez le nom NetBIOS ou le nom DNS d'un 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 : , \ / * ; : & ` ~ ! @ # $ ^ & ( ) = + [ ] { } | , < > %

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, réalisez une des opérations suivantes :
   - Pour ouvrir un groupe d'administration, dans le menu principal, accédez à **Ressources (Appareils)** → **Groupes** → **<nom du groupe>** → **Appareils administrés**.
   - Pour ouvrir le groupe **Appareils non définis**, dans le menu principal, accédez à **Découverte et déploiement** → **Appareils non définis**.

2. Si le groupe d'administration contient des clusters ou des groupes de serveurs, la section **Appareils administrés** est divisée en deux onglets : l'onglet **Appareils** et l'onglet **Clusters et matrices 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.

Configuration des règles de rétention pour les appareils non définis

Une fois le sondage du réseau Windows terminé, les appareils trouvés sont placés dans des sous-groupes du groupe d'administration Appareils non définis. Ce groupe d'administration se trouve à l'emplacement **Découverte et déploiement → Découverte → Domaines Windows**. Le dossier **Domaines Windows** est le groupe parent. Il contient les groupes enfants nommés après que les domaines et les groupes de travail correspondant ont été trouvés lors du sondage. Le groupe parent peut également contenir le groupe d'administration des appareils mobiles. Vous pouvez configurer les règles de rétention des appareils non définis pour le groupe parent et pour chacun des groupes enfant. Les règles de conservation ne dépendent pas des paramètres de recherche d'appareil et fonctionnent même si la recherche d'appareil est désactivée.

Les règles de conservation des appareils n'affectent pas les appareils dont un ou plusieurs disques sont chiffrés à l'aide du chiffrement du disque. Ces appareils ne sont pas supprimés automatiquement. Vous ne pouvez les supprimer que manuellement. Si vous devez supprimer un appareil doté d'un disque chiffré, commencez par déchiffrer le disque, puis supprimez l'appareil.

Pour configurer les règles de rétention pour les appareils non définis :

1. Dans le menu principal, accédez à **Découverte et déploiement → Découverte → Domaines Windows**.

2. Exécutez une des actions suivantes :

   - Pour configurer les paramètres du groupe parent, cliquez sur le bouton **Propriétés**.

     La fenêtre des propriétés du domaine Windows s'ouvre.

   - Pour configurer les paramètres d'un groupe enfant, cliquez sur son nom.

     La fenêtre des propriétés du groupe enfant s'ouvre.

3. Configurez les paramètres suivants :

   - **Supprimer l'appareil du groupe après une inactivité de plus de (jours)**

     Quand cette option est activée, vous pouvez définir la période à l'issue de laquelle un appareil est supprimé automatiquement du groupe. Cette option est également distribuée par défaut aux groupes enfants. Par défaut, la valeur de cet intervalle est de 7 jours.

     Cette option est activée par défaut.

- **Hériter du groupe parent**

  Si cette option est activée, la période de conservation pour les appareils dans le groupe actif est héritée du groupe parent et ne peut être modifiée.

  Cette option est disponible uniquement pour les groupes enfant.

  Cette option est activée par défaut.

- **Forcer l'héritage des groupes enfants**

  Les valeurs des paramètres sont diffusées dans les groupes enfants mais ces paramètres sont verrouillés dans les propriétés des groupes enfants.

  Cette option est Inactif par défaut.

4. Cliquez sur le bouton **Accepter**.

Vos modifications sont enregistrées et appliquées.

Configuration de la protection réseau

Cette section fournit des informations sur la configuration manuelle des stratégies et des tâches, sur les rôles des utilisateurs et sur la création d'une structure de groupe d'administration et d'une hiérarchie des tâches.

Scénario : Configuration de la protection réseau

L'Assistant de démarrage rapide de l'application crée des stratégies et des tâches en utilisant les paramètres par défaut. Ces paramètres peuvent s'avérer imparfaits, ou même être interdits par l'organisation. Par conséquent, nous vous recommandons d'adapter ces stratégies et tâches et de créer d'autres stratégies et tâches, si elles sont nécessaires à votre réseau.

Prérequis

Avant de commencer, assurez-vous d'avoir terminé le scénario de configuration principale de Kaspersky Security Center Cloud Console, et notamment, de l'assistant de démarrage rapide de l'application.

L'Assistant de démarrage rapide de l'application crée dans le groupe d'administration **Appareils administrés** les stratégies et tâches suivantes :

- 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
- Recherche de vulnérabilités et de mises à jour requises (tâche de l'agent d'administration)

Étapes

La configuration de la protection réseau se fait par étapes :

1. **Configuration et propagation des stratégies et des profils de stratégie de Kaspersky**

   Pour configurer et propager les paramètres des applications Kaspersky installées sur les appareils administrés, deux méthodes différentes de gestion de la sécurité sont possibles : centrés sur l'utilisateur ou sur l'appareil. Vous pouvez également combiner ces deux approches.

2. **Configuration des tâches de gestion à distance des applications Kaspersky**

   Vérifiez les tâches créées avec l'assistant de démarrage rapide de l'application et adaptez si nécessaire.

   Instructions pour :

   - Paramétrage de la tâche de groupe de mise à jour de Kaspersky Endpoint Security
   - Création de la tâche *Recherche de vulnérabilités et de mises à jour requises*

   Le cas échéant, créez des tâches supplémentaires gérer les applications Kaspersky installées sur les appareils clients.

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. Vous pouvez également différencier les appareils en fonction de leur utilisation dans Active Directory ou de leurs spécifications matérielles.

La gestion de la sécurité centrée sur l'utilisateur vous permet d'appliquer différents paramètres d'application de sécurité à différents rôles d'utilisateur. Vous pouvez créer plusieurs rôles d'utilisateur, attribuer un rôle d'utilisateur approprié à chaque utilisateur et définir différents paramètres d'application pour les appareils appartenant à des utilisateurs dotés de rôles différents. Ainsi, vous souhaitez peut-être appliquer des paramètres des applications divergents pour les appareils des comptables et des collaborateurs des ressources humaines (RH). Par conséquent, lorsque l'administration de la sécurité centrée sur l'utilisateur est mise en œuvre, chaque département (les départements de comptabilité et RH) dispose de sa propre configuration de paramètres pour gérer les applications de Kaspersky. Une configuration de paramètres définit les paramètres d'application pouvant être modifiés par les utilisateurs et ceux définis de manière obligatoire et verrouillés par l'administrateur.

Utilisez une gestion de la sécurité centrée sur l'utilisateur pour pouvoir appliquer des paramètres d'application spécifiques pour des utilisateurs individuels. Cela peut être nécessaire lorsqu'un employé a un rôle unique dans l'entreprise ou lorsque vous souhaitez surveiller les problèmes de sécurité liés aux appareils d'une personne en particulier. Selon le rôle de cet employé dans l'entreprise, vous pouvez étendre ou limiter les droits de cette personne pour modifier les paramètres de l'application. Par exemple, vous souhaiterez peut-être étendre les droits d'un administrateur système qui gère les appareils clients d'une agence locale.

Il est également possible de combiner l'administration de la sécurité centrée sur l'appareil et celle centrée sur l'utilisateur. Par exemple, vous pouvez configurer une stratégie pour une application définie pour chaque groupe d'administration, puis créer des profils des stratégies pour un ou plusieurs rôles d'utilisateurs de votre entreprise. Dans ce cas, les stratégies et les profils de stratégie s'appliquent selon l'ordre suivant :

1. Les stratégies créées pour la gestion de la sécurité centrée sur l'appareil s'appliquent.
2. Elles sont modifiées par les profils de stratégie selon les priorités du profil de stratégie.
3. Les stratégies sont modifiées par les profils de stratégie associés aux rôles d'utilisateur.

Configuration et diffusion des stratégies : approche centrée sur l'appareil

Cette section présente un scénario d'approche centrée sur l'appareil 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.

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.

Processus

Le scénario de gestion 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 démarrage rapide de l'application, Kaspersky Security Center Cloud Console crée la stratégie par défaut pour Kaspersky Endpoint Security for Windows. Si vous terminez cette procédure de configuration avec l'assistant, vous ne devez pas créer une nouvelle stratégie pour cette application. Continuez vers la configuration manuelle d'une stratégie de Kaspersky Endpoint Security.

   Si votre structure hiérarchique comporte plusieurs groupes d'administration, les groupes d'administration enfants héritent des stratégies du Serveur d'administration principal par défaut. Vous pouvez forcer l'héritage des groupes enfants à interdire 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 restants 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 situés dans une unité ou un groupe de sécurité d'Active Directory défini, avec une configuration matériel particulière ou avec des tags définis. Utilisez les tags pour filtrer les appareils qui répondent aux critères définis. Par exemple, vous pouvez créer un tag *Windows*, l'attribuez à tous les appareils qui tournent sous Windows, puis désignez ce tag comme condition d'activation pour un profil de stratégie. Par conséquent, les applications de Kaspersky installées sur tous les appareils tournant sous Windows seront administrées par leur propre profil de stratégie.

Instructions pour :

- 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**

   Kaspersky Security Center Cloud Console synchronise automatiquement le Serveur d'administration avec les appareils administrés plusieurs fois par heure. 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 Cloud Console 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.

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 démarrage rapide de l'application, Kaspersky Security Center Cloud Console crée la stratégie par défaut pour Kaspersky Endpoint Security. Si vous terminez cette procédure de configuration avec l'assistant, vous ne devez pas créer une nouvelle stratégie pour cette application. Continuez vers la configuration manuelle d'une stratégie de Kaspersky Endpoint Security.

Si votre structure hiérarchique comporte plusieurs groupes d'administration, les groupes d'administration enfants héritent des stratégies du Serveur d'administration principal par défaut. Vous pouvez forcer l'héritage des groupes enfants à interdire 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 restants 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**

Kaspersky Security Center Cloud Console synchronise automatiquement le Serveur d'administration avec les appareils administrés plusieurs fois par heure. 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 Cloud Console indique la date et l'heure de remise dans les propriétés de l'appareil.

Instructions pour : Synchronisation forcée

Résultats

Une fois le scénario centré sur l'utilisateur terminé, les applications de Kaspersky sont configurées selon les paramètres spécifiés et propagés par la hiérarchie des stratégies et les profils de stratégie.

Pour un nouvel utilisateur, il faudra créer un compte, attribuer à l'utilisateur un des rôles d'utilisateurs définis et attribuer les appareils à l'utilisateur. Les stratégies et les profils de stratégie de l'application configurés sont appliqués automatiquement aux appareils de cet utilisateur.

Paramètres de la stratégie de l'Agent d'administration

Pour configurer les paramètres de la stratégie de l'Agent d'administration, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Stratégies et profils**.
2. Cliquez sur le nom de la stratégie de l'Agent d'administration.
   La fenêtre des propriétés de la stratégie de l'Agent d'administration s'ouvre.

Consultez le tableau comparatif détaillant comment les paramètres ci-dessous s'appliquent, en fonction du type de système d'exploitation utilisé.

Onglet Général

Sur cet onglet, vous avez la possibilité de modifier l'état de la stratégie et de configurer l'héritage des paramètres de la stratégie :

- Le groupe **État de la stratégie** permet de sélectionner l'un des modes de stratégie :
  - **Actif**
  - **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.

Onglet Configuration des événements

Cet onglet permet de configurer l'enregistrement des événements dans le journal et les notifications relatives à ces derniers. Les événements sont répartis par niveau d'importance dans les sections suivantes de l'onglet **Configuration des événements** :

- **Erreur de fonctionnement**
- **Avertissement**
- **Information**

Dans chaque section, la liste de types d'événements reprend les types d'événements et la condition de stockage par défaut sur le Serveur d'administration (en jours). Le bouton **Propriétés** permet de définir les paramètres d'enregistrement des événements dans le journal et de notification des événements sélectionnés dans la liste. Par défaut, les paramètres de notification courants spécifiés pour l'ensemble du serveur d'administration servent pour tous les types d'événements. Cependant, vous pouvez modifier des paramètres spécifiques aux types d'événements requis.

Onglet 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 appareils clients reçoivent les mises à jour uniquement via les points de distribution, et non directement sur les serveurs de mises à jour.

  Si cette option est désactivée, les appareils clients peuvent récupérer les mises à jour de différentes sources : directement à partir des serveurs de mises à jour, d'un dossier local ou réseau.

  Cette option est Inactif par défaut.

- **Taille maximale de la file d'attente d'événements (Mo)**

- **&L'application est autorisée à récupérer des données étendues de stratégie sur l'appareil**

  L'Agent d'administration installé sur un appareil administré transfère des informations sur la stratégie d'application de sécurité appliquée à l'application de sécurité (par exemple, Kaspersky Endpoint Security for Windows). Vous pouvez afficher les informations transférées dans l'interface de l'application de sécurité.

  L'Agent d'administration transfère les informations suivantes :

  - Heure de remise de la stratégie à l'appareil administré.
  - Nom de la stratégie active au moment de la remise de la stratégie à l'appareil administré.
  - Nom de la stratégie pour les utilisateurs autonomes au moment de la remise de la stratégie à l'appareil administré (non disponible pour l'Agent d'administration pour Linux).
  - Nom et chemin d'accès complet au groupe d'administration qui contenait l'appareil administré au moment de la remise de la stratégie à l'appareil administré.
  - Liste des profils de stratégie actifs avec leurs noms et priorités au moment de la livraison de la stratégie à l'appareil administré.

  Vous pouvez utiliser les informations pour vous assurer que la bonne stratégie est appliquée à l'appareil et à des fins d'élimination des défaillances. Cette option est Inactif par défaut.

- **Protéger le service de l'Agent &d'administration contre la suppression ou l'arrêt non autorisé et empêcher la modification des paramètres**

  Lorsque cette option est activée, après l'installation de l'Agent d'administration sur un appareil administré, le module ne peut pas être supprimé ou reconfiguré sans les privilèges requis. Il est impossible d'arrêter le service de l'Agent d'administration. Cette option n'a aucun effet sur les contrôleurs de domaine.

  Activez cette option pour protéger l'Agent d'administration sur les postes de travail exploités avec des privilèges d'administrateur local.

  Cette option est Inactif par défaut.

- **Utiliser un mot de passe de désinstallation**

  Si cette option est activée, à l'aide du bouton **Modifier** vous pouvez indiquer le mot de passe pour l'utilitaire klmover et la désinstallation à distance de l'Agent d'administration.

  Notez que l'utilitaire klmover est utilisé uniquement pour déplacer des appareils administrés sous la gestion d'un Serveur d'administration virtuel.

  Cette option est Inactif par défaut.

Stockages

La section **Stockages** permet de sélectionner les types des objets dont les informations seront envoyées sur le Serveur d'administration par l'Agent d'administration. Si la stratégie de l'Agent d'administration bloque la modification ce certains paramètres de cette section, vous ne pouvez pas modifier ceux-ci :

- **Détails sur les applications installées**
- Inclut les informations sur les correctifs

  Les informations sur les correctifs des applications installées sur les appareils clients sont envoyées au Serveur d'administration. L'activation de cette option peut augmenter la charge sur le Serveur d'administration et le SGBD, et causer une augmentation du volume de la base de données.

  Cette option est activée par défaut. Il est disponible uniquement pour Windows.

- Détails sur les mises à jour Windows Update

  Si cette option est activée, les informations sur les mises à jour Microsoft Windows qui doivent être installées sur les appareils clients sont envoyées au Serveur d'administration.

  Parfois, même si l'option est désactivée, les mises à jour sont affichées dans les propriétés de l'appareil dans la section **Mises à jour disponibles**. Cela peut se produire si, par exemple, les appareils de l'organisation présentent des vulnérabilités qui pourraient être corrigées par ces mises à jour.

  Cette option est activée par défaut. Il est disponible uniquement pour Windows.

  Les informations sur les mises à jour facultatives de Microsoft Windows Update ne sont pas envoyées au Serveur d'administration.

- Détails sur les vulnérabilités dans les applications et les mises à jour correspondantes

  Si cette option est activée, les informations sur les vulnérabilités dans les applications tierces (y compris les logiciels Microsoft), détectées sur les appareils administrés, et sur les mises à jour du logiciel destinées à corriger les vulnérabilités dans les applications tierces (à l'exception des logiciels Microsoft) sont envoyées au Serveur d'administration.

  La sélection de cette option (**Détails sur les vulnérabilités dans les applications et les mises à jour correspondantes**) augmente la charge du réseau, la charge du disque du Serveur d'administration et la consommation des ressources de l'Agent d'administration.

  Cette option est activée par défaut. Il est disponible uniquement pour Windows.

  Pour administrer les mises à jour des logiciels Microsoft, utilisez l'option **Détails sur les mises à jour Windows Update**.

- **Informations sur le registre du matériel**

Mises à jour et vulnérabilités du logiciel

La section **Mises à jour et vulnérabilités du logiciel** permet de configurer la recherche des mises à jour Windows et de rechercher les vulnérabilités parmi les fichiers exécutables. Les paramètres dans la section **Mises à jour et vulnérabilités du logiciel** sont disponibles uniquement sur les appareils sous Windows :

- Le groupe de paramètres **Mode de recherche des mises à jour Windows Update** permet de sélectionner le mode de recherche des mises à jour :
  - Actif

Si cette option a été sélectionnée, le Serveur d'administration à l'aide de l'Agent d'administration initie la demande de l'Agent de mises à jour Windows sur l'appareil client à la source des mises à jour : Windows Update Servers or WSUS. Ensuite, l'Agent d'administration transmet sur le Serveur d'administration les informations obtenues en provenance de l'Agent de mises à jour Windows.

L'option ne prend effet que si l'option **Se connecter au serveur de mise à jour pour mettre à jour les données** de la tâche *Recherche de vulnérabilités et de mises à jour requises* est sélectionnée.

Cette option est sélectionnée par défaut.

- **Passif**

  Si cette option a été sélectionnée, l'Agent d'administration transmet périodiquement sur le Serveur d'administration les informations sur les mises à jour obtenues lors de la dernières synchronisation de l'Agent de mises à jour Windows avec la source des mises à jour. Si la synchronisation de l'Agent de mises à jour Windows avec la source des mises à jour n'est pas exécutée, les données sur les mises à jour sur le Serveur d'administration vieillissent.

  Sélectionnez cette option si vous souhaitez obtenir des mises à jour à partir du cache mémoire de la source des mises à jour.

- **Désactivé**

  Si cette option a été sélectionnée, le Serveur d'administration ne formule aucune requête d'informations sur les mises à jour.

  Sélectionnez cette option si, par exemple, vous souhaitez d'abord tester les mises à jour sur votre appareil local.

- **Analyser les fichiers exécutables à la recherche de vulnérabilités lors du lancement**

  Si cette option est activée, lors du lancement des fichiers exécutables, leur analyse sur la présence des vulnérabilités est exécutée.

  Cette option est Inactif par défaut.

Administration du redémarrage

Dans la section **Administration du redémarrage**, vous pouvez définir l'action à exécuter si le système d'exploitation d'un appareil administré doit être redémarré en vue d'une utilisation, d'une installation ou une désinstallation correctes d'une application :

- **Ne pas redémarrer le système d'exploitation**

  Les appareils clients ne redémarrent pas automatiquement après l'opération. Pour arrêter le fonctionnement, il faut redémarrer l'appareil (par exemple, manuellement ou à l'aide d'une tâche d'administration des appareils). Les informations sur la nécessité du redémarrage sont enregistrées dans les résultats de la tâche et dans l'état de l'appareil. Cette option convient aux tâches d' sur les serveurs et autres appareils pour lesquels la continuité des opérations est critique.

- **Redémarrer le système d'exploitation automatiquement si nécessaire**

Dans ce cas, le redémarrage des appareils clients est toujours exécuté automatiquement, si celui-ci est requis pour terminer l'opération. Cette option convient aux tâches d' sur des appareils pour lesquels des interruptions périodiques sont admises (débranchement, redémarrage).

- Confirmer l'action auprès de l'utilisateur

  Le message qui signale que l'appareil client doit être redémarré manuellement s'affiche sur l'écran de l'appareil. Pour cette option, il est possible de configurer des paramètres avancés : le texte du message pour l'utilisateur, la fréquence du message, ainsi que le délai à l'issue duquel le redémarrage sera forcé (sans confirmation de l'utilisateur). Cette option convient le mieux pour les postes de travail sur lesquels les utilisateurs doivent pouvoir sélectionner l'heure de redémarrage qui leur convient le mieux.

  Cette option est sélectionnée par défaut.

  - Fréquence de rappel de la nécessité de réaliser l'installation (min.)

    Quand cette option est activée, l'application invite l'utilisateur à redémarrer le système d'exploitation selon la fréquence indiquée.

    Cette option est activée par défaut. L'intervalle par défaut est de 5 minutes. La valeur peut être comprise entre 1 et 1 440 minutes.

    Si cette option est désactivée, l'invite est affichée une seule fois.

  - Forcer le redémarrage au bout de (min.)

    Après avoir averti l'utilisateur, l'application force le redémarrage du système d'exploitation à l'issue de l'intervalle défini.

    Cette option est activée par défaut. Le délai par défaut est de 30 minutes. La valeur peut être comprise entre 1 et 1 440 minutes.

- Forcer la fermeture des applications dans les sessions bloquées

  Les applications en cours d'exécution peuvent empêcher le redémarrage de l'appareil client. Par exemple, si un document est en train d'être modifié dans un logiciel de traitement de texte et qu'il n'est pas enregistré, l'application n'autorise pas le redémarrage de l'appareil.

  Quand cette option est activée, l'arrêt forcé de ces applications sur un appareil verrouillé doit avoir lieu avant de pouvoir redémarrer l'appareil. Les utilisateurs pourraient perdre toute modification qui n'a pas été enregistrée à ce moment.

  Si cette option est désactivée, un appareil verrouillé n'est pas redémarré. L'état de la tâche sur cet appareil indique qu'il faut redémarrer l'appareil. Les utilisateurs doivent quitter manuellement toutes les applications en cours d'exécution sur les appareils verrouillés, puis redémarrer ces appareils.

  Cette option est Inactif par défaut.

Partage du bureau Windows

La section **Partage du bureau Windows** permet d'activer et de configurer l'audit des actions de l'administrateur sur un appareil distant quand l'accès au bureau est partagé. Les paramètres de la section **Partage du bureau Windows** sont disponibles uniquement sur les appareils sous Windows :

- Activer l'audit

Si cette option est activée, l'audit des actions de l'administrateur sur l'appareil distant est activé. Les enregistrements des actions de l'administrateur sur l'appareil distant sont conservés :

- Dans le journal des événements de l'appareil distant
- Dans un fichier .syslog, situé dans le dossier d'installation de l'Agent d'administration sur l'appareil distant
- Dans la base des événements du Kaspersky Security Center Cloud Console

L'audit des actions de l'administrateur est accessible lorsque les conditions suivantes sont réunies :

- La licence pour le fonctionnement de Gestion des vulnérabilités et des correctifs est en cours d'utilisation
- L'administrateur est autorisé à lancer l'accès partagé au bureau de l'appareil distant

Si cette option est désactivée, l'audit des actions de l'administrateur sur l'appareil distant est désactivé.

Cette option est Inactif par défaut.

- **Masques de fichiers à suivre en cas de lecture**

  La liste contient des masques de fichiers. Lorsque l'audit est activé, l'application suit les fichiers lus par l'administrateur qui correspondent à ces masques et elle enregistre les informations relatives aux fichiers lus. La liste n'est accessible que si la case **Activer l'audit** est cochée. Il est possible de modifier les masques de fichiers et d'en ajouter à la liste. Les nouveaux masques de fichiers doivent être ajoutés sur une nouvelle ligne.

  Par défaut, les masques de fichiers indiqués sont : *.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt et *.pdf.

- **Masques de fichiers à suivre en cas de modification**

  La liste contient les masques des fichiers de l'appareil distant. Lorsque l'audit est activé, l'application suit les fichiers modifiés par l'administrateur qui correspondent à ces masques et elle enregistre les informations relatives aux fichiers modifiés. La liste n'est accessible que si la case **Activer l'audit** est cochée. Il est possible de modifier les masques de fichiers et d'en ajouter à la liste. Les nouveaux masques de fichiers doivent être ajoutés sur une nouvelle ligne.

  Par défaut, les masques de fichiers indiqués sont : *.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt et *.pdf.

Administration des correctifs et des mises à jour

Dans la section **Administration des correctifs et des mises à jour**, vous pouvez configurer la réception et la diffusion des mises à jour et l'installation des correctifs vers les appareils administrés : activer ou désactiver l'option **Installer automatiquement les mises à jour et les correctifs nécessaires pour les modules dont l'état est Non défini**.

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.

- Le groupe de paramètres **Connexion au Serveur d'administration** permet de définir les paramètres suivants :

  - 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 la passerelle de connexion sur le point de distribution (le cas échéant) dans les paramètres de connexion par défaut

    Si l'option est activée, la passerelle de connexion du point de distribution est utilisée avec les paramètres spécifiés par les propriétés du groupe d'administration.

    Cette option est activée par défaut.

- Utiliser un port UDP

  Si vous avez besoin que l'Agent d'administration se connecte au Serveur d'administration via un port UDP, activez l'option **Utiliser le port UDP** et indiquez le **Numéro de port UDP**. Cette option est activée par défaut. Par défaut, la connexion au Serveur d'administration est exécutée via le port UDP 15000.

- Numéro de port UDP

  Champ à saisir le numéro du port UDP. Le numéro de port par défaut est 15000.

  La forme d'écriture décimale est utilisée.

  Si un appareil client fonctionne sous le système d'exploitation Windows XP Service Pack 2, le pare-feu incorporé verrouillera le port UDP 15000. Ce port doit être ouvert à la main.

- Utiliser un point de distribution pour forcer la connexion au Serveur d'administration

  Sélectionnez cette option si vous avez sélectionné l'option **Exécuter le serveur push** dans la fenêtre des paramètres du point de distribution. Sinon, le point de distribution n'agira pas comme un serveur push.

Dans la sous-section **Profils de connexion**, aucun nouvel élément ne peut être ajouté à la liste **Profils de connexion au Serveur d'administration**, donc le bouton **Ajouter** est inactif. Les profils de connexion prédéfinis ne peuvent pas non plus être modifiés.

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**
- **Se connecter aux intervalles indiqués**

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. Les paramètres du sondage sont disponibles uniquement sur les appareils tournant sous Windows. Vous pouvez utiliser les options suivantes pour activer le sondage et définir sa fréquence :

- Réseau Windows

  Si cette option est activée, le point de distribution sonde automatiquement le réseau en respectant la planification configurée en cliquant sur les liens **Planifier le sondage rapide** et **Planifier le sondage complet**.

  Si cette option est désactivée, le Serveur d'administration ne sonde pas le réseau.

  Cette option est activée par défaut.

- Plages IP

  Si cette option est activée, le point de distribution sonde automatiquement les plages IP conformément à la planification configurée en cliquant sur le lien **Planifier le sondage**.

  Si cette option est désactivée, le point de distribution ne sonde pas les plages IP.

  Cette option est Inactif par défaut.

- Contrôleurs de domaine

Si l'option est activée, le point de distribution sonde automatiquement les contrôleurs de domaine selon la planification que vous avez configurée en cliquant sur le bouton **Planifier le sondage**.

Si cette option est désactivée, le point de distribution n'interroge pas les contrôleurs de domaine.

La fréquence de sondage du contrôleur de domaine pour les versions de l'Agent d'administration antérieures à 10.2 peut être configurée dans le champ **Période de sondage (min.)**. Le champ est disponible si l'option est activée.

Cette option est Inactif par défaut.

Paramètres du réseau pour les points de distribution

La section **Paramètres du réseau pour les points de distribution** permet de configurer les paramètres d'accès au réseau Internet :

- **Utiliser un serveur proxy**
- **Adresse**
- **Numéro de port**
- Ne pas utiliser le serveur proxy pour les adresses locales

  Si cette option est activée, le serveur proxy ne sera pas utilisé lors de la connexion aux appareils sur le réseau local.

  Cette option est Inactif par défaut.

- Authentification du serveur proxy

  Si la case est cochée, les champs de saisie permettent d'indiquer les identifiants pour l'authentification sur le serveur proxy.

  Celle-ci est décochée par défaut.

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

Proxy KSN (Points de distribution)

Dans la section **Proxy KSN (Points de distribution)**, vous pouvez configurer l'application afin qu'elle utilise le point de distribution pour transmettre les requêtes 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.

Cette fonctionnalité n'est pas prise en charge par les appareils de point de distribution exécutant Linux ou macOS.

Le point de distribution envoie les statistiques KSN, lesquelles sont répertoriées dans la Déclaration de Kaspersky Security Network, à Kaspersky. Par défaut, la Déclaration KSN se trouve dans %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\ksneula.

Cette option est Inactif par défaut. L'activation de cette option prend effet uniquement si l'option **J'accepte les termes du Kaspersky Security Network** est activée 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.

- **Port**

  Le numéro du port TCP que les appareils administrés utilisent pour se connecter au serveur proxy KSN. Le numéro de port par défaut est 13111.

- **Port UDP**

  Si vous avez besoin que l'Agent d'administration se connecte au Serveur d'administration via un port UDP, activez l'option **Utiliser le port UDP** et indiquez le **Numéro de port UDP**. Cette option est activée par défaut. Par défaut, la connexion au Serveur d'administration est exécutée via le port UDP 15000.

Comparaison des paramètres de stratégie de l'Agent d'administration par système d'exploitation

Le tableau ci-dessous indique les paramètres de stratégie de l'Agent d'administration que vous pouvez utiliser pour configurer l'Agent d'administration avec un système d'exploitation spécifique.

Paramètres de stratégie de l'Agent d'administration : comparaison par système d'exploitation

Section Stratégie	Windows	macOS	Linux
Général	✓	✓	✓
Configuration des événements	✓	✓	✓
Paramètres	✓	✓ À l'exception de la case **Utiliser un mot de passe de désinstallation**.	✓ À l'exception de la case **Utiliser un mot de passe de désinstallation**.
Stockages	✓	✓ La fonctionnalité **Informations sur le registre du matériel** est disponible.	✓ Les fonctionnalités suivantes sont disponibles : • **Détails sur les applications installées** • **Informations sur le registre du matériel**

Mises à jour et vulnérabilités du logiciel	✓	—	—
Administration du redémarrage	✓	—	—
Partage du bureau Windows	✓	—	—
Administration des correctifs et des mises à jour	✓	—	—
Connectivité → Réseau	✓	✓ Sauf la case à cocher **Ouvrir les ports de l'Agent d'administration dans le pare-feu Microsoft Windows**.	✓ Sauf la case à cocher **Ouvrir les ports de l'Agent d'administration dans le pare-feu Microsoft Windows**.
Connectivité → Calendrier de connexion	✓	✓	✓
Sondage du réseau par points de distribution	✓ Les options suivantes sont proposées : • **Réseau Windows** • **Plages IP** • **Contrôleurs de domaine** (Microsoft Active Directory)	—	✓ Les options suivantes sont proposées : • **Plages IP** • **Contrôleurs de domaine** (Microsoft Active Directory, Samba en tant qu'Active Directory)
Paramètres du réseau pour les points de distribution	✓	✓	✓
Proxy KSN (Points de distribution)	✓	—	✓

Configuration manuelle d'une stratégie de Kaspersky Endpoint Security

Cette section fournit des recommandations sur la configuration de la stratégie de Kaspersky Endpoint Security. Vous pouvez effectuer la configuration dans la fenêtre des propriétés de la stratégie. Lorsque vous modifiez un paramètre, cliquez sur l'icône en forme de cadenas à droite du groupe de paramètres concerné pour appliquer les valeurs spécifiées à un poste de travail.

Configuration de Kaspersky Security Network

Kaspersky Security Network (KSN) est l'infrastructure des services cloud qui contient des informations sur la réputation des fichiers, des ressources Internet et des logiciels. Kaspersky Security Network permet à Kaspersky Endpoint Security for Windows de réagir plus rapidement aux différents types de menaces, améliore les performances des modules de protection et réduit le risque de faux positifs. Pour en savoir plus sur Kaspersky Security Network, consultez l'aide de Kaspersky Endpoint Security for Windows.

Vous pouvez configurer le fonctionnement de Kaspersky Security Network dans la fenêtre des propriétés de la stratégie de Kaspersky Endpoint Security for Windows, dans la section **Paramètres de l'application → Protection avancée**.

Pour spécifier les paramètres KSN recommandés :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Stratégies et profils**.
2. Cliquez sur la stratégie de Kaspersky Endpoint Security for Windows.

   La fenêtre des propriétés de la stratégie sélectionnée s'ouvre.
3. Dans les propriétés de la stratégie, accédez à **Paramètres de l'application** → **Protection avancée** → **Kaspersky Security Network**.
4. Assurez-vous que l'option **Utiliser le Serveur d'administration comme serveur proxy KSN** est activée. L'utilisation de cette option aide à rediffuser et optimiser le trafic sur le réseau.

   Si vous utilisez Managed Detection and Response, vous devez activer l'option **Kaspersky Security Network** pour le point de distribution et activer le mode KSN étendu.
5. Activez l'utilisation des serveurs KSN si le service KSN proxy n'est pas disponible. Pour ce faire, activez l'option **Utiliser les serveurs de Kaspersky Security Network si le serveur proxy KSN n'est pas disponible**.

   Les serveurs de KSN peuvent se trouver aussi bien du côté de Kaspersky (utilisation du KSN) ou du côté d'un tiers (utilisation du KPSN).
6. Cliquez sur le bouton **OK**.

Les paramètres KSN recommandés sont spécifiés.

Consultation de la liste des réseaux protégés par le Pare-feu

Assurez-vous que le Pare-feu de Kaspersky Endpoint Security for Windows protège tous vos réseaux. Par défaut, le Pare-feu protège les réseaux avec les types de connexion suivants :

- **Réseau public**. Les applications de sécurité, les pare-feu ou les filtres ne protègent pas les appareils dans un tel réseau.
- **Réseau local**. L'accès aux fichiers et aux imprimantes est limité pour les appareils de ce réseau.
- **Réseau de confiance**. Les appareils d'un tel réseau sont protégés contre les attaques et l'accès non autorisé aux fichiers et aux données.

Si vous avez configuré un réseau personnalisé, assurez-vous que le Pare-feu le protège. Pour ce faire, consultez la liste des réseaux dans les propriétés de la stratégie de Kaspersky Endpoint Security for Windows. Il se peut que certains réseaux ne figurent pas dans la liste.

Pour en savoir plus sur le Pare-feu, consultez l'aide de Kaspersky Endpoint Security for Windows.

Pour vérifier la liste des réseaux, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Stratégies et profils**.
2. Cliquez sur la stratégie de Kaspersky Endpoint Security for Windows.

   La fenêtre des propriétés de la stratégie sélectionnée s'ouvre.

3. Dans les propriétés de la stratégie, accédez à **Paramètres de l'application → Protection principale → Pare-feu**.

4. Sous **Réseaux disponibles**, cliquez sur le lien **Paramètres du réseau**.

   La fenêtre **Connexions réseau** s'ouvre. Cette fenêtre affiche la liste des réseaux.

5. Si la liste contient un réseau manquant, ajoutez-le.

Exclusion des détails du logiciel de la mémoire du Serveur d'administration

Il est recommandé que le Serveur d'administration n'enregistre pas les informations relatives aux modules logiciels lancés sur les appareils du réseau. Par conséquent, la mémoire du Serveur d'administration n'est pas saturée.

Vous pouvez désactiver l'enregistrement de ces informations dans les propriétés de la stratégie de Kaspersky Endpoint Security for Windows.

Pour désactiver l'enregistrement d'informations sur les modules logiciels installés :

1. Dans le menu principal, accédez à **Ressources (Appareils) → Stratégies et profils**.

2. Cliquez sur la stratégie de Kaspersky Endpoint Security for Windows.

   La fenêtre des propriétés de la stratégie sélectionnée s'ouvre.

3. Dans les propriétés de la stratégie, accédez à **Paramètres de l'application → Paramètres généraux → Rapports et stockage**.

4. Sous **Transfert des données au Serveur d'administration**, décochez la case **À propos des applications exécutables** si elle est toujours cochée dans la stratégie de niveau supérieur.

   Quand cette case est cochée, la base de données du Serveur d'administration enregistre les informations relatives à toutes les versions de tous les modules logiciels sur les appareils dans le réseau. Les informations indiquées peuvent prendre un espace considérable dans la base de données de Kaspersky Security Center Cloud Console (des dizaines de gigaoctets).

Les informations sur les modules logiciels installés ne sont plus enregistrées dans la base de données du Serveur d'administration.

Configuration de l'enregistrement d'événements de stratégie importants dans la base de données du Serveur d'administration

Pour éviter le débordement de la base de données du Serveur d'administration, nous vous recommandons d'enregistrer uniquement des événements importants dans la base de données. Pour les événements que vous jugez sans importance, vous pouvez réduire ou désactiver la période de stockage.

Pour configurer les paramètres de stockage des événements, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils) → Stratégies et profils**.

2. Cliquez sur le nom de la stratégie concernée.

   La fenêtre des propriétés de la stratégie sélectionnée s'ouvre.

3. Accédez à l'onglet **Configuration des événements**, puis cliquez sur le nom du type d'événement pour lequel vous souhaitez configurer l'enregistrement dans la base de données.

4. Dans le volet droit qui s'ouvre, réalisez une des opérations suivantes :

   - Si vous souhaitez modifier la période de conservation pour le type d'événement, assurez-vous que le commutateur **Conserver dans la base de données du Serveur d'administration pendant (jours)** est activé, puis saisissez le nombre de jours requis pour la conservation du type d'événement.

   - Si vous ne voulez pas que le type d'événement soit conservé dans la base de données du Serveur d'administration, désactivez le commutateur **Conserver dans la base de données du Serveur d'administration pendant (jours)**.

5. Cliquez sur **OK**, puis après avoir fermé le volet droit, cliquez sur le bouton **Enregistrer**.

La fenêtre des propriétés de la stratégie se ferme et le paramètre que vous avez configuré est appliqué.

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.

Tâches

Cette section décrit les tâches utilisées par Kaspersky Security Center Cloud Console.

À propos des tâches

Kaspersky Security Center Cloud Console gère les applications de protection de Kaspersky installées sur des appareils en créant et en exécutant 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 peuvent être exécutées sur le Sur le Serveur d'administration et sur les appareils.

Les types de tâche suivants sont réalisés sur les appareils :

- *Tâches* exécutées sur un appareil particulier

  Les tâches locales peuvent être modifiées par l'administrateur à l'aide d'outils d'administration ou par l'utilisateur d'un appareil distant (par exemple, via 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.

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

Pour chaque application, vous pouvez créer plusieurs tâches de groupe, plusieurs tâches pour des ensembles d'appareils et plusieurs 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 et dans la base de données du Serveur d'administration.

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

À propos de la zone d'action des tâches

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

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

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

- Désignation manuelle de certains appareils.

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

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

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

- Indiquer une sélection d'appareils.

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

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

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

Création d'une tâche

Vous pouvez créer une tâche dans la liste des tâches. Vous pouvez également sélectionner des appareils dans la liste **Appareils administrés**, puis créer une tâche attribuée aux appareils sélectionnés.

Pour créer une tâche dans la liste des tâches, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Tâches**.
2. Cliquez sur **Ajouter**.

   Ceci permet de lancer l'assistant de création d'une tâche. Suivez-en les instructions.
3. Si vous souhaitez modifier les paramètres de la tâche par défaut, activez l'option **Ouvrir les détails de la tâche à la fin de la création** sur la page **Fin de la création de la tâche**. Si vous n'activez pas cette tâche, la tâche est créée selon les paramètres par défaut. Vous pourrez modifier ces paramètres par défaut plus tard, à tout moment.
4. Cliquez sur le bouton **Terminer**.

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

Pour créer une tâche attribuée aux appareils sélectionnés, procédez comme suit :

Dans le menu principal, accédez à **Ressources (Appareils)** → **Appareils administrés**.

La liste des appareils administrés s'affiche.

1. 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.
2. Cliquez sur le bouton **Lancer la tâche**, puis sélectionnez **Créer 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.
3. Cliquez sur le bouton **Terminer**.

La tâche pour les appareils sélectionnés est créée.

Affichage de la liste des tâches

Vous pouvez afficher la liste des tâches créées dans Kaspersky Security Center Cloud Console.

Pour afficher la liste des tâches,

Dans le menu principal, accédez à **Ressources (Appareils)** → **Tâches**.

La liste des tâches s'affiche. Les tâches sont regroupées par nom d'application auquel elles sont liées. Par exemple, la tâche *Désinstallation à distance d'une application* est liée au Serveur d'administration et la tâche *Recherche de vulnérabilités et de mises à jour requises* se rapporte à l'Agent d'administration.

Pour afficher les propriétés d'une tâche,

Cliquez sur le nom de la tâche.

La fenêtre des propriétés de la tâche s'affiche avec plusieurs onglets nommés. Par exemple, le **Type de tâche** s'affiche sous l'onglet **Général** et la planification des tâches, sous l'onglet **Programmation**.

Lancer une tâche manuellement

L'application démarre les tâches en fonction des paramètres de planification spécifiés dans les propriétés de chaque tâche. Vous pouvez lancer une tâche manuellement à tout moment à partir de la liste des tâches. Vous pouvez également sélectionner des appareils dans la liste **Appareils administrés**, puis démarrer une tâche existante pour eux.

Pour démarrer une tâche manuellement :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Tâches**.
2. Dans la liste des tâches, cochez la case en regard de la tâche que vous souhaitez démarrer.
3. Cliquez sur le bouton **Démarrer**.

La tâche sera lancée. Vous pouvez vérifier l'état de la tâche dans la colonne **État** ou en cliquant sur le bouton **Résultat**.

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.

Pour lancer une tâche pour les appareils sélectionnés :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Appareils administrés**. La liste des appareils administrés s'affiche.

   Utilisez les cases à cocher et sélectionnez les appareils dans la liste pour exécuter la tâche à leur place. Vous pouvez utiliser les fonctions de recherche et de filtrage pour trouver les appareils que vous cherchez.

2. Cliquez sur le bouton **Lancer la tâche**, puis sélectionnez **Appliquer la tâche existante**.

   La liste des tâches existantes s'affiche.

3. 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.

4. 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.

5. 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.

Paramètres et propriétés 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.

- 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

la tâche est affectée à un ensemble d'appareils. Vous pouvez spécifier des appareils de l'une des manières suivantes :

- Spécifiez l'adresse IP, le nom NetBIOS ou le nom DNS de l'appareil.
- Spécifiez la plage IP.

  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.
- Sélectionnez les appareils détectés par le Serveur d'administration, y compris les 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.

- 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.

- 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.

- Paramètres de redémarrage du système d'exploitation :

  - Ne pas redémarrer

    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 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.

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 du calendrier de la tâche :
  - **Paramètre Démarrer la tâche :**
    - **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.

    - **Toutes les N minutes**

      La tâche s'exécute régulièrement, à l'intervalle défini en minutes, à partir de l'heure indiquée le jour de la création de la tâche.

      La tâche s'exécute par défaut toutes les 30 minutes, à partir de l'heure actuelle du système.

    - **Toutes les N heures**

La tâche s'exécute régulièrement, selon l'intervalle défini en heures, à partir de la date et heure définis.

La tâche s'exécute par défaut toutes les six heures à partir de la date et de l'heure actuelles du système.

- **Tous les N jours**

  La tâche s'exécute régulièrement, selon l'intervalle défini en jours. En outre, vous pouvez spécifier la date et l'heure de la première exécution de la tâche. Ces options supplémentaires deviennent disponibles si elles sont prises en charge par l'application pour laquelle vous créez la tâche.

  La tâche s'exécute par défaut chaque jour, à partir de la date et de l'heure actuelle du système.

- **Selon les jours de la semaine**

  La tâche s'exécute régulièrement les jours définis de la semaine, à l'heure indiquée.

  Par défaut, la tâche s'exécute chaque vendredi à 18h00.

- **Chaque mois**

  La tâche s'exécute régulièrement le jour du mois défini, à l'heure indiquée.

  Si le jour en question ne figure pas dans le mois, la tâche s'exécute le dernier jour.

  La tâche s'exécute par défaut le premier jour de chaque mois, à l'heure système actuelle.

- **Mensuellement, les jours indiqués des semaines sélectionnées**

  La tâche s'exécute régulièrement les jours du mois définis, à l'heure indiquée.

  Par défaut, aucun jour du mois n'est sélectionné. L'heure de début par défaut est 18:00.

- **Lors du téléchargement des mises à jour sur les stockages**

  Lorsque de nouvelles mises à jour sont téléchargées dans les stockages des points de distribution, Kaspersky Security Center Cloud Console exécute toutes les tâches qui ont cette planification. L'Agent d'administration vérifie la disponibilité des mises à jour lors de la synchronisation périodique entre l'appareil administré et le Serveur d'administration (le battement de cœur).

  Par exemple, vous pourriez utiliser cette planification pour la tâche de mise à jour liée à une application de sécurité, telle que Kaspersky Endpoint Security.

  Si l'Agent d'administration sur un appareil administré ne détecte aucune nouvelle mise à jour pendant 25 heures ou plus, Kaspersky Security Center Cloud Console exécute sur cet appareil toutes les tâches qui ont cette planification. Ces tâches sont exécutées toutes les heures jusqu'à ce que de nouvelles mises à jour soient détectées. Kaspersky Security Center Cloud Console exécute également ces tâches toutes les heures s'il n'y a pas de connexion entre l'appareil administré et le point de distribution qui télécharge les mises à jour dans le stockage.

- **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. Ce paramètre 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**.

Les paramètres de planification peuvent **dépendre du fuseau horaire local du système d'exploitation de l'appareil**.

Corrélation entre le fuseau horaire local du système d'exploitation de l'appareil et l'heure de début de la tâche

Planification des tâches	L'heure locale est utilisée
Une fois	Non
Toutes les N minutes	Non
Toutes les N heures	Non
Tous les N jours	Oui
Selon les jours de la semaine	Oui
Chaque mois	Oui
Mensuellement, les jours indiqués des semaines sélectionnées	Oui
Lors du téléchargement des mises à jour sur les stockages	Un autre déclencheur pour exécuter la tâche (correspond au nom de la planification)
Lors de la détection d'une propagation de virus	Un autre déclencheur pour exécuter la tâche (correspond au nom de la planification)
À la fin d'une autre tâche	Un autre déclencheur pour exécuter la tâche (correspond au nom de la planification)
Immédiatement	Un autre déclencheur pour exécuter la tâche (correspond au nom de la planification)
Mode manuel	Un autre déclencheur pour exécuter la tâche (correspond au nom de la planification)

- **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.

- 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'arrête automatiquement, qu'elle soit finie ou non.

  Activez cette option si vous souhaitez interrompre (ou arrêter) les tâches dont l'exécution dure trop longtemps.

  Cette option est Inactif par défaut. La durée d'exécution de la tâche par défaut est de 120 minutes.

- Notifications :

  - Groupe **Sauvegarder le résultat** :

    - **Sauvegarder tous les événements**
    - **Sauvegarder les événements relatifs au déroulement des tâches**
    - **Sauvegarder uniquement le résultat de la tâche**
    - 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 Windows de chaque appareil client.

  Cette option est Inactif par défaut.

- **Notifier uniquement les erreurs**
- **Notifier par email**

- Paramètres de la zone d'action de la tâche
- Exclusions de la zone

  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 Cloud Console vous permet d'enregistrer une tâche et ses paramètres dans un fichier KLT. Vous pouvez utiliser ce fichier KLT pour importer la tâche enregistrée dans Kaspersky Security Center Windows et Kaspersky Security Center Linux.

Pour exporter une tâche, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Tâches**.
2. Cochez la case en regard de la tâche que vous souhaitez exporter.

   Vous ne pouvez pas exporter plusieurs tâches à la fois. Si vous sélectionnez plusieurs tâches, le bouton **Exporter** sera désactivé. Les tâches du Serveur d'administration ne sont pas non plus disponibles à l'exportation.
3. Cliquez sur le bouton **Exporter**.
4. Dans la fenêtre ouverte **Enregistrer sous**, indiquez le nom du fichier et le chemin d'accès de la tâche. Cliquez sur **Enregistrer**.

   La fenêtre **Enregistrer sous** s'affiche uniquement si vous utilisez Google Chrome, Microsoft Edge ou Opera. Si vous utilisez un autre navigateur, le fichier de la tâche est automatiquement enregistré dans le dossier **Téléchargements**.

Importation d'une tâche

Kaspersky Security Center Cloud Console vous permet d'importer une tâche à partir d'un fichier KLT. Le fichier KLT contient la tâche exportée et ses paramètres.

Pour importer une tâche, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Tâches**.
2. Cliquez sur le bouton **Importer**.
3. Cliquez sur le bouton **Parcourir** pour choisir un fichier de tâche à importer.
4. Dans la fenêtre qui s'ouvre, indiquez le chemin d'accès au fichier de la tâche KLT, puis cliquez sur le bouton **Ouvrir**. Notez que vous ne pouvez sélectionner qu'un seul fichier de tâche.

   Le traitement de la tâche démarre.
5. Une fois que la tâche a été traitée avec succès, sélectionnez les appareils auxquels vous souhaitez affecter la tâche. Pour ce faire, sélectionnez une des options suivantes :

   - **Attribuer la tâche à un groupe d'administration**

     La tâche est affectée aux appareils qui appartiennent à un groupe d'administration. Vous pouvez renseigner un des groupes existants ou en créer un.

     Par exemple, vous pourriez souhaiter utiliser cette option pour exécuter une tâche d'envoi de messages pour les utilisateurs si le message est particulier pour les appareils repris dans un groupe d'administration spécifique.

     Si une tâche est attribuée à un groupe d'administration, l'onglet **Sécurité** ne s'affiche pas dans la fenêtre des propriétés de la tâche, car les tâches de groupe sont soumises aux paramètres de sécurité des groupes auxquels elles s'appliquent.

   - **Définir les adresses des appareils manuellement ou les importer à partir de la liste**

     Vous pouvez définir les noms NetBIOS, les noms DNS, les adresses IP, ainsi que les plages d'adresses IP auxquels il convient d'affecter la tâche.

     Vous pourriez utiliser cette option pour exécuter une tâche pour un sous-réseau défini. Par exemple, vous pourriez souhaiter installer une certaine application sur les appareils des comptables ou analyser des appareils dans un sous-réseau qui est probablement infecté.

   - **Attribuer la tâche à une sélection d'appareils**

     La tâche est affectée aux appareils qui appartiennent à une sélection d'appareils. Vous pouvez définir une des sélections existantes.

     Par exemple, vous pourriez souhaiter utiliser cette option pour exécuter une tâche sur des appareils dotés d'une version du système d'exploitation spécifique.
6. Spécifiez la zone de la tâche.
7. Cliquez sur le bouton **Terminée** pour terminer l'importation de la tâche.

La notification avec les résultats de l'importation s'affiche. Si la tâche est importée avec succès, vous pouvez cliquer sur le lien **En savoir plus** pour afficher les propriétés de la tâche.

Après une importation réussie, la tâche s'affiche dans la liste des tâches. Les paramètres et la planification de la tâche sont également importés. La tâche sera lancée conformément à sa planification.

Si la tâche importée porte le même nom qu'une tâche existante, le nom de la tâche importée est suivi de l'index **(<numéro de séquence suivant>)**, par exemple : **(1)**, **(2)**.

Affichage de l'historique des tâches entreposé sur le Serveur d'administration

Kaspersky Security Center Cloud Console permet de consulter les résultats d'exécution des tâches de groupe, des tâches pour des ensembles d'appareils et des tâches du Serveur d'administration.

Pour consulter les résultats de l'exécution de la tâche, procédez comme suit :

1. Dans la fenêtre des propriétés de la tâche, sélectionnez la section **Général**.
2. Cliquez sur le lien **Résultats** pour ouvrir la fenêtre **Résultats de la tâche**.

Administration des appareils clients

Kaspersky Security Center Cloud Console permet de gérer les appareils clients :

- Afficher les paramètres et les états des appareils administrés, y compris les clusters et les groupes de serveurs.
- Configurer les points de distribution.
- Gérer les tâches.

Grâce aux groupes d'administration, les appareils clients peuvent former un ensemble administrable comme une seule unité. Un appareil client ne peut être inclus que dans un seul groupe d'administration. Les appareils peuvent être alloués automatiquement à un groupe en fonction des **Conditions de la règle :**

- Création des règles de déplacement des appareils.
- Copie des règles de déplacement des appareils.
- Conditions d'une règle de déplacement de l'appareil.

Vous pouvez utiliser les sélections d'appareils pour filtrer les appareils en fonction d'une condition. Vous pouvez également taguer les appareils pour créer des sélections, rechercher des appareils et répartir les appareils dans les groupes d'administration.

Paramètres de l'appareil administré

Pour voir les paramètres de l'appareil administré :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Appareils administrés**.

   La liste des appareils administrés s'affiche.

2. Cliquez sur le lien avec le nom de l'appareil requis dans la liste des appareils administrés.

La fenêtre des propriétés de l'appareil sélectionné s'affiche.

Les onglets suivants s'affichent dans la partie supérieure de la fenêtre des propriétés et représentent les principaux groupes de paramètres :

- Général

Cet onglet comprend les sections suivantes :

- La section **Général** contient les informations générales sur l'appareil client. La boîte de dialogue affiche des informations mises à jour lors de la dernière synchronisation de l'appareil client avec le Serveur d'administration :

  - Nom

    Champ à consulter et à modifier le nom de l'appareil client dans le groupe d'administration.

  - Description

    Champ de saisie d'une description complémentaire de l'appareil client.

  - État de l'appareil

    État de l'appareil client formé d'après les critères d'état de la protection antivirus et de l'activité réseau de l'appareil, tels que déterminés par l'administrateur.

  - Propriétaire de l'appareil

    Nom du propriétaire de l'appareil. Vous pouvez désigner ou supprimer un utilisateur en tant que propriétaire de l'appareil en cliquant sur le lien **Administrer le propriétaire de l'appareil**.

  - Nom complet du groupe

    Groupe d'administration contenant l'appareil client.

  - Dernière mise à jour des bases antivirus

    Date de la dernière mise à jour des bases de données antivirus ou des applications sur l'appareil.

  - Connexion au Serveur d'administration

    Date et heure de la dernière connexion de l'Agent d'administration installé sur l'appareil client au Serveur d'administration.

  - Heure de la dernière connexion

    Date et heure où l'appareil a été visible sur le réseau pour la dernière fois.

  - Version de l'Agent d'administration

    Version de l'Agent d'administration installé.

  - Date de création

Date de création de l'appareil au sein de Kaspersky Security Center Cloud Console.

- **Maintenir la connexion au Serveur &d'administration**

  Si cette option est activée, la connectivité continue entre l'appareil administré et le Serveur d'administration est conservée. Vous pouvez utiliser cette option si vous n'utilisez pas des serveurs push, qui fournissent une telle connectivité.

  Si cette option est désactivée et les serveurs push ne sont pas utilisés, l'appareil administré se connecte uniquement au Serveur d'administration pour synchroniser les données ou transmettre des informations.

  Le total des appareils pour lesquels l'option **Maintenir la connexion au Serveur &d'administration** a été sélectionnée ne peut être supérieur à 300.

  Cette option est désactivée par défaut sur les appareils administrés. Cette option est activée par défaut sur l'appareil sur lequel le Serveur d'administration est installé et reste activée même si vous essayez de la désactiver.

- **Sessions**

  Cette section contient un tableau avec des informations sur les utilisateurs actuellement connectés à l'appareil. Le tableau affiche les données suivantes dans les colonnes correspondantes :

  - Nom d'utilisateur
  - Nom du compte SAM
  - Nom d'utilisateur principal
  - Adresse email

  Pour afficher correctement les informations sur les sessions des utilisateurs du domaine, vous devez utiliser l'interrogation du contrôleur de domaine.

- La section **Réseau** affiche les informations suivantes sur les propriétés réseau de l'appareil client :

  - **Adresse IP**

    Adresse IP de l'appareil.

  - **Domaine Windows**

    Domaine Windows ou groupe de travail auquel appartient l'appareil.

  - **Nom DNS**

    Nom du domaine DNS de l'appareil client.

  - **Nom NetBIOS**

Nom de l'appareil client sur le réseau Windows.

- **Adresse IPv6**

- La section **Système** reprend les informations relatives au système d'exploitation sur l'appareil client :
  - **Système d'exploitation**
  - **Architecture du processeur**
  - **Fournisseur du système d'exploitation**
  - **Dossier du système d'exploitation**
  - **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.

  - **Version du système d'exploitation**
- La section **Protection** affiche des informations relatives à l'état actuel de la protection antivirus sur l'appareil client :
  - **Visible**

    État de visibilité de l'appareil client.

  - **État de l'appareil**

    État de l'appareil client formé d'après les critères d'état de la protection antivirus et de l'activité réseau de l'appareil, tels que déterminés par l'administrateur.

  - **Description de l'état**

    État de la protection de l'appareil client et de la connexion au Serveur d'administration.

  - **État de la protection**

    État actuel de la protection en temps réel de l'appareil client.

    Quand l'état change sur l'appareil, le nouvel état est affiché dans la fenêtre des propriétés des appareils uniquement après la synchronisation de l'appareil client avec le Serveur d'administration.

- Dernière analyse complète

  Date et heure de la dernière recherche de logiciels malveillants sur l'appareil client.

- Virus détecté

  Nombre total de menaces détectées sur l'appareil client depuis l'installation de l'application de sécurité (première analyse de l'appareil) ou depuis la dernière remise à zéro du compteur.

- Objets dont la désinfection a échoué

  Nombre de fichiers non traités sur l'appareil client.

  Ce champ ne tient pas compte du nombre de fichiers non traités pour les appareils mobiles.

- État de chiffrement des disques

  État actuel de chiffrement des fichiers sur les disques locaux de l'appareil. Pour obtenir une description des états, consultez l'aide de Kaspersky Endpoint Security for Windows.

- La section **État de l'appareil défini par l'application** fournit des informations sur l'état de l'appareil défini par l'application administrée installée sur l'appareil. Cet état de l'appareil peut différer de celui défini par Kaspersky Security Center Cloud Console.

- Applications

  Cet onglet dresse la liste de toutes les applications de Kaspersky installées sur l'appareil client. Cet onglet contient les boutons **Démarrer** et **Arrêter** qui permettent de lancer et d'arrêter l'application Kaspersky sélectionnée (à l'exception de l'Agent d'administration). Vous pouvez utiliser ces boutons si le port 15000 UDP est disponible sur l'appareil géré pour recevoir des notifications push du Serveur d'administration. Si l'appareil géré ne peut pas recevoir de notifications push, mais que le mode de connexion permanente au Serveur d'administration est activé (l'option **Maintenir la connexion au Serveur &d'administration** est activée dans la section **Général**), les boutons **Démarrer** et **Arrêter** sont également disponibles. Dans le cas contraire, lorsque vous essayez de démarrer ou d'arrêter l'application, un message d'erreur s'affiche. Vous pouvez également cliquer sur le nom de l'application pour afficher des informations générales sur l'application, une liste des événements qui se sont produits sur l'appareil et les paramètres de l'application.

- Stratégies actives et profils de stratégies

  Cet onglet répertorie les stratégies et les profils de stratégie actuellement attribués à l'appareil administré.

- Tâches

L'onglet **Tâches** permet d'administrer les tâches de l'appareil client : consulter la liste des tâches existantes, créer des tâches, supprimer, lancer ou suspendre des tâches, modifier leurs paramètres et consulter les résultats de l'exécution. La liste des tâches est fournie sur la base des données réceptionnées pendant la dernière session de synchronisation client avec le serveur d'administration. Le Serveur d'administration questionne l'appareil client au sujet de l'état courant de tâche. Si le port 15000 UDP est disponible sur l'appareil administré pour recevoir les notifications push en provenance du Serveur d'administration, l'état de la tâche est affiché et les boutons d'administration de la tâche sont activés. Si l'appareil géré ne peut pas recevoir de notifications push, mais que le mode de connexion permanente au Serveur d'administration est activé (l'option **Maintenir la connexion au Serveur &d'administration** est activée dans la section **Général**), les actions avec les tâches sont également disponibles.

Si la connexion n'est pas établie, l'état n'est pas affiché et les boutons sont désactivés.

- Événements

  L'onglet **Événements** affiche les événements enregistrés sur le Serveur d'administration pour l'appareil client sélectionné.

- Problèmes de sécurité

  L'onglet **Problèmes de sécurité** permet de consulter, de modifier et de créer des problèmes de sécurité pour l'appareil client. Les problèmes de sécurité peuvent être créés automatiquement, à l'aide des applications administrées de Kaspersky installées sur l'appareil client, ou manuellement par l'administrateur. Ainsi, si un utilisateur transfère toujours des applications malveillantes de son disque amovible personnel vers d'autres appareils, l'administrateur peut créer un problème de sécurité. L'administrateur peut fournir une brève description du cas et recommandés des actions, (comme des mesures disciplinaires à adopter contre un utilisateur) dans le texte du problème de sécurité et il peut ajouter un lien vers le ou les utilisateurs.

  Un problème de sécurité pour lequel les actions nécessaires ont été exécutées est un problème *traité*. La présence de problèmes de sécurité non traités peut être sélectionnée comme condition pour faire passer l'état de l'appareil à *Critique* ou *Avertissement*.

  La section contient la liste des problèmes de sécurité créés pour l'appareil. Les problèmes de sécurité sont classés par niveau de gravité et par type. C'est l'application Kaspersky qui crée le problème de sécurité qui en définit le type. Les problèmes de sécurité traités peuvent être identifiés dans la liste en cochant la case de la colonne **Traité**.

- Tags

  L'onglet **Tags** permet d'administrer la liste des mots-clés utilisés pour effectuer la recherche d'appareils clients : consulter la liste des tags existants, désigner les tags de la liste, configurer des règles de désignation automatique des tags, ajouter de nouveaux tags, renommer d'anciens tags et supprimer des tags.

- Avancé

Cet onglet comprend les sections suivantes :

- **Registre des applications**. Cette section permet de consulter le registre des applications installées sur l'appareil client, ainsi que leurs mises à jour, et de configurer l'affichage du registre des applications.

  Les informations relatives aux applications installées sont présentées si l'Agent d'administration installé sur l'appareil client transmet les informations nécessaires au Serveur d'administration. Les paramètres de transfert des informations sur le Serveur d'administration peuvent être configurés dans la fenêtre des propriétés de l'Agent d'administration ou de sa stratégie, dans la section **Stockages**.

  Cliquez sur le nom d'une application pour ouvrir une fenêtre contenant les détails de l'application ainsi qu'une liste des paquets de mise à jour installés pour l'application.

- **Fichiers exécutables**. Cette section affiche les fichiers exécutables trouvés sur la machine cliente.

- **Points de distribution**. Cette section présente la liste des points de distribution avec lesquels l'appareil interagit.

  - Exporter dans un fichier

    Le bouton **Exporter dans un fichier** vous permet d'enregistrer dans le fichier la liste des points de distribution avec lesquels l'appareil interagit. Par défaut, l'application exporte la liste des appareils dans un fichier au format CSV.

  - Propriétés

    Le bouton **Propriétés** vous permet de consulter et de configurer les paramètres du point de distribution avec lequel l'appareil interagit.

- **Registre du matériel**. Cette section permet de consulter les informations sur le matériel installé sur l'appareil client.

  Si l'Agent d'administration est installé sur un appareil exécutant Windows, il envoie au Serveur d'administration les informations suivantes sur le matériel de l'appareil :

  - Mémoire vive
  - Appareils de stockage de masse
  - Carte mère
  - Processeur
  - Adaptateurs réseau
  - Surveillance
  - Adaptateur vidéo
  - Carte son

  Si l'Agent d'administration est installé sur un appareil exécutant Linux ou macOS, il envoie au Serveur d'administration les informations suivantes sur le matériel de l'appareil, si ces informations sont fournies par le système d'exploitation :

- Volume total de mémoire vive
- Volume total des appareils de stockage de masse
- Carte mère
- Processeur
- Adaptateurs réseau

- **Mises à jour 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 :

    - Ignorez la vulnérabilité dans l'application sur cet appareil administré (dans la Console d'administration ou Kaspersky Security Center Cloud Console).
    - Afficher la liste des correctifs recommandés pour la vulnérabilité.
    - Spécifiez manuellement les mises à jour du logiciel pour corriger la vulnérabilité (dans la Console d'administration ou dans Kaspersky Security Center Cloud 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.

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 Cloud Console 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 Cloud Console vous permet d'afficher la liste des appareils à partir d'une sélection d'appareils.

Pour consulter la liste des appareils à partir de la sélection d'appareils, procédez comme suit :

1. Dans le menu principal, accédez à la section **Ressources (Appareils)** → **Sélections d'appareils** ou **Découverte et déploiement** → **Sélections d'appareils**.

2. Dans la liste de sélection, cliquez sur le nom de la sélection d'appareils.

   La page affiche un tableau avec des informations sur les appareils inclus dans la sélection d'appareils.

3. Vous pouvez regrouper et filtrer les données du tableau des appareils comme suit :

   - Cliquez sur l'icône des paramètres (⚙), puis sélectionnez les colonnes à afficher dans le tableau.
   - Cliquez sur l'icône du filtre (▽), puis spécifiez et appliquez le critère de filtre dans le menu appelé.

     Le tableau filtré des appareils s'affiche.

Vous pouvez sélectionner un ou plusieurs appareils dans la sélection d'appareils et cliquer sur le bouton **Nouvelle tâche** pour créer une tâche qui sera appliquée à ces appareils.

Pour déplacer les appareils sélectionnés de la sélection d'appareils vers un autre groupe d'administration, cliquez sur le bouton **Déplacer vers le groupe**, puis sélectionnez le groupe d'administration cible.

Création d'une sélection d'appareils

Pour créer une sélection d'appareils, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Sélections d'appareils**.

   Une page comportant une liste de sélections d'appareils s'affiche.

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

La fenêtre **Paramètres de sélection d'appareils** s'ouvre.

3. Saisissez le nom de la nouvelle sélection.
4. Indiquez le groupe qui contient les appareils à inclure dans la sélection d'appareils :

   - **Rechercher tous les appareils** : recherche d'appareils qui répondent aux critères de sélection et qui sont inclus dans le groupe **Appareils administrés** ou **Appareils non définis**.
   - **Rechercher les appareils administrés** : recherche d'appareils qui répondent aux critères de sélection et qui sont inclus dans le groupe **Appareils administrés**.
   - **Rechercher les appareils non définis** : recherche d'appareils qui répondent aux critères de sélection et qui sont inclus dans le groupe **Appareils non définis**.

   Vous pouvez cocher la case **Inclure les données des Serveurs d'administration secondaires** pour activer la recherche d'appareils qui répondent aux critères de sélection et qui sont administrés par les Serveurs d'administration secondaires.
5. Cliquez sur le bouton **Ajouter**.
6. Dans la fenêtre qui s'ouvre, spécifiez les conditions à remplir pour inclure les appareils dans cette sélection, puis cliquez sur le bouton **OK**.
7. Cliquez sur le bouton **Enregistrer**.

La sélection d'appareils est créée et ajoutée à la liste des sélections d'appareils.

Configuration d'une sélection d'appareils

Pour configurer la sélection d'appareils, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Sélections d'appareils**.

   Une page comportant une liste de sélections d'appareils s'affiche.
2. Sélectionnez la sélection d'appareils définie par l'utilisateur pertinente, puis cliquez sur le bouton **Propriétés**.

   La fenêtre **Paramètres de sélection d'appareils** s'ouvre.
3. Sous l'onglet **Général**, cliquez sur le lien **Nouvelle condition**.
4. Définissez les conditions à remplir pour inclure les appareils dans cette sélection.
5. Cliquez sur le bouton **Enregistrer**.

Les paramètres sont appliqués et enregistrés.

Les paramètres des conditions d'ajout des appareils à une sélection sont décrits ci-dessous. Les conditions sont combinées à l'aide de l'opérateur logique " ou " : la sélection reprend les appareils qui répondent au moins à une des conditions présentées.

Général

La section **Général** permet de modifier le nom de la condition de la sélection et d'indiquer si cette condition doit être intervertie :

Inverser la condition de sélection

Si l'option est activée, la condition de sélection définie sera inversée. Tous les appareils qui ne correspondent pas à la condition feront partie de la sélection.

Cette option est Inactif par défaut.

Infrastructure réseau

La sous-section **Réseau** permet de configurer les critères d'inclusion des appareils dans une sélection sur la base de leurs données de réseau.

- Nom de l'appareil

  Nom de réseau Windows (nom NetBIOS) de l'appareil ou adresse IPv4 ou IPv6.

- Domaine

  Les appareils faisant partie du domaine Windows indiqué seront affichés.

- Groupe d'administration

  Les appareils faisant partie du groupe d'administration seront affichés.

- Description

Texte apparaissant dans la fenêtre des propriétés de l'appareil : dans le champ **Description** de la section **Général**.

Pour décrire le texte dans le champ **Description**, vous pouvez utiliser les caractères suivants :

- A l'intérieur d'un seul mot :
  - *****. Remplace n'importe quelle ligne quel que soit le nombre de caractères.

    Exemple :

    Pour décrire les mots **Serveur**, **Serveurs** ou de serveur, il est possible d'utiliser la ligne **Serveur***.
  - **?.** Remplace un n'importe quel caractère.

    Exemple :

    Pour décrire les mots **Fenêtre** ou **Fenêtres**, il est possible d'utiliser la ligne **Fenêtr?**.

    Caractère ***** ou **?** ne peut pas être utilisé en tant que premier caractère dans la description du texte.
- Pour lier plusieurs mots :
  - Espace. Affiche l'ensemble des appareils dont la description contient l'un des mots de la liste.

    Exemple :

    Pour décrire la phrase contenant le mot **Secondaire** ou **Virtuel**, il est possible d'utiliser la ligne **Secondaire Virtuel**.
  - **+**. Avant le mot signifie la présence obligatoire du mot dans le texte.

    Exemple :

    Pour décrire la phrase contenant le mot **Secondaire**, et le mot **Virtuel**, il est possible de saisir la demande **+Secondaire+Virtuel**.
  - **-**. Avant le mot signifie l'absence obligatoire du mot dans le texte.

    Exemple :

    Pour décrire la phrase avec le mot **Secondaire** et sans le mot **Virtuel**, il est possible de saisir la demande **+Secondaire-Virtuel**.
  - **"<le texte>"**. Le fragment du texte entre guillemets doit être entièrement présent dans le texte.

    Exemple :

    Pour décrire la phrase contenant le groupe de mots **Serveur secondaire**, il est possible de saisir la demande **"Serveur secondaire"**.

- Plage IP

  Si l'option est activée, vous pouvez saisir les adresses IP de début et de fin de la plage IP à laquelle les appareils concernés doivent appartenir.

  Cette option est Inactif par défaut.

- Administrés par un autre Serveur d'administration

Sélectionnez l'une des valeurs ci-dessous :

- **Oui**. Une règle de déplacement des appareils s'applique uniquement aux appareils clients administrés par d'autres Serveurs d'administration. Ces Serveurs sont différents du Serveur sur lequel vous configurez la règle de déplacement des appareils.
- **Non**. La règle de déplacement des appareils s'applique uniquement aux appareils clients administrés par le Serveur d'administration actuel.
- **La valeur n'est pas sélectionnée**. La condition ne s'applique pas.

La sous-section **Active Directory** permet de configurer les critères d'inclusion d'appareils dans une sélection sur la base de leurs données Active Directory :

- L'appareil se trouve dans une unité &organisationnelle Active Directory

  Si l'option est activée, la sélection inclura les appareils de l'unité d'organisation Active Directory indiquée dans le champ de saisie.

  Cette option est Inactif par défaut.

- Inclure les organisations enfants

  Si l'option est activée, la sélection inclut les appareils appartenant aux unités organisationnelles enfants de l'unité organisationnelle Active Directory.

  Cette option est Inactif par défaut.

- L'appareil est un membre du &groupe Active Directory

  Si l'option est activée, la sélection inclut les appareils issus du groupe Active Directory indiqué dans le champ de saisie.

  Cette option est Inactif par défaut.

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.

La sous-section **Segments dans le Cloud** permet de configurer les critères d'inclusion des appareils dans une sélection sur la base de leur appartenance aux segments dans le Cloud :

- **L'appareil se trouve dans le segment dans le Cloud**

  Si cette option est activée, vous pouvez choisir des appareils dans les segments dans le cloud AWS, Azure et Google.

  Si l'option **Objets enfants inclus** est également activée, la recherche est exécutée sur l'ensemble des objets enfants du segment sélectionné.

  Seuls les appareils du segment choisi figurent dans les résultats de la recherche.

- **L'appareil est détecté via l'utilisation de l'API**

  La liste déroulante permet de choisir si vous pouvez détecter un appareil à l'aide des outils de l'API :

  - **Oui**. L'appareil est détecté à l'aide de l'API AWS, Azure ou Google.
  - **Non**. L'appareil ne peut pas être détecté à l'aide de l'API AWS, Azure ou Google. C'est-à-dire que l'appareil se trouve soit en dehors de l'environnement cloud, soit dans l'environnement cloud, mais il ne peut pas être détecté à l'aide d'une API.
  - Pas de valeur. Cette condition ne s'applique pas.

États 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 **Système d'exploitation** permet de configurer les critères d'inclusion d'appareils dans une sélection en fonction du type de système d'exploitation installé.

- **Type de plateforme**

  Si la case est cochée, la liste permet de sélectionner les systèmes d'exploitation. Les appareils avec les systèmes d'exploitation indiqués installés sont inclus dans les résultats de recherche.

- **Version du paquet de mise à jour 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.

- Capacité du système d'exploitation

  Dans la liste déroulante, vous pouvez sélectionner l'architecture du système d'exploitation qui détermine la manière dont la règle de déplacement est appliquée à l'appareil (**Inconnu**, **x86**, **AMD64** ou **IA64**). Par défaut, aucune option n'est sélectionnée dans la liste, l'architecture du système d'exploitation n'est pas définie.

- Version du système d'exploitation

  Ce paramètre concerne uniquement les systèmes d'exploitation Windows.

  Le numéro de version du système d'exploitation. Vous pouvez indiquer si le système d'exploitation sélectionné doit avoir un numéro de version égal, antérieur ou supérieur. Vous pouvez également configurer la recherche de tous les numéros de version à l'exception du numéro indiqué.

- Numéro de version du système d'exploitation

  Ce paramètre concerne uniquement les systèmes d'exploitation Windows.

  L'identifiant de version du système d'exploitation. Vous pouvez indiquer si le système d'exploitation sélectionné doit avoir un ID de version égal, antérieur ou supérieur. Vous pouvez également configurer la recherche de tous les ID de version à l'exception du numéro indiqué.

La section **Machines virtuelles** permet de configurer les critères d'inclusion des appareils dans une sélection selon qu'il s'agit de machines virtuelles ou d'appareils inclus dans une infrastructure de type Virtual Desktop Infrastructure (VDI) :

- Est une machine virtuelle

  La liste déroulante permet de sélectionner les éléments suivants :

  - **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

  Nom de l'appareil dans le réseau Windows. L'appareil portant le nom indiqué est repris dans la sélection.

- Description

  Description de l'appareil ou du matériel. Les appareils dont la description figure dans le champ seront inclus dans la sélection.

  La description de l'appareil peut être librement saisie dans la fenêtre des propriétés. Le champ prend en charge la recherche en texte intégral.

- Fabricant 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 mémoire vive de l'appareil. Les appareils dont la mémoire vive correspond à la plage de tailles indiquée dans les champs de saisie (incluse) seront inclus dans la sélection.

- Taille de la mémoire vive, en Mo, à

  La taille maximale de la mémoire vive de l'appareil. Les appareils dont la mémoire vive correspond à la plage de tailles indiquée dans les champs de saisie (incluse) seront inclus dans la sélection.

Détails 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

  La liste déroulante qui permet de sélectionner l'état de l'application (*Installé*, *Non installé*). Les appareils sur lesquels l'application indiquée est installée ou non sont inclus dans la sélection en fonction de l'état sélectionné.

Champ de saisie qui permet de saisir les critères d'inclusion des appareils dans la sélection lors de la recherche du paquet de mise à jour installé pour l'application par nom ou numéro.

Si le champ n'est pas rempli, les critères ne sont pas appliqués.

- **Sélectionnez la période de la dernière mise à jour des modules**

  Cette option permet de définir les critères de recherche d'appareils selon l'heure de la dernière mise à jour des modules des applications installées sur les appareils.

  Si la case est cochée, le champ de saisie permet d'indiquer les valeurs de l'intervalle de temps (date et heure), durant lequel la dernière mise à jour des modules des applications installées sur les appareils a été effectuée.

  Si la case est décochée, le critère ne sera pas appliqué.

  Celle-ci est décochée par défaut.

- **L'appareil est administré via le Serveur d'administration**

  Dans la liste déroulante, vous pouvez inclure dans la sélection les appareils administrés via Kaspersky Security Center Cloud Console :

  - **Oui**. L'application inclut dans la sélection les appareils administrés via Kaspersky Security Center Cloud Console.
  - **Non**. L'application inclut les appareils dans la sélection s'ils ne sont pas administrés via Kaspersky Security Center Cloud Console.
  - **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**

  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*.

  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 **Modules de l'application** contient la liste des modules des applications pour lesquelles les plug-ins d'administration correspondants sont installés dans Kaspersky Security Center Cloud Console.

La sous-section **Modules de l'application** permet de définir les critères d'inclusion des appareils dans une sélection sur la base des états et des numéros de version des modules faisant référence à l'application que vous avez sélectionnée :

- **État**

Recherchez les appareils selon les états des modules renvoyés par une application au Serveur d'administration. Vous pouvez sélectionner l'un des états suivants : *N/A*, *Arrêté*, *En pause*, *Lancement*, *En cours d'exécution*, *Échec*, *Non installé*, *Non pris en charge par la licence*. Si le module sélectionné de l'application installée sur un appareil administré possède l'état indiqué, l'appareil est repris dans la sélection d'appareils.

États envoyés par les applications :

- *Arrêté* : le module est désactivé et ne fonctionne pas pour l'instant.
- *Suspendu* : le module est suspendu, par exemple, après que l'utilisateur a suspendu la protection dans l'application administrée.
- *En cours de démarrage* : l'initialisation du module est actuellement en cours.
- *En cours d'exécution* : le module est activé et fonctionne correctement.
- *Échec* : une erreur s'est produite lors de l'opération du module.
- *Non installé* : l'utilisateur n'a pas sélectionné le module en vue de l'installer lors de la configuration de l'installation personnalisée de l'application.
- *Non pris en charge par la licence* : la licence ne couvre pas le module sélectionné.

À la différence des autres états, l'état *N/A* n'est pas envoyé par les applications. Cette option indique que les applications n'ont aucune information sur l'état du module sélectionné. Cela peut se produire, par exemple, quand le module sélectionné n'appartient à aucune des applications installées sur l'appareil ou quand l'appareil est éteint.

- **Version**

  Recherchez les appareils en fonction du numéro de version du module que vous avez sélectionné dans la liste. Vous pouvez taper un numéro de version, par exemple `3.4.1.0`, puis indiquez si le numéro de version du module sélectionné doit être égal, antérieur ou postérieur. Vous pouvez également configurer la recherche de toutes les versions à l'exception du numéro indiqué.

Tags

La section **Tags** permet de configurer les critères d'inclusion des appareils dans une sélection sur la base des mots clés (tags) ajoutés au préalable aux descriptions des appareils administrés :

Appliquer si au moins un tag sélectionné coïncide

Si l'option est activée, les appareils dont la description contient au moins l'un des tags sélectionnés figureront dans les résultats de la recherche.

Si l'option est désactivée, seuls les appareils dont la description contient l'ensemble des tags sélectionnés figureront dans les résultats de la recherche.

Cette option est Inactif par défaut.

Pour ajouter des tags au critère, cliquez sur le bouton **Ajouter** et sélectionnez les tags en cliquant dans le champ de saisie **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 utilisateur pour configurer le critère. Notez que la liste des utilisateurs est filtrée et affiche les utilisateurs internes. 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 cette option est activée, vous pouvez sélectionner le compte utilisateur pour configurer le critère. Notez que la liste des utilisateurs est filtrée et affiche les utilisateurs internes. Les résultats de la recherche incluent les appareils sur lesquels l'utilisateur indiqué a déjà accédé au système.

Exportation de la liste des appareils à partir d'une sélection d'appareils

Kaspersky Security Center Cloud Console 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**.

Cliquez sur le bouton **Exporter vers un fichier CSV** ou **Exporter vers un fichier TXT**. Toutes les informations sur les appareils sélectionnés inclus dans le tableau seront exportées.

Notez que si vous avez appliqué un critère de filtre à la table des appareils, seules les données filtrées des colonnes affichées seront exportées.

Suppression des appareils depuis les groupes d'administration dans la sélection

Lors de l'utilisation de la sélection d'appareils, vous pouvez supprimer les appareils des groupes d'administration directement dans la sélection sans avoir à supprimer les appareils des groupes d'administration.

Pour supprimer les appareils depuis les groupes d'administration, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Sélections d'appareils** ou **Découverte et déploiement** → **Sélections d'appareils**.
2. Dans la liste de sélection, cliquez sur le nom de la sélection d'appareils.

   La page affiche un tableau avec des informations sur les appareils inclus dans la sélection d'appareils.
3. Sélectionnez les appareils que vous souhaitez supprimer, puis cliquez sur **Supprimer ;**.

   Finalement, les appareils sélectionnés seront supprimés depuis les groupes d'administration dont ils faisaient partie.

Consultation et configuration des actions quand les appareils sont inactifs

Si les appareils client au sein d'un groupe sont inactifs, vous pouvez recevoir des notifications à ce sujet. Vous pouvez également supprimer automatiquement ces appareils.

Pour voir ou configurer les actions lorsque les appareils du groupe sont inactifs :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Hiérarchie des groupes**.
2. Cliquez sur le nom du groupe d'administration concerné.

   La fenêtre des propriétés du groupe d'administration s'ouvre.
3. Dans la fenêtre des propriétés, allez à l'onglet **Paramètres**.
4. Dans la section **Héritage**, activez ou désactivez les options suivantes :

   - Hériter du groupe parent

Les paramètres de cette section sont hérités du groupe parent auquel appartient l'appareil client. Quand cette option est activée, les paramètres du groupe **Activité des appareils sur le réseau** sont verrouillés et ne peuvent être modifiés.

Cette option est disponible uniquement si le groupe d'administration possède un groupe parent.

Cette option est activée par défaut.

- Imposer l'héritage des paramètres aux groupes enfants

  Les valeurs des paramètres sont diffusées dans les groupes enfants mais ces paramètres sont verrouillés dans les propriétés des groupes enfants.

  Cette option est Inactif par défaut.

5. Dans la section **Activité des appareils**, activez ou désactivez les options suivantes :

   - Informer l'administrateur si l'appareil n'est pas actif pendant plus de (jours)

     Quand cette option est activée, l'administrateur reçoit des notifications sur les appareils inactifs. Vous pouvez définir la période à l'issue de laquelle l'événement **L'appareil est resté inactif sur le réseau depuis longtemps** est créé. Par défaut, la valeur de cet intervalle est de 7 jours.

     Cette option est activée par défaut.

   - Supprimer l'appareil du groupe après une inactivité de plus de (jours)

     Quand cette option est activée, vous pouvez définir la période à l'issue de laquelle un appareil est supprimé automatiquement du groupe. Par défaut, la valeur de cet intervalle est de 60 jours.

     Cette option est activée par défaut.

6. Cliquez sur **Enregistrer**.

Vos modifications sont enregistrées et appliquées.

À propos des états des appareils

Kaspersky Security Center Cloud Console attribue un état à chaque appareil administré. Chaque état dépend du respect des conditions définies par l'utilisateur. Dans certains cas, lors de l'attribution d'un état à un appareil, Kaspersky Security Center Cloud Console prend en compte l'indicateur de visibilité de l'appareil sur le réseau (voir le tableau ci-dessous). Si Kaspersky Security Center Cloud Console 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 de recherche de virus, et le nombre de virus détectés dépasse la valeur spécifiée.	Plus de 0.
Le niveau de la Protection en temps réel diffère de celui défini par l'Administrateur	L'appareil est visible sur le réseau, mais le niveau de protection en temps réel est différent de celui défini par l'administrateur (dans la condition) pour l'état de l'appareil.	• Arrêté. • Suspendu(e). • En cours.
La recherche d'applications malveillantes n'a pas été exécutée depuis longtemps	L'appareil est visible sur le réseau et une application de sécurité est installée sur l'appareil, mais ni la tâche d'*Analyse des logiciels malveillants* ni une tâche d'analyse locale n'ont été exécutées dans l'intervalle de temps spécifié. La condition s'applique uniquement aux appareils qui ont été ajoutés à la base de données du Serveur d'administration il y a 7 jours ou avant.	Plus de 1 jour.
Les bases sont dépassées	L'appareil est visible sur le réseau, et une application de sécurité est installée sur l'appareil, mais les bases antivirus n'ont pas été mises à jour sur cet appareil dans la période indiquée. La condition s'applique uniquement aux appareils qui ont été ajoutés à la base de données du Serveur d'administration il y a 1 jour ou avant.	Plus de 1 jour.
Ne s'est pas connecté depuis longtemps	L'Agent d'administration est installé sur l'appareil, mais l'appareil ne s'est pas connecté au Serveur d'administration dans la période indiquée car l'appareil était désactivé.	Plus de 1 jour.
Des menaces actives sont détectées	La quantité d'objets non traités dans le dossier **Menaces actives** dépasse la valeur indiquée.	Plus de 0 pièce.
Redémarrage requis	L'appareil est visible sur le réseau, mais une application nécessite le redémarrage de l'appareil depuis la durée indiquée et pour l'une des raisons sélectionnées.	Plus de 0 minute.
Des applications incompatibles sont installées	L'appareil est visible sur le réseau, mais l'inventaire des applications effectué par l'Agent d'administration a détecté des applications incompatibles installées sur l'appareil.	• Le bouton radio est éteint. • Le bouton radio est allumé.
Vulnérabilités dans les applications	L'appareil est visible sur le réseau, et l'Agent d'administration est installé sur l'appareil, mais la tâche *Recherche de vulnérabilités et de mises à jour requises* a détecté des vulnérabilités avec le niveau de gravité indiqué dans les applications installées sur l'appareil.	• Critique. • Élevé. • Normal. • Ignorer s'il est impossible de fermer la vulnérabilité. • Ignorer si la mise à jour a été désignée à l'installation.
La licence a expiré	L'appareil est visible sur le réseau, mais la licence a expiré.	• Le bouton radio est éteint. • Le bouton radio est allumé.

La licence expire bientôt	L'appareil est visible sur le réseau, mais la licence expirera sur l'appareil dans moins de jours que le nombre indiqué.	Plus de 0 jour.
La vérification de mises à jour Windows Update n'a pas eu lieu depuis longtemps	L'appareil est visible sur le réseau, mais la tâche Synchronisation des mises à jour Windows Update n'a plus été exécutée dans la période indiquée.	Plus de 1 jour.
État de chiffrement non valide	L'Agent d'administration est installé sur l'appareil mais le résultat du chiffrement de l'appareil est égal à la valeur indiquée.	• Ne correspond pas à la stratégie à cause du refus de l'utilisateur (uniquement pour les appareils externes). • Ne correspond pas à la stratégie à cause de l'erreur. • Stratégie en cours d'application – le redémarrage est requis. • La stratégie de chiffrement n'est pas définie. • Non pris en charge. • Stratégie en cours d'application.
Les paramètres de l'appareil mobile ne correspondent pas à la stratégie	Les paramètres de l'appareil mobile se distinguent des paramètres définis dans la stratégie Kaspersky Endpoint Security for Android lors de l'analyse des règles de concordance.	• Le bouton radio est éteint. • Le bouton radio est allumé.
Problèmes de sécurité non traités détectés	Certains problèmes de sécurité non traités ont été détectés sur l'appareil. Les problèmes de sécurité peuvent être créés automatiquement, à l'aide des applications administrées de Kaspersky installées sur l'appareil client, ou manuellement par l'administrateur.	• Le bouton radio est éteint. • Le bouton radio est allumé.
État de l'appareil défini par l'application	L'état de l'appareil est défini par l'application administrée.	• Le bouton radio est éteint. • Le bouton radio est allumé.
Espace disque épuisé sur l'appareil	L'espace disque disponible est inférieur à la valeur indiquée ou l'appareil n'a pas pu être synchronisé avec le Serveur d'administration. L'état *Critique* ou *Avertissement* 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 Cloud Console 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*.

Lorsque Kaspersky Security Center Cloud Console attribue un statut à un appareil, pour certaines conditions (voir la colonne Description de la condition), l'indicateur de visibilité est pris en considération. Par exemple, si un appareil administré a reçu l'état *Critique* parce que la condition Les bases sont dépassées a été remplie, et qu'ensuite l'indicateur de visibilité a été placé pour l'appareil, alors l'appareil reçoit l'état *OK*.

Configuration de la permutation des états des appareils

Vous pouvez modifier les conditions pour attribuer le statut *Critique* ou *Avertissement* à un appareil.

Pour activer le changement d'état de l'appareil sur Critique :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Hiérarchie des groupes**.
2. Dans la liste des groupes qui s'affiche, cliquez sur le lien portant le nom d'un groupe dont vous voulez changer les états de l'appareil.
3. Dans la fenêtre des propriétés qui s'ouvre, sélectionnez l'onglet **État de l'appareil**.
4. Dans le volet de gauche, sélectionnez **Critique**.
5. Dans le volet droit, dans la section **Définir l'état comme "Critique" si les options suivantes sont définies**, activez la condition pour basculer un appareil en état *Critique*.

   Vous pouvez modifier seulement les paramètres qui ne sont pas verrouillés dans la stratégie parent.

6. Sélectionnez le bouton radio à côté de la condition dans la liste.
7. Dans le coin supérieur gauche de la liste, cliquez sur le bouton **Modifier**.
8. Définissez la valeur requise pour la condition sélectionnée.

   Certaines conditions n'acceptent pas de valeurs.

9. Cliquez sur le bouton **OK**.

Lorsque les conditions spécifiées sont remplies, l'appareil administré se voit affecter l'état *Critique*.

Pour activer le changement d'état de l'appareil sur Avertissement :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Hiérarchie des groupes**.
2. Dans la liste des groupes qui s'affiche, cliquez sur le lien portant le nom d'un groupe dont vous voulez changer les états de l'appareil.
3. Dans la fenêtre des propriétés qui s'ouvre, sélectionnez l'onglet **État de l'appareil**.
4. Dans le volet gauche, sélectionnez **Avertissement**.
5. Dans le volet droit, dans la section **Définir l'état comme "Avertissement" si les options suivantes sont définies,** activez la condition pour basculer un appareil en état *Avertissement*.

   Vous pouvez modifier seulement les paramètres qui ne sont pas verrouillés dans la stratégie parent.

6. Sélectionnez le bouton radio à côté de la condition dans la liste.
7. Dans le coin supérieur gauche de la liste, cliquez sur le bouton **Modifier**.
8. Définissez la valeur requise pour la condition sélectionnée.

   Certaines conditions n'acceptent pas de valeurs.

9. Cliquez sur le bouton **OK**.

Lorsque certaines conditions spécifiées sont remplies, l'appareil administré se voit affecter l'état *Avertissement*.

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 pouvez basculer la gestion des appareils entre les Serveurs d'administration suivants :

- Serveur d'administration principal et l'un de ses Serveurs d'administration virtuels
- Deux Serveurs d'administration virtuels du même Serveur d'administration principal

Pour modifier le Serveur d'administration, sous lequel les appareils clients se trouvent, par un autre Serveur, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Tâches**.
2. Cliquez sur **Ajouter**.

   Ceci permet de lancer l'assistant de création d'une tâche. Parcourez les étapes de l'assistant à l'aide du bouton **Suivant**.

3. À l'étape **Paramètres de nouvelle tâche**, spécifiez les paramètres suivants :

   a. Dans la liste déroulante **Application**, sélectionnez **Kaspersky Security Center Cloud Console**.

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 NetBIOS, les noms DNS, les adresses IP, ainsi que les plages d'adresses IP auxquels il convient d'affecter la tâche.

  Vous pourriez utiliser cette option pour exécuter une tâche pour un sous-réseau défini. Par exemple, vous pourriez souhaiter installer une certaine application sur les appareils des comptables ou analyser des appareils dans un sous-réseau qui est probablement infecté.

- **Attribuer la tâche à une sélection d'appareils**

  La tâche est affectée aux appareils qui appartiennent à une sélection d'appareils. Vous pouvez définir une des sélections existantes.

  Par exemple, vous pourriez souhaiter utiliser cette option pour exécuter une tâche sur des appareils dotés d'une version du système d'exploitation spécifique.

4. À l'étape Zone d' **Zone d'action d'une tâche**, indiquez un groupe d'administration, des appareils avec des adresses spécifiques ou une sélection d'appareils.

5. À l'étape suivante, confirmez que vous acceptez les conditions de modification du Serveur d'administration pour les appareils clients.

6. À l'étape suivante, sélectionnez le Serveur d'administration virtuel que vous souhaitez utiliser pour administrer les appareils sélectionnés.

7. À l'étape **Sélection du compte utilisateur pour exécuter la tâche**, spécifiez 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 sur la page **Fin de la création de la tâche** vous activez l'option **Ouvrir les détails de la tâche à la fin de la création**, vous pouvez modifier les paramètres de la tâche par défaut.

   Si vous n'activez pas cette tâche, la tâche est créée selon les paramètres par défaut. Vous pourrez modifier ces paramètres par défaut plus tard, à tout moment.

9. Cliquez sur le bouton **Terminer**.

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

10. Cliquez sur le nom de la tâche créée pour ouvrir la fenêtre de propriétés de la tâche.

11. Dans la fenêtre des propriétés de la tâche, indiquez les paramètres généraux de la tâche en fonction de vos besoins.

12. Cliquez sur le bouton **Enregistrer**.

    La tâche est créée et configurée.

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.

Évitement des conflits entre plusieurs Serveurs d'administration

Si le réseau compte plus d'un Serveur d'administration, ils peuvent voir les mêmes appareils clients. Cela peut entraîner, par exemple, l'installation par le Serveur d'administration d'une application déjà installée par un autre Serveur d'administration, et d'autres conflits. Pour empêcher l'installation d'une application sur un appareil administré par un autre Serveur d'administration, vous devez activer l'option **Installer uniquement sur les appareils administrés via &ce Serveur d'administration** dans les propriétés de la tâche *Installation à distance d'une application*.

Si vous activez l'option **Installer uniquement sur les appareils administrés via &ce Serveur d'administration**, puis que vous exécutez la tâche *Installation à distance d'une application*, une vérification est effectuée afin de déterminer si les appareils sont administrés par un autre Serveur d'administration. Pour les appareils administrés par un autre Serveur d'administration, la valeur de l'attribut **Administré par un autre Serveur d'administration** est définie sur `true`. La tâche *Installation à distance d'une application* ne sera pas appliquée à ces appareils.

Les valeurs de l'attribut **Administré par un autre Serveur d'administration** s'affichent dans la colonne **Administré par un autre Serveur d'administration** dans la liste des appareils administrés et la liste des appareils non définis.

Vous pouvez également utiliser la propriété **Administré par un autre Serveur d'administration** en tant que critère aux fins suivantes :

- Affichage des appareils administrés
- Sélections d'appareils
- Règles de déplacement des appareils
- Règles d'attribution automatique de tags

Pour réinitialiser l'attribut Administré par un autre Serveur d'administration,

Dans le menu principal de Kaspersky Security Center Cloud Console, accédez à **Découverte et déploiement** → **Appareils non définis**, sélectionnez les appareils requis, puis cliquez sur le bouton **Supprimer l'attribut Administré par un autre Serveur d'administration**.

L'attribut **Administré par un autre Serveur d'administration** est réinitialisé.

Création de profils de connexion au Serveur d'administration

Pour permettre aux utilisateurs itinérants de modifier le mode de connexion de l'Agent d'administration au Serveur d'administration, vous devez configurer les profils de connexion du Serveur d'administration.

Les profils des connexions ne sont pris en charge que pour les appareils fonctionnant sous Windows et macOS.

Pour créer un profil de connexion, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)**, puis exécutez une des actions suivantes :
   - Si vous souhaitez créer un profil de connexion pour un groupe d'appareils administrés, cliquez sur **Stratégies et profils**, puis sur **Agent d'administration de Kaspersky Security Center**.
   - Si vous souhaitez créer un profil de connexion pour un appareil administré en particulier, cliquez sur **Appareils administrés**, puis sur le nom de l'appareil. Dans la fenêtre qui s'ouvre, accédez à l'onglet **Applications** puis cliquez sur **Agent d'administration de Kaspersky Security Center**.

   La fenêtre des propriétés de la stratégie de l'Agent d'administration s'ouvre.
2. Accédez à l'onglet **Paramètres de l'application**, puis passez à la section **Connectivité**.
3. Dans la section **Profils de connexion**, cliquez sur le bouton **Paramètres**.
   La sous-section **Profils de connexion au Serveur d'administration** affiche le tableau des profils de connexion.

   Il est impossible d'afficher, de modifier ou de supprimer les profils de connexion de **Serveur d'administration domestique** et **Mode hors ligne**.
4. Cliquez sur le bouton **Ajouter**, puis dans la fenêtre qui s'ouvre, indiquez le nom du profil.

Le nom doit être unique. Vous ne pouvez pas utiliser le même nom pour plusieurs profils.

5. Si nécessaire, cochez les cases dans les champs suivants :

   - **Activer le mode de l'utilisateur autonome quand le Serveur d'administration n'est pas disponible**.
   - **Utiliser un serveur proxy**.
     Si vous sélectionnez cette option, procédez comme suit :
     - Indiquez les informations dans le champ **Adresse** et le champ **Numéro de port**.
     - Si nécessaire, cochez la case **Authentification du serveur proxy**, puis indiquez le nom d'utilisateur et le mot de passe dans les champs correspondants.

6. Cliquez sur **Enregistrer**.

Le nouveau profil s'affiche dans le tableau des profils de connexion. Vous pouvez l'utiliser pour configurer les 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.

Vous pouvez modifier et supprimer les profils de connexion.

Pour modifier un profil de connexion, procédez comme suit :

1. Dans le tableau des profils de connexion, cliquez sur le nom du profil de connexion que vous souhaitez modifier.
2. Apportez les modifications nécessaires, puis cliquez sur le bouton **Enregistrer**.

Les modifications sont appliquées au profil de connexion.

Pour supprimer un profil de connexion, procédez comme suit :

1. Dans le tableau des profils de connexion, cochez les cases en regard des profils de connexion que vous souhaitez supprimer.
2. Cliquez sur le bouton **Supprimer**.

Les profils de connexion sélectionnés sont supprimés.

À propos des clusters et des groupes des serveurs

Kaspersky Security Center Cloud Console prend en charge la technologie de cluster. Si l'Agent d'administration transmet au Serveur d'administration les informations sur le fait que l'application installée sur l'appareil client est une partie de la matrice du serveur, alors l'appareil client devient le nœud du cluster.

Si un groupe d'administration contient des clusters ou des groupes de serveurs, la page **Appareils administrés** affiche deux onglets, un pour les appareils individuels et un pour les clusters et les groupes de serveurs. Une fois que les appareils administrés ont été détectés en tant que nœuds de cluster, le cluster est ajouté en tant qu'objet individuel à l'onglet **Clusters et matrices 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 Cloud Console remet automatiquement le cluster supprimé et ses nœuds dans la liste des appareils administrés.

Propriétés d'un cluster ou d'un groupe de serveurs

Pour consulter les paramètres d'un cluster ou d'un groupe de serveurs, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Appareils administrés** → **Clusters et matrices 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 Cloud Console 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.

Tags de l'appareil

Kaspersky Security Center Cloud Console permet de désigner les tags pour les appareils. Un *tag* est un identificateur de l'appareil qui peut être utilisé pour regrouper, décrire ou rechercher des appareils. Les tags désignés pour les appareils peuvent être utilisés lors de la création de sélections d'appareils, lors de la recherche d'appareils et lors de la répartition d'appareils en groupes d'administration.

Les tags peuvent être désignés pour les appareils manuellement ou automatiquement. Vous pouvez utiliser l'attribution manuelle de tag quand vous souhaitez attribuer un tag à un seul appareil. La désignation automatique des tags est l'œuvre du Kaspersky Security Center Cloud Console administration conformément aux règles spécifiées de l'attribution des tags.

L'attribution automatique de tags aux appareils s'opère lors de l'exécution des règle définies. A chaque tag correspond une règle distincte. Les règles peuvent être appliquées aux propriétés réseau de l'appareil, au système d'exploitation de l'appareil, aux applications installées sur l'appareil ou à d'autres propriétés de l'appareil. Par exemple, si votre réseau comprend des appareils fonctionnant sous Windows, Linux et macOS, vous pouvez configurer une règle qui attribuera la balise `[Linux]` à tous les appareils fonctionnant sous Linux. 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 Linux et à leur attribuer une tâche. Un tag est automatiquement supprimé d'un appareil dans les cas suivants :

- Dès que l'appareil cesse de remplir les conditions de la règle qui attribue le tag.

- Lorsque la règle qui attribue la balise est désactivée ou supprimée.

La liste des tags et la liste des règles sur chaque Serveur d'administration sont indépendantes de tous les autres Serveurs d'administration, y compris du Serveur d'administration principal ou des Serveurs d'administration secondaires virtuels. Une règle est appliquée uniquement aux appareils du même Serveur d'administration sur lequel la règle est créée.

Création d'un tag de l'appareil

Pour créer un tag de l'appareil, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Tags** → **Tags de l'appareil**.
2. Cliquez sur **Ajouter**.
   Une fenêtre de nouveau tag s'ouvre.
3. Dans le champ **Tags**, saisissez le nom du tag.
4. Cliquez sur le bouton **Enregistrer** afin d'enregistrer les modifications.

Le nouveau tag apparaît dans la liste des tags de l'appareil.

Renommage d'un tag de l'appareil

Pour renommer un tag de l'appareil, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Tags** → **Tags de l'appareil**.
2. Cliquez le nom du tag que vous souhaitez modifier.
   Une fenêtre de propriété du tag s'ouvre.
3. Dans le champ **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

Pour supprimer un tag de l'appareil, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Tags** → **Tags de l'appareil**.
2. Dans la liste, sélectionnez le tag de l'appareil que vous souhaitez supprimer.
3. Cliquez sur le bouton **Supprimer**.
4. Dans la fenêtre qui s'ouvre, cliquez sur **Oui**.

Le tag de l'appareil est supprimé. Le tag supprimé est automatiquement retiré de tous les appareils auxquels il était attribué.

Le tag que vous avez supprimé n'est pas automatiquement supprimé des règles d'attribution automatique de tags. Une fois le tag supprimé, il est attribué à un nouvel appareil seulement lorsque l'appareil répond tout d'abord aux conditions d'une règle qui attribue le tag.

Le tag supprimé n'est pas supprimé automatiquement de l'appareil si ce tag est attribué à l'appareil par une application ou un Agent d'administration. Pour supprimer le tag de votre appareil, utilisez l'utilitaire klscflag.

Affichage des appareils ayant reçu un tag

Pour voir les appareils auxquels un tag a été attribué, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Tags** → **Tags de l'appareil**.
2. Cliquez sur le lien **Consulter les appareils** en regard du tag pour lequel vous souhaitez voir les appareils associés.

   Vous serez redirigé vers la section **Appareils administrés** du menu principal, avec les appareils filtrés en fonction du tag pour lequel vous avez cliqué sur le lien **Consulter les appareils**.
3. Pour revenir à la liste des tags de l'appareil, cliquez sur le bouton **Retour** de votre navigateur.

Après avoir consulté les appareils auxquels le tag est attribué, vous pouvez créer et attribuer un nouveau tag ou attribuer le tag existant à d'autres appareils. Dans ce cas, vous devez supprimer le filtre par tag, sélectionner les appareils, puis attribuer le tag.

Consultation des tags attribués à un appareil

Pour voir les tags attribués à un appareil :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Appareils administrés**.
2. Cliquez sur le nom de l'appareil dont vous souhaitez voir les tags.
3. Dans la fenêtre des propriétés de l'appareil qui s'ouvre, sélectionnez l'onglet **Tags**.

   La liste des tags attribués à l'appareil sélectionné s'affiche. La colonne **Tag défini** permet de consulter la manière dont le tag a été attribué.

Vous pouvez attribuer un autre tag à l'appareil ou retirer un tag déjà attribué. Vous pouvez aussi afficher tous les tags de l'appareil qui existent sur le Serveur d'administration.

Vous pouvez également afficher les balises attribuées à un appareil dans la ligne de commande à l'aide de l'utilitaire klscflag.

Pour afficher les balises attribuées à un appareil dans la ligne de commande, exécutez la commande suivante :

```
klscflag -ssvget -pv 1103/1.0.0.0 -s KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -svt
ARRAY_T -ss "|ss_type = \"SS_PRODINFO\";"
```

Marquage manuel des appareils

Pour attribuer un tag à un appareil, procédez comme suit :

1. Consultez les tags attribués à l'appareil auquel vous souhaitez attribuer un autre tag.
2. Cliquez sur **Ajouter**.
3. Dans la fenêtre qui s'ouvre, réalisez une des opérations suivantes :
   - Pour créer un tag et l'attribuer, sélectionnez **Créer un tag**, puis renseignez le nom du nouveau tag.
   - Pour sélectionner un tag existant, sélectionnez **Attribuer un tag existant**, puis sélectionnez le tag nécessaire dans la liste déroulante.
4. Cliquez sur le bouton **OK** pour appliquer les modifications.
5. Cliquez sur le bouton **Enregistrer** afin d'enregistrer les modifications.

Le tag sélectionné est attribué à l'appareil.

Pour attribuer un tag à plusieurs appareils, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Appareils administrés**.
2. Sélectionnez les appareils auxquels vous souhaitez attribuer un tag.
3. Cliquez sur **Tags**, puis sélectionnez **Désigner** dans la liste déroulante.
4. Dans la fenêtre qui s'ouvre, sélectionnez un tag dans la liste déroulante.
   Si nécessaire, vous pouvez sélectionner plusieurs tags.
   Vous pouvez aussi réaliser les opérations suivantes :
   - Modifiez le nom d'un tag en cliquant sur le bouton **Modifier** ( ).
     Spécifiez le nouveau nom du tag, puis cliquez sur le bouton **Enregistrer**.

     Notez que le tag sera également renommé dans la liste des tags de l'appareil.
   - Supprimez un tag à l'aide du bouton **Supprimer** ( ).
     Dans la fenêtre qui s'ouvre, cliquez sur **Supprimer ;**.

     Notez que le tag sera également supprimé du Serveur d'administration.
5. Cliquez sur **Enregistrer**.

Les tags sont attribués aux appareils sélectionnés. Vous pouvez supprimer les tags attribués.

Suppression de tags attribués des appareils

Le tag de l'appareil non défini n'est pas supprimé. Si vous le voulez, vous pouvez le supprimer manuellement.

Vous ne pouvez pas supprimer manuellement les tags attribués à l'appareil par les applications ou l'Agent d'administration. Pour supprimer ces tags, utilisez l'utilitaire klscflag.

Pour supprimer un tag attribué à un appareil, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Appareils administrés**.
2. Cliquez sur le nom de l'appareil dont vous souhaitez voir les tags.
3. Dans la fenêtre des propriétés de l'appareil qui s'ouvre, sélectionnez l'onglet **Tags**.
4. Cochez la case en regard du tag que vous souhaitez supprimer.
5. En haut de la liste, cliquez sur le bouton **Désattribuer un tag ?**.
6. Dans la fenêtre qui s'ouvre, cliquez sur **Oui**.

Le tag est supprimé de l'appareil.

Pour supprimer les tags de plusieurs appareils, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Appareils administrés**.
2. Sélectionnez les appareils dont vous souhaitez supprimer les tags.
3. Cliquez sur **Tags**, puis sélectionnez **Désaffecter** dans la liste déroulante.
4. Dans la fenêtre qui s'ouvre, cochez les cases en regard des tags que vous souhaitez supprimer.

   La fenêtre affiche tous les tags attribués à tous les appareils que vous avez sélectionnés à l'étape 2.

5. Cliquez sur **Enregistrer**.

Les tags sont supprimés des appareils.

Consultation des règles pour l'attribution automatique de tags aux appareils

Pour consulter les règles d'attribution automatique de tags aux appareils, procédez comme suit :

Réalisez une des opérations suivantes :

- Dans le menu principal, accédez à **Ressources (Appareils)** → **Tags** → **Règles d'attribution automatique de tags**.
- Dans le menu principal, accédez à **Ressources (Appareils)** → **Tags** → **Tags de l'appareil**, puis cliquez sur le lien **Configurer les règles d'attribution automatique de tags**.
- Consultez les tags attribués à un appareil, puis cliquez sur le bouton **Configuration**.

La liste des règles d'attribution automatique de tags aux appareils s'affiche.

Modification d'une règle d'attribution automatique de tags aux appareils

Pour éditer une règle d'attribution automatique de tags aux appareils, procédez comme suit :

1. Consultez les règles pour l'attribution automatique de tags aux appareils.
2. Cliquez sur le nom de la règle que vous souhaitez modifier.

   Une fenêtre de paramètres de la règle s'ouvre.
3. Modifiez les propriétés générales de la règle :

   a. Dans le champ **Nom de la règle**, modifiez le nom de la règle.

   Le nom ne peut pas contenir plus de 256 caractères.

   b. Réalisez une des opérations suivantes :

   - Activez la règle en basculant le commutateur sur **Règle activée**.
   - Désactivez la règle en basculant le commutateur sur **Règle désactivée**.
4. Réalisez une des opérations suivantes :

   - Si vous souhaitez ajouter une nouvelle condition, cliquez sur le bouton **Ajouter** et définissez les paramètres de la nouvelle condition dans la fenêtre qui s'ouvre.
   - Si vous souhaitez modifier une condition existante, cliquez sur le nom de la condition que vous voulez modifier, puis modifiez les paramètres de la condition.
   - Si vous souhaitez supprimer une condition, cochez la case en regard du nom de la condition que vous souhaitez supprimer, puis cliquez sur **Supprimer**.
5. Cliquez sur **OK** dans la fenêtre des paramètres de conditions.
6. Cliquez sur le bouton **Enregistrer** afin d'enregistrer les modifications.

La règle modifiée apparaît dans la liste.

Création d'une règle d'attribution automatique de tags aux appareils

Pour créer une règle d'attribution automatique de tags aux appareils, procédez comme suit :

1. Consultez les règles pour l'attribution automatique de tags aux appareils.

2. Cliquez sur **Ajouter**.

   Une fenêtre de paramètres de nouvelle règle s'ouvre.

3. Configurez les propriétés générales de la règle :

   a. Dans le champ **Nom de la règle**, saisissez le nom de la règle.

      Le nom ne peut pas contenir plus de 256 caractères.

   b. Exécutez une des actions suivantes :

      - Activez la règle en basculant le commutateur sur **Règle activée**.
      - Désactivez la règle en basculant le commutateur sur **Règle désactivée**.

   c. Dans le champ **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 le déclenchement de la règle d'appareils selon les conditions suivantes . Il est possible de choisir plusieurs conditions.

   - **Réseau** : propriétés réseau des appareils (par exemple, nom de l'appareil sur le réseau Windows, appartenance de l'appareil au domaine, à un sous-réseau IP).

     Si le classement sensible à la casse est défini pour la base de données que vous utilisez pour Kaspersky Security Center Cloud Console, respectez la casse lorsque vous indiquez le nom DNS de l'appareil. Sinon, la règle de marquage automatique ne fonctionnera pas.

   - **Applications** : présence sur l'appareil de l'Agent d'administration, le type, la version et l'architecture du système d'exploitation.
   - **Machines virtuelles** : l'appareil appartient à un type particulier de machine virtuelle.
   - **Active Directory** : présence de l'appareil dans la sous-section Active Directory et appartenance de l'appareil au groupe Active Directory.
   - **Registre des applications** : présence sur l'appareil d'applications de différents éditeurs.

7. Cliquez sur le bouton **OK** afin d'enregistrer les modifications.

   Le cas échéant, il est possible d'attribuer plusieurs catégories à une règle. Dans ce cas, le tag est attribué aux appareils quand au moins une des conditions est remplie.

8. Cliquez sur le bouton **Enregistrer** afin d'enregistrer les modifications.

La règle nouvellement créée est exécutée sur les appareils administrés par le Serveur d'administration sélectionné. Si les paramètres de l'appareil correspondent aux conditions de la règle, cet appareil reçoit ce tag.

Plus tard, la règle est appliquée dans les cas suivants :

- Automatiquement et de manière périodique en fonction de la charge de travail du serveur
- Après que vous avez modifié la règle
- Quand vous exécutez la règle manuellement
- Une fois que le serveur d'administration a détecté une modification des paramètres d'un appareil qui remplit les conditions de la règle ou des paramètres d'un groupe qui contient cet appareil

Vous pouvez créer plusieurs règles d'attribution des tags. Plusieurs tags peuvent être attribués à un appareil si vous aviez créé plusieurs règles et que les conditions d'exécution de ces règles sont remplies simultanément. Vous pouvez consulter la liste de tous les tags attribués dans les propriétés de l'appareil.

Règles d'exécution pour l'attribution automatique de tags aux appareils

Quand une règle est appliquée, le tag défini dans les propriétés de cette règle est attribué aux appareils qui remplissent les conditions définies dans les propriétés de la même règle. Vous pouvez exécuter uniquement des règles actives.

Pour exécuter des règles d'attribution automatique de tags aux appareils, procédez comme suit :

1. Consultez les règles pour l'attribution automatique de tags aux appareils.
2. Cochez les cases en regard des règles activez que vous souhaitez exécuter.
3. Cliquez sur le bouton **Exécuter la règle**.

   Les règles sélectionnées s'exécutent.

Suppression d'une règle d'attribution automatique de tags aux appareils

Pour supprimer une règle d'attribution automatique de tags aux appareils, procédez comme suit :

1. Consultez les règles pour l'attribution automatique de tags aux appareils.
2. Cochez les cases en regard de la règle que vous souhaitez supprimer.
3. Cliquez sur **Supprimer**.
4. Dans la fenêtre qui s'ouvre, cliquez une nouvelle fois sur **Supprimer ;**.

   La règle sélectionnée est supprimée. Le tag défini dans les propriétés de cette règle est retiré de tous les appareils auxquels il avait été attribué.

> Le tag de l'appareil non défini n'est pas supprimé. Si vous le voulez, vous pouvez le supprimer manuellement.

Quarantaine et sauvegarde

Les applications antivirus de Kaspersky installées sur les appareils clients peuvent placer les fichiers en quarantaine ou dans le dossier de sauvegarde lors de l'analyse des appareils.

La *Quarantaine* est un stockage spécial qui contient les fichiers probablement infectés par les virus ou irréparables lors de la découverte.

La *Sauvegarde* est conçue pour enregistrer les copies de sauvegarde des fichiers qui ont été supprimés ou modifiés lors de la désinfection.

Kaspersky Security Center Cloud Console forme une liste générale des fichiers placés en quarantaine ou dans le dossier de sauvegarde par les applications de Kaspersky sur les appareils. Les Agents d'administration des appareils clients transmettent les informations sur les fichiers en quarantaine et dans les dossiers de sauvegarde sur le Serveur d'administration.

Kaspersky Security Center Cloud Console ne copie pas les fichiers sur le Serveur d'administration à partir des stockages. Tous les fichiers sont placés dans les stockages des appareils.

Téléchargement d'un fichier à partir de stockages

Kaspersky Security Center Cloud Console permet de télécharger des copies des fichiers placés par l'application de sécurité en quarantaine ou dans le dossier de sauvegarde sur l'appareil client. Les fichiers sont copiés vers la destination que vous indiquez.

Vous pouvez télécharger des fichiers si l'une des conditions suivantes est remplie : l'option **Maintenir la connexion au Serveur d'administration** est activée dans les paramètres de l'appareil, un serveur push ou une passerelle de connexion est en cours d'utilisation. Dans le cas contraire, il n'est pas possible d'effectuer de téléchargement.

Le total des appareils pour lesquels l'option **Maintenir la connexion au Serveur &d'administration** a été sélectionnée ne peut être supérieur à 300.

Pour enregistrer une copie du fichier de la quarantaine ou du dossier de sauvegarde sur le disque dur, procédez comme suit :

1. Exécutez une des actions suivantes :

   - Si vous souhaitez enregistrer une copie du fichier en quarantaine, dans le menu principal, accédez à **Opérations → Stockages → Quarantaine**.

   - Si vous souhaitez enregistrer une copie du fichier du dossier de sauvegarde, dans le menu principal, accédez à **Opérations → Stockages → Sauvegarde**.

2. Dans la fenêtre qui s'ouvre, sélectionnez un fichier que vous souhaitez télécharger et cliquez sur **Télécharger**.

   Le téléchargement démarre. Une copie du fichier qui avait été placé en quarantaine sur l'appareil client est enregistrée dans le dossier indiqué.

Suppression des fichiers depuis les stockages

Pour supprimer le fichier placé en quarantaine ou dans le dossier de sauvegarde, procédez comme suit :

1. Exécutez une des actions suivantes :

   - Si vous souhaitez enregistrer une copie du fichier en quarantaine, dans le menu principal, accédez à **Opérations → Stockages → Quarantaine**.

   - Si vous souhaitez enregistrer une copie du fichier du dossier de sauvegarde, dans le menu principal, accédez à **Opérations → Stockages → Sauvegarde**.

2. Dans la fenêtre qui s'ouvre, sélectionnez un fichier que vous souhaitez supprimer, puis cliquez sur **Supprimer**.

3. Confirmez la suppression du fichier.

   L'application de sécurité sur l'appareil client qui avait placé des fichiers dans le stockage (quarantaine ou sauvegarde) supprime les mêmes fichiers de ce stockage.

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 principal, accédez à **Ressources (Appareils)** → **Groupes** → **<nom du groupe>** → **Appareils administrés**.
   - Si l'appareil appartient au groupe Appareils non définis, dans le menu principal, accédez à **Découverte et déploiement** → **Appareils non définis**.

2. Cliquez sur le nom de l'appareil concerné.

3. Dans la fenêtre des propriétés de l'appareil qui s'ouvre, sélectionnez l'onglet **Avancé**.

4. Dans 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, un 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 paramètres suivants sont disponibles :

      - Niveau de traçage

        Le niveau de traçage définit le volume de détails repris dans le fichier de traçage.

      - Traçage sur la base d'une rotation

L'application écrase les informations de traçage afin d'empêcher l'augmentation excessive de la taille du fichier de traçage. Indiquez le nombre maximal de fichiers à utiliser pour stocker les informations de traçage ainsi que la taille maximale de chaque fichier. Quand le nombre maximum de fichiers de traçage de la taille maximale est atteint, le fichier de traçage le plus ancien est supprimé afin de pouvoir écrire un nouveau fichier de traçage.

Ce paramètre est disponible uniquement pour Kaspersky Endpoint Security.

c. Cliquez sur **Enregistrer**.

Le traçage est activé pour l'application sélectionnée. Dans certains cas, pour activer le traçage de l'application de sécurité, il faut relancer cette application et sa tâche.

Sur les appareils clients basés sur Linux, le traçage pour le module Programme de mise à jour de Kaspersky Security Agent 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 **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

Vous pouvez télécharger des fichiers de traçage à partir d'un appareil client si l'une des conditions suivantes est remplie : l'option **Maintenir la connexion au Serveur d'administration** est activée dans les paramètres de l'appareil, un serveur push ou une passerelle de connexion est en cours d'utilisation. Dans le cas contraire, il n'est pas possible d'effectuer de téléchargement.

Le total des appareils pour lesquels l'option **Maintenir la connexion au Serveur &d'administration** a été sélectionnée ne peut être supérieur à 300.

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 l'option **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.

   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.

Télécharger les paramètres de l'application

Vous pouvez télécharger les paramètres d'application à partir d'un appareil client si l'une des conditions suivantes est remplie : l'option **Maintenir la connexion au Serveur d'administration** est activée dans les paramètres de l'appareil, un serveur push ou une passerelle de connexion est en cours d'utilisation. Dans le cas contraire, il n'est pas possible d'effectuer de téléchargement.

Le total des appareils pour lesquels l'option **Maintenir la connexion au Serveur &d'administration** a été sélectionnée ne peut être supérieur à 300.

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

Vous pouvez télécharger les informations système sur votre appareil à partir d'un appareil client uniquement si l'une des conditions suivantes est remplie : l'option **Maintenir la connexion au Serveur d'administration** est activée dans les paramètres de l'appareil, un serveur push ou une passerelle de connexion est en cours d'utilisation. Dans le cas contraire, il n'est pas possible d'effectuer de téléchargement.

Le total des appareils pour lesquels l'option **Maintenir la connexion au Serveur &d'administration** a été sélectionnée ne peut être supérieur à 300.

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.

Le fichier avec les informations est téléchargé à l'emplacement indiqué.

Téléchargement des journaux des événements

Vous pouvez télécharger les journaux d'événements sur votre appareil à partir d'un appareil client uniquement si l'une des conditions suivantes est remplie : l'option **Maintenir la connexion au Serveur d'administration** est activée dans les paramètres de l'appareil, un serveur push ou une passerelle de connexion est en cours d'utilisation. Dans le cas contraire, il n'est pas possible d'effectuer de téléchargement.

Le total des appareils pour lesquels l'option **Maintenir la connexion au Serveur &d'administration** a été sélectionnée ne peut être supérieur à 300.

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.
     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.

Exécution du diagnostic à distance d'une application et téléchargement des résultats

Pour lancer le diagnostic de l'application sur l'appareil distant 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 l'application pour laquelle vous souhaitez exécuter un diagnostic à distance.

   La liste des options de diagnostic à distance s'ouvre.
4. Dans la section **Rapport de diagnostic**, cliquez sur le bouton **Poser le diagnostic**.

   Cette action permet de lancer le processus de diagnostic à distance et de générer un rapport de diagnostic. Le processus de diagnostic est terminé, le bouton **Télécharger le rapport des diagnostics** devient accessible.
5. Cliquez sur le bouton **Télécharger le rapport des diagnostics** pour télécharger le rapport.

Le rapport est téléchargé à l'emplacement indiqué.

Exécution d'une application sur un appareil client

Vous devrez peut-être exécuter une application sur l'appareil client si un expert du support Kaspersky vous le demande. Vous n'avez pas besoin d'installer l'application sur cet appareil.

Pour exécuter une application sur l'appareil client, procédez comme suit :

1. Ouvrez la fenêtre de diagnostic à distance d'un l'appareil client.
2. Dans la fenêtre de diagnostic à distance, sélectionnez l'onglet **Exécution d'une application à distance**.
3. Dans le 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 dans le dossier que vous souhaitez exécuter sur l'appareil client. 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. Dans le groupe **Exécution d'une application à distance**, cliquez sur le bouton **Charger** afin de sélectionner une archive ZIP contenant l'application que vous souhaitez exécuter sur l'appareil client.

7. Cliquez sur le bouton **Charger et exécuter** pour lancer l'application indiquée sur l'appareil client.

8. 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.

Génération d'un fichier dump pour une application

Le fichier de sauvegarde de l'application vous permet de consulter les paramètres de l'application exécutée sur l'appareil client à un moment donné. Ce fichier contient également des informations sur les modules chargés pour une application.

La génération de fichiers de vidage est disponible uniquement pour les processus 32 bits s'exécutant sur les appareils clients Windows. Pour les appareils clients exécutant Linux et pour les processus 64 bits, cette fonctionnalité n'est pas prise en charge.

Pour créer un fichier de vidage pour une application :

1. Ouvrez la fenêtre de diagnostic à distance d'un l'appareil client.

2. Dans la fenêtre de diagnostic à distance, sélectionnez l'onglet **Exécution d'une application à distance**.

3. Dans la section **Génération du fichier dump du processus**, indiquez le fichier exécutable de l'application pour lequel vous souhaitez générer le fichier dump.

4. Cliquez sur le bouton **Télécharger** afin d'enregistrer le fichier de vidage pour l'application indiquée.

   Si l'application indiquée n'est pas en cours d'exécution sur l'appareil client, le message d'erreur s'affiche.

Connexion à distance au bureau de l'appareil client

Vous pouvez obtenir l'accès au bureau de l'appareil client à l'aide d'une instance de l'Agent d'administration installée 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, vous obtenez l'accès complet aux informations sur cet appareil et pouvez administrer les applications installées sur celui-ci.

La connexion à distance doit être autorisée dans les paramètres du système d'exploitation de l'appareil administré cible. Par exemple, dans Windows 10, cette option est appelée **Autoriser les connexions d'assistance à distance vers cet ordinateur** (vous pouvez trouver cette option dans **Panneau de configuration → Système et sécurité → Système → Paramètres d'utilisation à distance**). Si vous disposez d'une licence pour la fonctionnalité de la gestion des vulnérabilités et des correctifs, vous pouvez imposer l'activation de cette option lorsque vous établissez une connexion à un appareil administré. Si vous ne disposez pas de la licence, activez cette option localement sur l'appareil administré cible. Si cette option est désactivée, la connexion à distance n'est pas possible.

Pour établir une connexion à distance à un appareil, vous devez disposer de deux utilitaires :

- Utilitaire Kaspersky intitulé klsctunnel. Cet utilitaire doit être stocké sur votre poste de travail. Vous utilisez cet utilitaire pour établir une connexion en tunnel entre un appareil client et le Serveur d'administration.

  Kaspersky Security Center Cloud Console permet d'établir des connexions TPC en tunnel depuis la Console d'administration via le Serveur d'administration et puis via l'Agent d'administration vers le port défini sur l'appareil administré. Le tunnel est utilisé pour connecter une app cliente qui se trouve sur un appareil doté de la Console d'administration au port TCP sur l'appareil administré si la connexion directe de l'appareil avec la Console d'administration et l'appareil n'est pas possible.

  La connexion en tunnel de l'appareil client à distance avec le Serveur d'administration est nécessaire si le port de connexion au Serveur d'administration est inaccessible sur l'appareil. Le port sur l'appareil peut être inaccessible dans les cas suivants :

  - L'appareil à distance est connecté au réseau local avec le mécanisme NAT utilisé.
  - L'appareil à distance fait partie du réseau local du Serveur d'administration, mais son port est fermé par un pare-feu.

- Module standard de Microsoft Windows intitulé " Connexion Bureau à distance ". La connexion au bureau à distance est exécutée à l'aide de l'utilitaire titulaire de Windows mstsc.exe conformément aux paramètres de fonctionnement de cet utilitaire.

  La connexion à la session en cours sur le poste de travail distant de l'utilisateur s'établit sans notification. Une fois que vous êtes connecté à la session, l'utilisateur de l'appareil sera déconnecté sans notification.

Pour se connecter au bureau d'un appareil client, une des conditions suivantes doit être remplie :

- L'appareil client est membre d'un groupe d'administration qui possède un point de distribution avec l'option **Maintenir la connexion au Serveur d'administration** activée.
- Dans les paramètres de l'appareil client, l'option **Maintenir la connexion au Serveur d'administration** est activée.

  Le total des appareils clients pour lesquels l'option **Maintenir la connexion au Serveur d'administration** a été activée ne peut être supérieur à 300.

Pour se connecter à distance au bureau de l'appareil client, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils) → Appareils administrés**.
2. Cochez la case en regard du nom de l'appareil auquel vous souhaitez avoir accès.

3. Cliquez sur le bouton **Se connecter au bureau distant**.

   La fenêtre Se connecter au bureau distant s'ouvre.

4. Cliquez sur le bouton **Télécharger** pour télécharger l'utilitaire klsctunnel.

5. Cliquez sur le bouton **Copier dans le presse-papiers** pour copier le texte du champ de texte. Ce texte est un objet de données binaires (BLOB) qui contient les paramètres requis pour établir la connexion entre le Serveur d'administration et l'appareil administré.

   Un BLOB est valide pendant 3 minutes. Si celui-ci a expiré, ouvrez de nouveau la fenêtre Se connecter au bureau distant pour générer un nouveau BLOB.

6. Exécutez l'utilitaire klsctunnel.

   La fenêtre de l'utilitaire s'ouvre.

7. Collez le texte copié dans le champ de texte.

8. Si vous utilisez un serveur proxy, cochez la case **Utiliser un serveur proxy**, puis indiquez les paramètres de connexion du serveur proxy.

9. Cliquez sur **Ouvrir le port**.

   La fenêtre Connexion Bureau à distance s'ouvre.

10. Indiquez les informations d'identification du compte à partir duquel vous êtes actuellement connecté à Kaspersky Security Center Cloud Console.

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

Lorsque la connexion à l'appareil client est établie, le bureau de l'appareil client est accessible dans la fenêtre Connexion Bureau à distance de Microsoft Windows.

Connexion aux appareils à l'aide du Partage du bureau Windows

Vous pouvez obtenir l'accès au bureau de l'appareil client à l'aide d'une instance de l'Agent d'administration installée 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.

Vous pouvez vous connecter à la séance existante sur l'appareil client sans la déconnexion de l'utilisateur travaillant dans cette séance. Dans ce cas, l'utilisateur de la session sur l'appareil et vous disposez d'un accès collectif au bureau.

Pour établir une connexion à distance à un appareil, vous devez disposer de deux utilitaires :

- Utilitaire Kaspersky intitulé klsctunnel. Cet utilitaire doit être stocké sur votre poste de travail. Vous utilisez cet utilitaire pour établir une connexion en tunnel entre un appareil client et le Serveur d'administration.

  Kaspersky Security Center Cloud Console permet d'établir des connexions TPC en tunnel depuis la Console d'administration via le Serveur d'administration et puis via l'Agent d'administration vers le port défini sur l'appareil administré. Le tunnel est utilisé pour connecter une app cliente qui se trouve sur un appareil doté de la Console d'administration au port TCP sur l'appareil administré si la connexion directe de l'appareil avec la Console d'administration et l'appareil n'est pas possible.

La connexion en tunnel de l'appareil client à distance avec le Serveur d'administration est nécessaire si le port de connexion au Serveur d'administration est inaccessible sur l'appareil. Le port sur l'appareil peut être inaccessible dans les cas suivants :

- L'appareil à distance est connecté au réseau local avec le mécanisme NAT utilisé.
- L'appareil à distance fait partie du réseau local du Serveur d'administration, mais son port est fermé par un pare-feu.

- Partage du bureau Windows. Lors de la connexion à la séance existante du bureau à distance, l'utilisateur de la session sur l'appareil recevra une demande de connexion de votre part. 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 Cloud Console.

  Vous pouvez configurer l'audit des actions sur l'appareil client distant. Lors de l'audit, l'application enregistre les informations relatives aux fichiers que l'administrateur a ouverts et/ou modifiés sur l'appareil client.

Pour se connecter au bureau d'un appareil client à l'aide du Partage du bureau Windows, les conditions suivantes doivent être remplies :

- Microsoft Windows Vista ou une version plus récente est installée sur votre poste de travail.

  Pour vérifier si la fonctionnalité de Partage du bureau Windows est incluse dans votre édition Windows, assurez-vous que le CLSID {32BE5ED2-5C86-480F-A914-0FF8885A1B3F} est inclus dans le registre 32 bits.

- Microsoft Windows Vista ou une version plus récente est installée sur l'appareil client.

- Kaspersky Security Center Cloud Console utilise une licence pour la gestion des vulnérabilités et des correctifs.

- L'appareil client est membre d'un groupe d'administration qui possède un point de distribution avec l'option **Maintenir la connexion au Serveur d'administration** activée, ou cette option est activée dans les paramètres de l'appareil client.

  Notez que, le total des appareils clients pour lesquels l'option **Maintenir la connexion au Serveur d'administration** a été sélectionnée ne peut être supérieur à 300.

Pour se connecter au bureau de l'appareil client à l'aide de la technologie Partage du bureau Windows, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Appareils administrés**.
2. Cochez la case en regard du nom de l'appareil auquel vous souhaitez avoir accès.
3. Cliquez sur le bouton **Partage du bureau Windows**.

   L'Assistant Partage du bureau Windows s'ouvre.
4. Cliquez sur le bouton **Télécharger** pour télécharger l'utilitaire klsctunnel et attendez la fin du processus de téléchargement.

   Si vous disposez déjà de l'utilitaire klsctunnel, ignorez cette étape.
5. Cliquez sur le bouton **Suivant**.
6. Sélectionnez la session sur l'appareil auquel vous souhaitez vous connecter, puis cliquez sur le bouton **Suivant**.
7. Sur l'appareil cible, dans la boîte de dialogue qui s'ouvre, l'utilisateur doit autoriser une session de partage de bureau. Dans le cas contraire, il n'est pas possible d'ouvrir une session.

Une fois que l'utilisateur de l'appareil a confirmé la session de partage de bureau, la page suivante de l'assistant s'ouvre.

8. Cliquez sur le bouton **Copier dans le presse-papiers** pour copier le texte du champ de texte. Ce texte est un objet de données binaires (BLOB) qui contient les paramètres requis pour établir la connexion entre le Serveur d'administration et l'appareil administré.

   Un BLOB est valide pendant 3 minutes. Si celui-ci a expiré, générez un nouveau BLOB.

9. Exécutez l'utilitaire klsctunnel.

   La fenêtre de l'utilitaire s'ouvre.

10. Collez le texte copié dans le champ de texte.

11. Si vous utilisez un serveur proxy, cochez la case **Utiliser un serveur proxy**, puis indiquez les paramètres de connexion du serveur proxy.

12. Cliquez sur **Ouvrir le port**.

Le partage du bureau démarre dans une nouvelle fenêtre. Si vous souhaitez interagir avec l'appareil, cliquez sur l'icône du menu ( ) dans le coin supérieur gauche de la fenêtre, puis sélectionnez **Mode interactif**.

Déclenchement des règles en mode Apprentissage intelligent

Cette section fournit des informations relatives aux détections réalisées par les règles du contrôle évolutif des anomalies dans Kaspersky Endpoint Security for Windows sur les appareils clients.

Les règles détectent le comportement anormal sur les appareils clients et peuvent le bloquer. Si les règles fonctionnent en mode Apprentissage intelligent, elles détectent tout comportement anormal et envoient des rapports sur chaque cas au Serveur d'administration de Kaspersky Security Center Cloud Console. Ces informations sont stockées sous forme de liste dans le sous-dossier **Déclenchements de règles dans le mode Apprentissage intelligent** du dossier **Stockages**. Vous pouvez confirmer les détections comme étant correctes ou les ajouter en tant qu'exclusions afin que ce type de comportement ne soit plus considéré comme une anomalie.

Les informations relatives aux détections sont stockées dans le journal des événements sur le Serveur d'administration (avec les autres événements) et dans le rapport Contrôle évolutif des anomalies.

Pour en savoir plus sur le Contrôle évolutif des anomalies, les règles, leur mode et les états, consultez l'aide de Kaspersky Endpoint Security.

Consultation de la liste des détections réalisées à l'aide des règles du contrôle évolutif des anomalies

Pour consulter la liste des détections réalisées à l'aide des règles du contrôle évolutif des anomalies, procédez comme suit :

1. Dans le menu principal, accédez à **Opérations** → **Stockages**.

2. Sélectionnez le lien **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.

- 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.

- Nom d'utilisateur

  Le nom de l'utilisateur de l'appareil client qui exécute le processus qui a généré la détection.

- Traité

  Date de détection de l'anomalie.

- 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).

Pour voir les propriétés de chaque élément d'information, procédez comme suit :

1. Dans le menu principal, accédez à **Opérations → Stockages**.
2. Sélectionnez le lien **Déclenchements de règles dans le mode Apprentissage intelligent**.
3. Dans la fenêtre qui s'ouvre, sélectionnez l'objet souhaité.
4. Cliquez sur le lien **Propriétés**.

   La fenêtre des propriétés de l'objet s'ouvre et présente les informations relatives à l'élément sélectionné.

Vous pouvez confirmer ou ajouter aux exclusions n'importe quel élément de la liste des détections des règles du contrôle évolutif des anomalies.

Pour confirmer un élément,

Sélectionnez un (ou plusieurs éléments) dans la liste des détections, puis cliquez sur le bouton **Confirmer**.

L'état du ou des éléments devient **Confirmation en cours**.

Votre confirmation va contribuer aux statistiques utilisées par les règles (pour en savoir plus, se reporter à la documentation relative à Kaspersky Endpoint Security for Windows).

Pour ajouter un élément en tant qu'exclusion,

Sélectionnez un (ou plusieurs éléments) dans la liste des détections, puis cliquez sur le bouton **Exclure**.

L'Assistant d'ajout d'une exclusion démarre. Suivez les instructions de l'assistant.

Si vous rejetez ou confirmez un élément, celui-ci est exclu de la liste des Détections après la prochaine synchronisation de l'appareil client avec le Serveur d'administration et il n'apparaît plus dans la liste.

Ajout d'exclusions au départ des règles du contrôle évolutif des anomalies

L'Assistant d'ajout d'une exclusion permet d'ajouter des exclusions au départ des règles du Contrôle évolutif des anomalies pour Kaspersky Endpoint Security for Windows.

Pour lancer l'assistant d'ajout d'une exclusion via l'entrée Contrôle évolutif des anomalies :

1. Dans le menu principal, accédez à **Opérations → Stockages → Déclenchements de règles dans le mode Apprentissage intelligent**.
2. Dans la fenêtre qui s'ouvre, sélectionnez un élément un élément (ou plusieurs éléments) dans la liste des détections, puis cliquez sur le bouton **Exclure**.

   Vous pouvez ajouter un maximum de 1 000 exclusions en une fois. Si vous sélectionnez plus d'éléments et que vous tentez de les ajouter aux exclusions, un message d'erreur s'affiche.

L'Assistant d'ajout d'une exclusion démarre. Naviguez dans les fenêtres de l'Assistant à l'aide du bouton **Suivant**.

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

Initialement, la hiérarchie des groupes d'administration contient le seul groupe d'administration appelé **Appareils administrés**. Vous pouvez ajouter des appareils et des groupes imbriqués dans le groupe **Appareils administrés**.

Pour créer un groupe d'administration, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Hiérarchie des groupes**.
2. Dans la hiérarchie, sélectionnez le groupe d'administration qui doit inclure le nouveau groupe d'administration.
3. Cliquez sur le bouton **Ajouter**.
4. Dans la fenêtre 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 structure hiérarchique du groupe d'administration.

L'application permet de créer une structure de groupes d'administration sur la base de la structure d'Active Directory ou de la structure du réseau de domaine. Vous pouvez aussi créer une structure de groupes du fichier texte.

Pour créer une structure de groupes d'administration, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Hiérarchie des groupes**.
2. Cliquez sur le bouton **Importer**.

   Finalement, l'assistant de création de la structure des groupes d'administration se lance. Suivez les instructions de l'assistant.

Installation automatique des applications sur les appareils du groupe d'administration

Vous pouvez définir les paquets d'installation à utiliser pour l'installation automatique à distance des applications Kaspersky sur les appareils clients d'un groupe d'administration.

Afin de configurer l'installation automatique des applications sur les appareils dans le groupe d'administration, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Hiérarchie des groupes**, puis cliquez sur le nom du groupe d'administration requis.
2. Dans la fenêtre des propriétés qui s'ouvre, sélectionnez l'onglet **Installation automatique**.
3. Sélectionnez les paquets d'installation des applications à installer sur les appareils, puis cliquez sur le bouton **Enregistrer**.

Si vous sélectionnez plusieurs paquets d'installation de la même application qui diffèrent uniquement par leurs versions, le paquet d'installation avec la dernière version est enregistré.

Après avoir sélectionné les paquets d'installation, un groupe de tâches pour l'installation des applications sur les appareils du groupe d'administration est créé pour chacune des applications. Ces tâches sont lancées sur les appareils clients juste après avoir été ajoutées au groupe d'administration.

Déplacement des groupes d'administration

Vous pouvez déplacer les groupes d'administration à l'intérieur de la hiérarchie des groupes.

Le groupe d'administration est déplacé avec tous les sous-groupes, les Serveurs d'administration secondaires, les appareils, les stratégies et les tâches de groupe. L'application applique au groupe tous les paramètres correspondant à sa nouvelle position dans la hiérarchie des groupes d'administration lui seront appliqués.

Le nom de groupe doit être unique entre groupes du même niveau de hiérarchie. Si dans le dossier dans lequel vous déplacez le groupe d'administration, un groupe avec un tel nom existe déjà, le nom du groupe doit être modifié avec le déplacement. Si vous n'avez pas modifié préalablement le nom du groupe déplacé, le suffixe **<next sequence number>** sera automatiquement ajouté à son nom lors du déplacement, par exemple : **(1)**, **(2)**.

Vous ne pouvez pas renommer ni déplacer le groupe d'**appareils administrés**.

Pour déplacer un groupe d'administration vers un autre niveau de la hiérarchie des groupes d'administration :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Hiérarchie des groupes**, puis cochez la case en regard du groupe d'administration que vous souhaitez déplacer.

2. Dans la barre d'outils, cliquez sur le bouton **Déplacer**.

3. Dans la fenêtre qui s'ouvre, sélectionnez l'endroit où vous souhaitez déplacer le groupe d'administration et cliquez sur le bouton **Déplacer**.

   La fenêtre est fermée et le groupe d'administration est déplacé vers un autre niveau de la hiérarchie des groupes.

Suppression des groupes d'administration

Si vous supprimez un groupe d'administration contenant des Serveurs d'administration secondaires, des groupes imbriqués, des appareils clients, des tâches de groupe ou des stratégies créées pour ce groupe, tous ces éléments seront également supprimés.

Avant la suppression du groupe d'administration, il faut supprimer de ce groupe les Serveurs d'administration secondaires, les groupes imbriqués et les appareils clients.

Pour supprimer un groupe d'administration, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Hiérarchie des groupes**, puis cochez la case en regard du groupe d'administration que vous souhaitez supprimer.

2. Dans la barre d'outils, cliquez sur le bouton **Supprimer ;**.

Le groupe d'administration est supprimé.

Stratégies et profils de stratégie

Kaspersky Security Center Cloud 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.

À propos des 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 Cloud Console fournit une stratégie propre à chaque application Kaspersky d'un groupe d'administration. La stratégie possède un des états suivants (voir le tableau ci-dessous) :

L'état de la stratégie

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

Le fonctionnement des stratégies obéit aux règles suivantes :

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

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

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

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

Les profils de stratégie fonctionnent conformément aux règles suivantes :

- Un profil de stratégie prend effet lorsqu'une condition d'activation particulière est réalisée.
- Les profils de stratégie contiennent des valeurs de paramètres qui diffèrent des paramètres de stratégie.

- L'activation d'un profil de stratégie modifie les paramètres effectifs de l'appareil administré.
- Une stratégie ne peut pas compter plus de 100 profils de stratégie.

Vous ne pouvez pas créer de stratégie pour le Serveur d'administration.

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
Non défini	Si une icône de cadenas ouvert s'affiche en regard d'un paramètre alors que le commutateur est désactivé, le paramètre n'est pas spécifié dans la stratégie. Un utilisateur peut modifier ces paramètres dans l'interface de l'application administrée. Les paramètres de ce type sont dits *déverrouillés*.
Verrouillé	Si un cadenas verrouillé s'affiche à côté d'un paramètre et si le commutateur est désactivé, le paramètre est appliqué aux appareils sur lesquels la stratégie est appliquée. Un utilisateur ne peut pas modifier les valeurs de ces paramètres dans l'interface de l'application administrée. Les paramètres de ce type sont dits *verrouillés*.

Nous vous recommandons fortement de fermer les verrous pour les paramètres de stratégie que vous souhaitez appliquer sur les appareils administrés. Les paramètres de stratégie déverrouillés peuvent être réattribués par les paramètres de l'application Kaspersky sur un appareil administré.

Vous pouvez utiliser un bouton de verrouillage pour effectuer les actions suivantes :

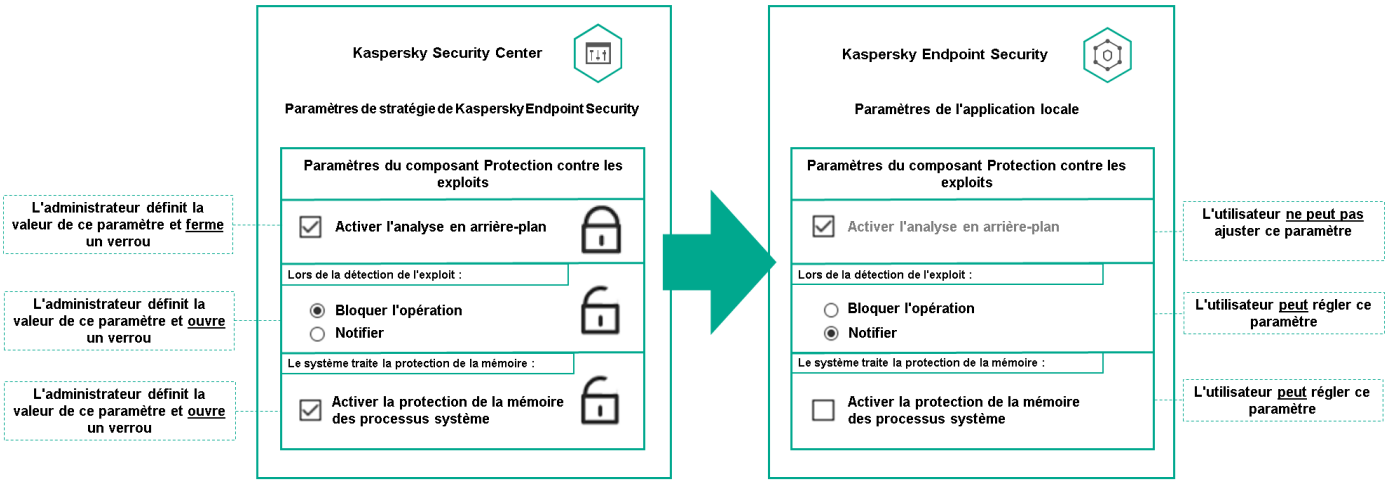
- Paramètres de verrouillage pour une stratégie de sous-groupe d'administration
- Paramètres de verrouillage d'une application Kaspersky sur un appareil administré

Un paramètre verrouillé est ainsi utilisé pour mettre en œuvre des paramètres efficaces sur un appareil administré.

Un processus de mise en œuvre efficace des paramètres comprend les actions suivantes :

- L'appareil administré applique les valeurs des paramètres de l'application Kaspersky.
- L'appareil administré applique les valeurs des paramètres verrouillés d'une stratégie.

Une stratégie et une application Kaspersky administrée contiennent le même ensemble de paramètres. Lorsque vous configurez des paramètres de stratégie, les paramètres de l'application Kaspersky modifient les valeurs sur un appareil administré. Vous ne pouvez pas ajuster les paramètres verrouillés sur un appareil administré (voir le schéma ci-dessous) :



Verrous et paramètres de l'application Kaspersky

Héritage des stratégies, utilisation des profils des stratégies

Cette section comporte des informations sur la hiérarchie et l'héritage des stratégies et des profils de stratégie.

Hiérarchie des stratégies

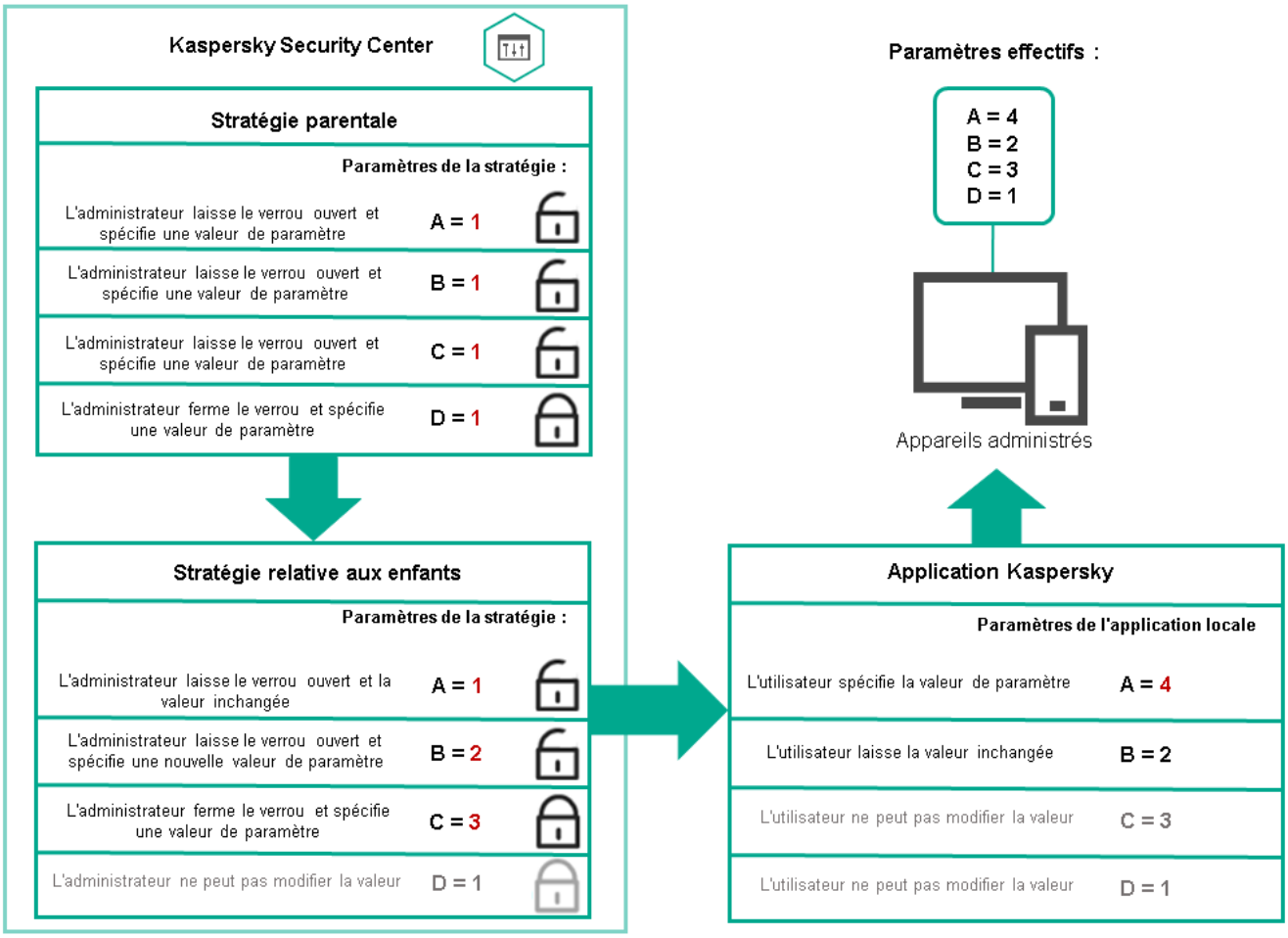
Si des appareils différents requièrent des paramètres différents, vous pouvez organiser les appareils en groupes d'administration.

Vous pouvez spécifier une stratégie pour un seul groupe d'administration. Les paramètres de stratégie peuvent être *hérités*. L'héritage signifie recevoir des valeurs de paramètres de stratégie dans des sous-groupes (groupes enfants) d'une stratégie d'un groupe d'administration de niveau supérieur (parent).

Par la suite, une stratégie pour un groupe parent est également désignée par l'expression *stratégie parent*. Une stratégie pour un sous-groupe (groupe enfant) est également désignée par l'expression *stratégie enfant*.

Par défaut, il existe au moins un groupe d'appareils administrés existe sur le Serveur d'administration. Si vous souhaitez créer des groupes personnalisés, ils sont créés sous forme de sous-groupes (groupes enfants) dans le groupe d'appareils administrés.

Les stratégies d'une même application agissent les unes sur les autres sur la base d'une hiérarchie de groupes d'administration. Les paramètres verrouillés d'une stratégie d'un groupe d'administration de niveau supérieur (parent) réaffecteront les valeurs des paramètres de stratégie d'un sous-groupe (voir la figure ci-dessous).

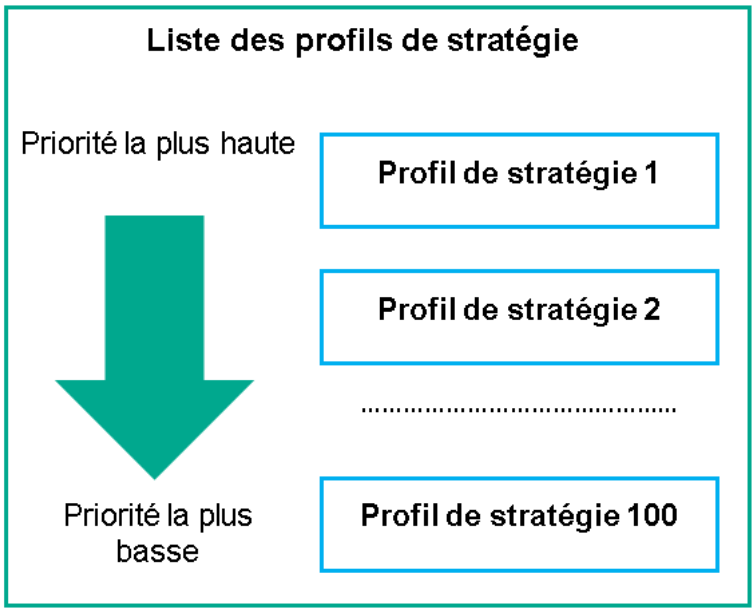


Hiérarchie des stratégies

Profils de stratégie dans une hiérarchie de stratégies

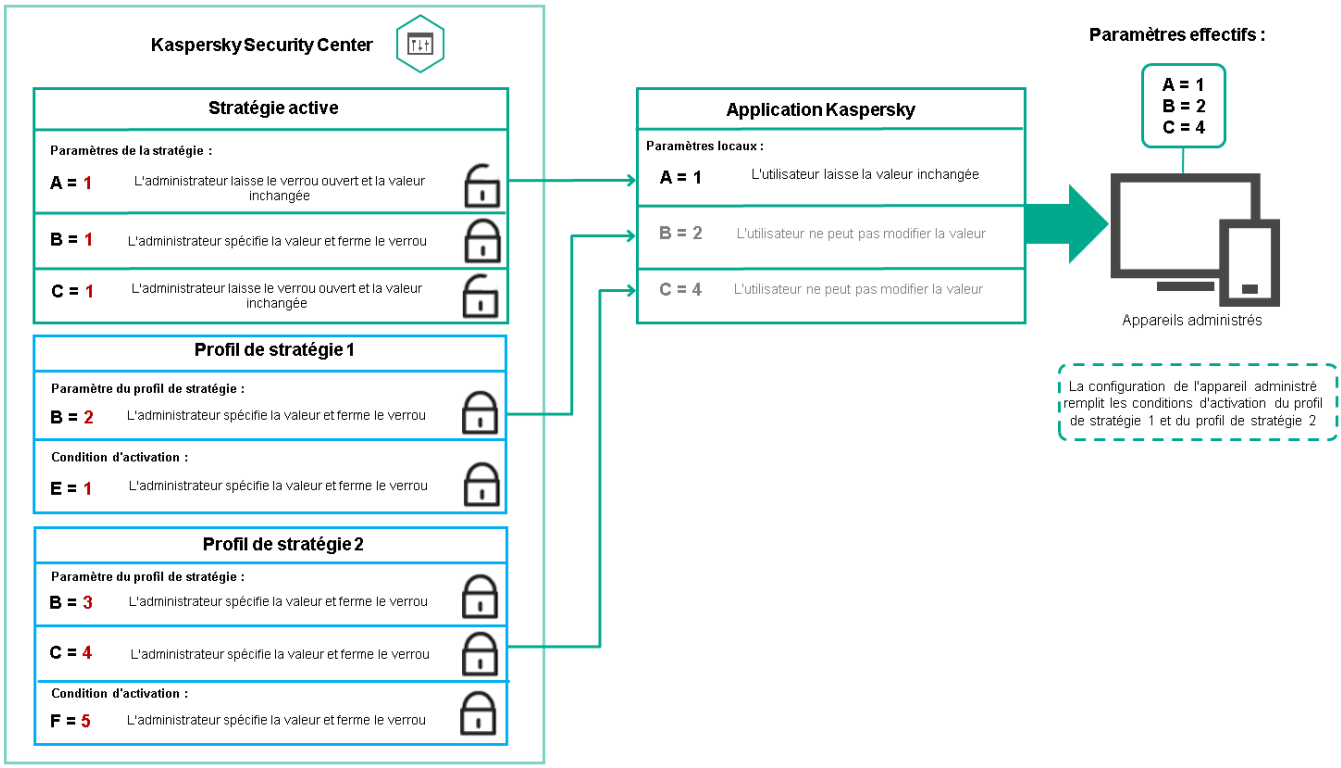
Les conditions d'attribution de priorité des profils de stratégie sont les suivantes :

- la position d'un profil dans une liste de profils de stratégie indique son degré de priorité. Vous pouvez modifier la priorité d'un profil de stratégie. La position la plus élevée dans une liste indique le degré de priorité le plus élevé (voir la figure ci-dessous).



Définition prioritaire d'un profil de stratégie

- Les conditions d'activation des profils de stratégie ne dépendent pas les unes des autres. Plusieurs profils de stratégie peuvent être activés simultanément. Si plusieurs profils de stratégie affectent le même paramètre, l'appareil sélectionne la valeur de paramètre du profil de stratégie dont la priorité est la plus élevée (voir la figure ci-dessous).



La configuration de l'appareil administré satisfait aux conditions d'activation de plusieurs profils de stratégie

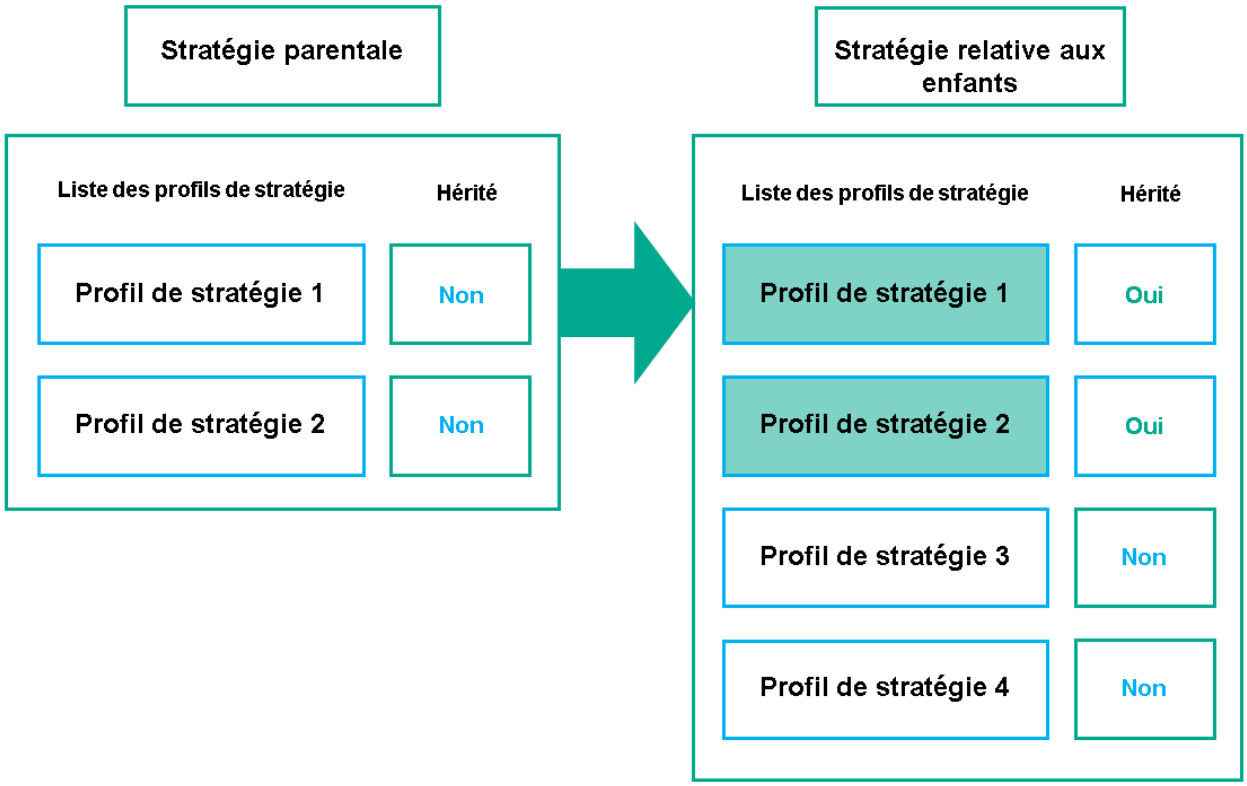
Profils de stratégie dans une hiérarchie d'héritage

Les profils de stratégie de différentes stratégies de niveau hiérarchique sont conformes aux conditions suivantes :

- une stratégie de niveau inférieur hérite des profils de stratégie d'une stratégie de niveau supérieur. Un profil de stratégie hérité d'une stratégie de niveau supérieur obtient une priorité plus élevée que le niveau du profil de

stratégie d'origine.

- Vous ne pouvez pas modifier la priorité d'un profil de stratégie hérité (voir la figure ci-dessous).

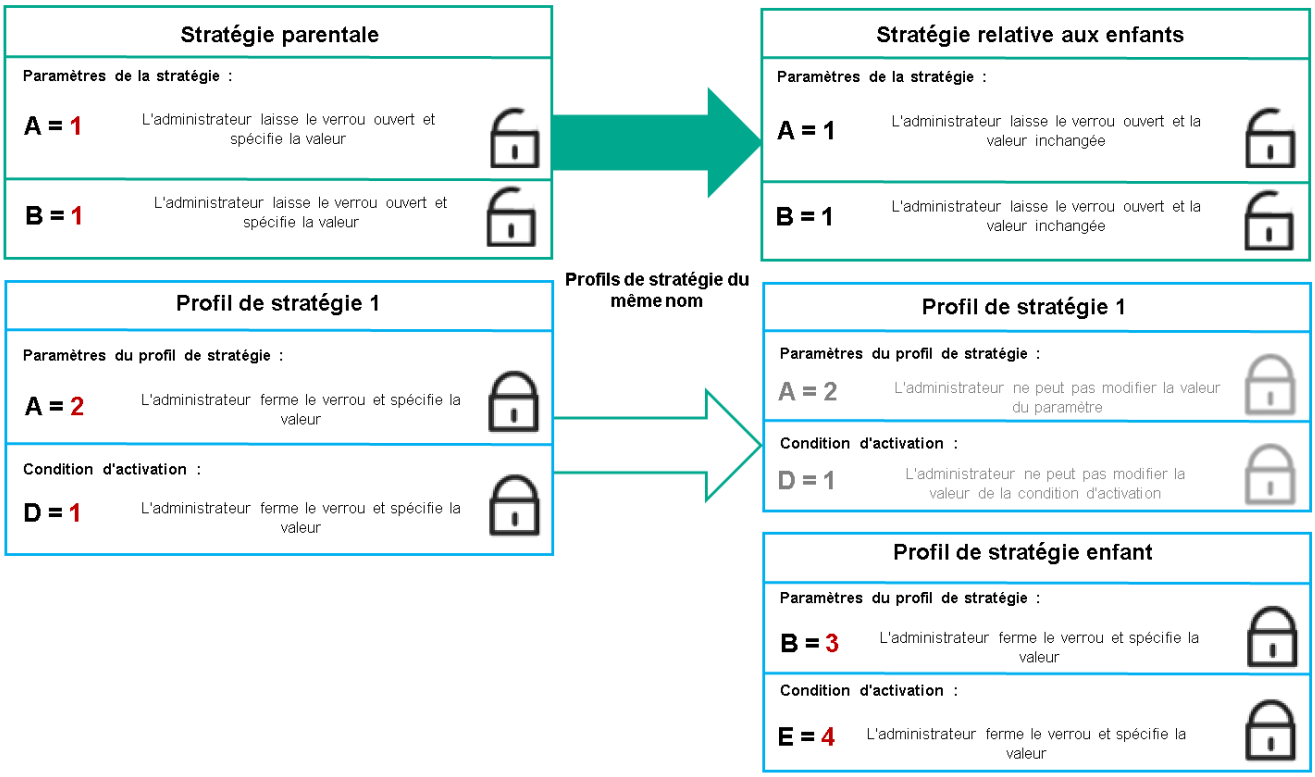


Héritage des profils de stratégie

Profils de stratégie du même nom

S'il existe, à des niveaux hiérarchiques différents, deux stratégies portant le même nom, leur fonctionnement est régi par les règles suivantes :

- Les paramètres verrouillés et la condition d'activation du profil d'un profil de stratégie de niveau supérieur modifient les paramètres et la condition d'activation de profil d'un profil de stratégie de niveau inférieur (voir la figure ci-dessous).



Le profil enfant hérite des valeurs de paramètres d'un profil de stratégie parent

- Les paramètres déverrouillés et la condition d'activation de profil d'un profil de stratégie de niveau supérieur ne modifient pas les paramètres et la condition d'activation de profil d'un profil de stratégie de niveau inférieur.

Comment les paramètres sont mis en œuvre sur un appareil administré

La mise en œuvre des paramètres effectifs sur un appareil administré peut être décrite comme suit :

- les valeurs de tous les paramètres qui n'ont pas été verrouillés sont tirées de la stratégie.
- Ils sont ensuite remplacés par les valeurs des paramètres de l'application administrée.
- Les valeurs des paramètres verrouillés de la stratégie effective sont ensuite appliquées. Les valeurs des paramètres verrouillés modifient celles des paramètres effectifs déverrouillés.

Administration des stratégies

Cette section décrit l'administration des stratégies et comporte des informations sur l'affichage de la liste des stratégies, l'élaboration d'une stratégie, sa modification, sa copie et son déplacement, la synchronisation forcée, l'affichage du graphique d'état de diffusion des stratégies et la suppression de stratégie.

Affichage de la liste des stratégies

Vous pouvez afficher la liste des stratégies créées pour le Serveur d'administration ou pour un groupe d'administration.

Pour consulter la liste des stratégies, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Hiérarchie des groupes**.
2. Dans la structure du groupe d'administration, sélectionnez le groupe d'administration dont vous voulez voir la liste des stratégies.

   La liste des stratégies s'affiche dans un tableau. S'il n'y a pas de stratégies, le tableau est vide. Vous pouvez afficher ou masquer les colonnes du tableau, modifier leur ordre, afficher uniquement les lignes qui contiennent une valeur que vous définissez, ou utiliser la recherche.

Création d'une stratégie

Vous pouvez créer des stratégies ; vous pouvez également modifier et supprimer des stratégies existantes.

> Vous ne pouvez pas créer de stratégie pour le Serveur d'administration.

Pour créer un de stratégie, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Stratégies et profils**.
2. Cliquez sur **Ajouter**.

   La fenêtre **Sélectionnez l'application** s'ouvre.
3. Sélectionnez l'application pour laquelle vous souhaitez créer une stratégie.
4. Cliquez sur **Suivant**.

   La fenêtre des paramètres de la nouvelle stratégie s'ouvre à l'onglet **Général**.
5. Si vous le souhaitez, modifiez le nom par défaut, l'état par défaut et les paramètres d'héritage par défaut pour la stratégie.
6. Cliquez sur 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.
7. 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).

   Les paramètres de l'application dépendent de l'application pour laquelle vous créez une stratégie. Pour plus de détails, reportez-vous à ce qui suit :

   - Configuration du Serveur d'administration
   - Paramètres de la stratégie de l'Agent d'administration
   - Documentation de Kaspersky Endpoint Security for Windows

Pour plus de détails sur les paramètres des autres programmes de protection, consultez la documentation du programme correspondant.

Pendant la modification des paramètres, vous pouvez cliquer sur **Annuler** pour annuler la dernière opération.

8. Cliquez sur **Enregistrer** afin d'enregistrer la stratégie.

Finalement, la stratégie ajoutée s'affiche dans la liste des stratégies.

Modification d'une stratégie

Pour modifier une stratégie, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Stratégies et profils**.
2. Cliquez sur la stratégie que vous souhaitez modifier.

   La fenêtre des paramètres de la stratégie s'ouvre.
3. Spécifiez les paramètres généraux et les paramètres de l'application pour laquelle vous créez une stratégie. Pour plus de détails, reportez-vous à ce qui suit :

   - Configuration du Serveur d'administration
   - Paramètres de la stratégie de l'Agent d'administration
   - Documentation de Kaspersky Endpoint Security for Windows

   Pour plus de détails sur les paramètres des autres applications de sécurité, consultez la documentation de l'application concernée.
4. Cliquez sur **Enregistrer**.

Les modifications de la stratégie seront enregistrées dans les propriétés de la stratégie et seront affichées dans la section **Historique des révisions**.

Paramètres généraux de la stratégie

Général

Sous l'onglet **Général**, vous pouvez modifier l'état de la stratégie et configurer l'héritage des paramètres de la stratégie :

- Le groupe **État de la stratégie** permet de sélectionner l'un des modes de stratégie :
  - **Actif**
  - **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

L'onglet **Configuration des événements** vous permet de configurer l'enregistrement des événements dans le journal et les notifications relatives à ceux-ci. Les événements sont répartis par niveau d'importance sur différents onglets :

- **Critique**

  La section **Critique** ne s'affiche pas dans les propriétés de la stratégie de l'Agent d'administration.

- **Erreur de fonctionnement**
- **Avertissement**
- **Information**

Dans chaque section, la liste reprend les types d'événements et la condition de stockage sur le serveur d'administration par défaut (en jours). Cliquez sur un type d'événement pour définir les paramètres suivants :

- **Enregistrement des événements**

Vous pouvez spécifier le nombre de jours de stockage de l'événement et sélectionner l'emplacement du stockage de l'événement :

- **Conserver dans la base de données du Serveur d'administration pendant (jours)**
- **Conserver dans le journal des événements du SE sur l'appareil**

- **Notifications d'événement**

  Vous pouvez choisir si vous souhaitez être averti de l'événement par email.

  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 dans l'onglet **Email**.

De plus, l'onglet **Configuration des événements** affiche une notification lorsque de nouveaux types d'événements sont ajoutés (par exemple, dans une nouvelle version du produit) 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 et de restaurer les modifications apportées à la stratégie, si nécessaire.

Activation et désactivation d'une option d'héritage de stratégie

Pour activer ou désactiver l'option d'héritage dans une stratégie :

1. ouvrez la stratégie concernée.
2. Ouvrez l'onglet **Général**.
3. Activez ou désactivez l'héritage de la stratégie :
   - si vous activez l'option **Hériter 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.
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 **Ressources (Appareils)** → **Stratégies et profils**.
2. Cochez la case en regard de la stratégie (ou des stratégies) que vous souhaitez copier.
3. Cliquez sur le bouton **Copier**.

   A droite de l'écran, l'arborescence des groupes d'administration s'affiche.
4. Dans l'arborescence, sélectionnez le groupe cible, à savoir le groupe dans lequel vous souhaitez copier la stratégie (ou les stratégies).
5. Cliquez sur le bouton **Copier** en bas de l'écran.
6. Cliquez sur le bouton **OK** pour confirmer l'opération.

La stratégie (les stratégies) sera (seront) copiée(s) dans le groupe cible avec tous ses profils. L'état de chaque stratégie copiée dans le groupe cible est **Inactive**. Vous pouvez remplacer l'état par **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.

Pour déplacer une stratégie vers un autre groupe d'administration, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Stratégies et profils**.
2. Cochez les cases en regard de la stratégie (ou des stratégies) que vous souhaitez déplacer.
3. Cliquez sur le bouton **Déplacer**.

   A droite de l'écran, l'arborescence des groupes d'administration s'affiche.
4. Dans l'arborescence, sélectionnez le groupe cible, à savoir le groupe dans lequel vous souhaitez déplacer la stratégie (ou les stratégies).
5. Cliquez sur le bouton **Déplacer** en bas de l'écran.
6. Cliquez sur le bouton **OK** pour confirmer l'opération.

Si une stratégie n'est pas héritée du groupe source, elle est déplacée vers le groupe cible avec tous ses profils. L'état de la stratégie dans le groupe cible est **Inactive**. Vous pouvez remplacer l'état par **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 Cloud Console vous permet d'enregistrer une stratégie, ses paramètres et les profils de stratégie dans un fichier KLP. Vous pouvez utiliser ce fichier KLP pour importer la stratégie enregistrée dans Kaspersky Security Center Windows et Kaspersky Security Center Linux.

Pour exporter une stratégie, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Stratégies et profils**.
2. Cochez la case en regard de la stratégie que vous souhaitez corriger.

   Vous ne pouvez pas exporter plusieurs stratégies à la fois. Si vous sélectionnez plusieurs stratégies, le bouton **Exporter** sera désactivé.
3. Cliquez sur le bouton **Exporter**.
4. Dans la fenêtre ouverte **Enregistrer sous**, indiquez le nom et le chemin du fichier de stratégie. Cliquez sur **Enregistrer**.

   La fenêtre **Enregistrer sous** s'affiche uniquement si vous utilisez Google Chrome, Microsoft Edge ou Opera. Si vous utilisez un autre navigateur, le fichier de stratégie est automatiquement enregistré dans le dossier **Téléchargements**.

Importation d'une stratégie

Kaspersky Security Center Cloud Console vous permet d'importer une stratégie à partir d'un fichier KLP. Le fichier KLP contient la stratégie exportée, ses paramètres et les profils de stratégie.

Pour importer une stratégie, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Stratégies et profils**.
2. Cliquez sur le bouton **Importer**.
3. Cliquez sur le bouton **Parcourir** pour choisir le fichier de stratégie à importer.
4. Dans la fenêtre qui s'ouvre, indiquez le chemin d'accès au fichier de stratégie KLP, puis cliquez sur le bouton **Ouvrir**. Notez que vous ne pouvez sélectionner qu'un seul fichier de stratégie.

   Le traitement de la stratégie démarre.
5. Une fois que la stratégie a été traitée avec succès, sélectionnez le groupe d'administration auquel vous souhaitez appliquer la stratégie.
6. Cliquez sur le bouton **Terminée** pour terminer l'importation de la stratégie.

La notification avec les résultats de l'importation s'affiche. Si la stratégie est importée avec succès, vous pouvez cliquer sur le lien **En savoir plus** pour afficher les propriétés de la stratégie.

Après une importation réussie, la stratégie s'affiche dans la liste des stratégies. Les paramètres et les profils de la stratégie sont également importés. Quel que soit l'état de la stratégie sélectionné lors de l'exportation, la stratégie importée est inactive. Vous pouvez modifier l'état de la stratégie dans les propriétés de la stratégie.

Si la stratégie importée porte le même nom que la stratégie existante, le nom de la stratégie importée est suivi de l'index **(<numéro de séquence suivant>)**, par exemple : **(1)**, **(2)**.

Affichage du graphique de l'état de la distribution des stratégies

Dans Kaspersky Security Center Cloud Console, vous pouvez afficher l'état de l'application de la stratégie sur chaque appareil dans un graphique de l'état de distribution des stratégies.

Pour afficher l'état de la distribution des stratégies sur chaque appareil, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Stratégies et profils**.
2. Cochez la case située à côté du nom de la stratégie dont vous souhaitez consulter l'état de la distribution sur les appareils.
3. Dans le menu qui s'affiche, cliquez sur le lien **Distribution**.

   La fenêtre **Résultats de distribution de la stratégie <Nom de la stratégie>** s'ouvre.
4. Dans la fenêtre **Résultats de distribution de la stratégie <Nom de la stratégie>** qui s'ouvre, la **Description de l'état (si disponible)** de la stratégie s'affiche.

Vous pouvez modifier le nombre de résultats affichés dans la liste avec la distribution des stratégies. Le nombre d'appareils maximal est égal à 100 000.

Pour modifier le nombre d'appareils affichés dans la liste avec les résultats de la distribution des stratégies, procédez comme suit :

1. Dans le menu principal, allez dans les paramètres de votre compte et puis sélectionnez **Options d'interface**.
2. Dans **Nombre maximal 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 "Propagation de virus", procédez comme suit :

1. Dans le menu principal, cliquez sur l'icône des paramètres ( ) en regard du nom du Serveur d'administration requis.

   La fenêtre des propriétés du Serveur d'administration s'ouvre 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 le bouton **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.

Synchronisation forcée

Malgré le fait que Kaspersky Security Center Cloud Console synchronise automatiquement l'état, les paramètres, les tâches et les stratégies pour les appareils administrés, il existe des cas où vous devez savoir exactement si la synchronisation a déjà eu lieu à un moment précis et pour un appareil en particulier.

Synchronisation d'un seul appareil

Pour forcer la synchronisation entre le Serveur d'administration et l'appareil administré, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Appareils administrés**.

2. Cliquez sur le nom de l'appareil que vous souhaitez synchroniser avec le Serveur d'administration.

La fenêtre des propriétés s'ouvre avec la section **Général** sélectionnée.

3. Cliquez sur le bouton **Forcer la synchronisation**.

L'application synchronise l'appareil administré avec le Serveur d'administration.

Synchronisation de plusieurs appareils

Pour forcer la synchronisation entre le Serveur d'administration et plusieurs appareils administrés, procédez comme suit :

1. Ouvrez la liste des appareils d'un groupe d'administration ou une sélection d'appareils :
   - Dans le menu principal, accédez à **Ressources (Appareils)** → **Appareils administrés** → **Groupes**, puis sélectionnez le groupe d'administration qui contient les appareils à synchroniser.
   - Exécutez une sélection d'appareils pour afficher la liste des appareils.
2. Cochez les cases en regard des appareils que vous souhaitez synchroniser avec le Serveur d'administration.
3. Cliquez 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, vous pouvez vérifier si la stratégie modifiée a été remise à un appareil administré défini. Une stratégie peut être remise lors d'une synchronisation normale ou forcée.

Pour voir la date et l'heure de remise d'une stratégie d'application sur un appareil administré, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Appareils administrés**.
2. Cliquez sur le nom de l'appareil que vous souhaitez synchroniser avec le Serveur d'administration.

   La fenêtre des propriétés s'ouvre avec la section **Général** sélectionnée.
3. Sélectionnez l'onglet **Applications**.
4. Sélectionnez l'application pour laquelle vous souhaitez consulter la date de synchronisation des stratégies.

La fenêtre de la stratégie de l'application s'ouvre avec la section **Général** sélectionnée, et affiche la date et l'heure de remise de la stratégie.

Suppression d'une stratégie

Vous pouvez supprimer une stratégie si vous n'en avez plus besoin. Vous pouvez supprimer uniquement une stratégie qui n'est pas héritée dans le groupe d'administration indiqué. Si une stratégie est héritée, vous ne pouvez la supprimer que dans le groupe de niveau supérieur pour lequel elle a été créée.

Pour supprimer une stratégie, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Stratégies et profils**.
2. Cochez la case en regard de la stratégie que vous voulez supprimer, puis cliquez sur **Supprimer ;**.

   Le bouton **Supprimer ;** devient indisponible (grisé) si vous sélectionnez une stratégie héritée.
3. Cliquez sur le bouton **OK** pour confirmer l'opération.

La stratégie est supprimée ainsi que tous ses profils.

Administration des profils de stratégies

Cette section décrit la gestion des profils de stratégie et comporte des informations sur l'affichage des profils d'une stratégie, le changement, la création, la modification ou la copie d'un profil de stratégie, la création d'une règle d'activation de profil de stratégie et la suppression de profil de stratégie.

Consultation des profils d'une stratégie

Pour consulter les profils d'une stratégie, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Stratégies et profils**.
2. Cliquez sur le nom de la stratégie dont vous souhaitez voir les profils.

   La fenêtre des propriétés de la stratégie s'ouvre à l'onglet **Général**.
3. Ouvrez l'onglet **Profils de stratégie**.

La liste des profils des stratégies s'affiche dans un tableau. Si la stratégie n'a pas de profils, un tableau vide s'affiche.

Modification de la priorité d'un profil de stratégie

Pour modifier la priorité d'un profil de stratégie, procédez comme suit :

1. Passez à la liste des profils d'une stratégie que vous voulez.

   La liste des profils de la stratégie s'ouvre.
2. Sous l'onglet **Profils de stratégie**, cochez la case en regard du profil de stratégie dont vous souhaitez modifier la priorité.

3. Définissez une nouvelle position du profil de stratégie dans la liste en cliquant sur **Augmenter la priorité** ou **Réduire la priorité**.

   Plus un profil de stratégie se trouve haut dans la liste, plus sa priorité est élevée.

4. Cliquez sur le bouton **Enregistrer**.

La priorité du profil de stratégie sélectionné est modifiée et appliquée.

Création d'un profil de stratégie

Pour créer un profil de stratégie, procédez comme suit :

1. Passez à la liste des profils d'une stratégie que vous voulez.

   La liste des profils de la stratégie s'ouvre. Si la stratégie n'a pas de profils, un tableau vide s'affiche.

2. Cliquez sur **Ajouter**.

3. Si vous le souhaitez, modifiez le nom par défaut et les paramètres d'héritage par défaut pour le profil.

4. Sélectionnez l'onglet **Paramètres de l'application**.

   Ou vous pouvez cliquer sur **Enregistrer** et quitter. Le profil que vous avez créé apparaît dans la liste des profils des stratégies et vous pouvez modifier ses paramètres ultérieurement.

5. Sous l'onglet **Paramètres de l'application**, sélectionnez dans le volet de gauche la catégorie que vous souhaitez, puis dans le panneau des résultats à droite, modifiez les paramètres du profil. Vous pouvez modifier les paramètres du profil de stratégie dans chaque catégorie (section).

   Pendant la modification des paramètres, vous pouvez cliquer sur **Annuler** pour annuler la dernière opération.

6. Cliquez sur le bouton **Enregistrer** afin d'enregistrer le profil.

Le profil apparaît dans la liste des profils des stratégies.

Modification du profil de stratégie

La modification d'un profil de stratégie est uniquement possible pour les stratégies de Kaspersky Endpoint Security for Windows.

Pour modifier un profil de stratégie, procédez comme suit :

1. Passez à la liste des profils d'une stratégie que vous voulez.

   La liste des profils de la stratégie s'ouvre.

2. Sous l'onglet **Profils de stratégie**, cliquez sur le profil de stratégie que vous souhaitez modifier.

   Cette action entraîne l'ouverture de la fenêtre des propriétés du profil de stratégie.

3. Configurez les paramètres du profil dans la fenêtre des propriétés :

- Si nécessaire, sous l'onglet **Général**, modifiez le nom du profil et activez ou désactivez le profil.
- Modifiez les règles d'activation du profil.
- Modifiez les paramètres de l'application.

Pour plus de détails sur les applications de sécurité, veuillez consulter la documentation de l'application correspondante.

4. Cliquez sur **Enregistrer**.

Les paramètres modifiés entrent en vigueur après la synchronisation de l'appareil avec le Serveur d'administration (si le profil de stratégie est actif), ou après l'exécution de la règle d'activation (si le profil de stratégie est inactif).

Copie d'un profil de stratégie

Vous pouvez copier un profil de stratégie dans la stratégie actuelle ou une autre, par exemple, si vous souhaitez avoir des profils identiques pour les différentes stratégies. Vous pouvez également utiliser la copie si vous avez deux ou plusieurs profils qui diffèrent seulement sur un petit nombre de paramètres.

Pour copier un profil de stratégie, procédez comme suit :

1. Passez à la liste des profils d'une stratégie que vous voulez.

   La liste des profils de la stratégie s'ouvre. Si la stratégie n'a pas de profils, un tableau vide s'affiche.

2. Sous l'onglet **Profils de stratégie**, cliquez sur le profil de stratégie que vous souhaitez copier.
3. Cliquez sur **Copier**.
4. Dans la fenêtre qui s'ouvre, sélectionnez la stratégie dans laquelle vous souhaitez copier le profil.

   Vous pouvez copier un profil de stratégie dans la même stratégie ou dans une stratégie que vous précisez.

5. Cliquez sur **Copier**.

Le profil de stratégie est copié dans la stratégie que vous avez sélectionnée. Le profil récemment copié obtient la priorité la plus basse. Si vous copiez le profil dans la même stratégie, la nom de la stratégie récemment copiée, le suffixe (), par exemple : (1), (2) est ajouté au profil récemment copié.

Ensuite, vous pouvez modifier les paramètres du profil, y compris son nom et sa priorité ; le profil de stratégie ne sera pas modifié dans ce cas.

Création d'une règle d'activation du profil de stratégie

Pour créer une règle d'activation du profil de stratégie, procédez comme suit :

1. Passez à la liste des profils d'une stratégie que vous voulez.

   La liste des profils de la stratégie s'ouvre.

2. Sous l'onglet **Profils de stratégie**, cliquez sur le profil de stratégie pour lequel vous devez créer une règle d'activation.

Si la liste des profils de stratégie est vide, vous pouvez créer le profil de stratégie.

3. Sous l'onglet **Règles d'activation**, cliquez sur le bouton **Ajouter**.

   La fenêtre avec des règles d'activation du profil de stratégie s'ouvre.

4. Définissez un nom pour la règle.

5. Cochez les cases en regard des conditions qui doivent influencer l'activation du profil de stratégie que vous créez :

   - **Règles générales d'activation du profil de stratégie**

     Cochez la case pour configurer les règles de l'activation du profil de stratégie sur l'appareil en fonction de l'état du mode déconnecté de l'appareil, de la règle de connexion de l'appareil au Serveur d'administration et des tags attribués à l'appareil.

     Définissez cette option à l'étape suivante :

     - **État de l'appareil**

       Définit la condition de la présence de l'appareil sur le réseau :

       - **En ligne** : L'appareil se trouve sur le réseau et le Serveur d'administration est donc accessible.
       - **Déconnecté** : L'appareil se trouve sur un réseau extérieur, c'est-à-dire que le Serveur d'administration n'est pas accessible.
       - **N/A** : Les critères ne sont pas appliqués.

     - **La règle pour la connexion du Serveur d'administration est active sur cet appareil**

       Choisissez la condition d'activation du profil de stratégie (si la règle est exécutée ou non) et sélectionnez le nom de la règle.

       La règle définit l'emplacement réseau de l'appareil pour la connexion au Serveur d'administration dont les conditions doivent être remplies (ou ne doivent pas être remplies) pour l'activation du profil de stratégie.

       La description de l'emplacement réseau de l'appareil pour la connexion au Serveur d'administration peut être créée ou configurée dans la règle de permutation de l'Agent d'administration.

   - **Règles d'un propriétaire particulier de l'appareil**

     Définissez cette option à l'étape suivante :

     - **Propriétaire de l'appareil**

Activez l'option pour configurer et activer une règle d'activation de profil sur l'appareil en fonction de son propriétaire. La liste déroulante située sous la case permet de sélectionner les critères d'activation du profil :

- L'appareil appartient au propriétaire indiqué (le symbole " = ").
- L'appareil n'appartient pas au propriétaire indiqué (le symbole " ≠ ").

  Notez que la liste des utilisateurs est filtrée et affiche les propriétaires d'appareils qui sont des utilisateurs internes.

  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 l'option pour configurer et activer la règle d'activation du profil sur l'appareil en fonction de l'appartenance de son propriétaire au groupe de sécurité interne de Kaspersky Security Center Cloud Console. 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 " ≠ ").

    Notez que la liste des utilisateurs est filtrée et affiche les propriétaires d'appareils qui sont des utilisateurs internes.

    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 Cloud Console. 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 :

  - Tags

    Définissez dans la liste des tags la règle d'inclusion des appareils dans le profil de stratégie en cochant la case des tags souhaités.

    Vous pouvez ajouter à la liste de nouveaux tags en les saisissant dans le champ sur la liste et en cliquant sur le bouton **Ajouter**.

    Le profil de stratégie reprendra les appareils dont la description reprend tous les tags sélectionnés. Si les cases sont décochées, les critères ne sont pas appliqués. Les cases sont décochées par défaut.

  - Appliquer aux appareils sans les tags sélectionnés

    Activez cette option s'il est nécessaire d'intervertir la sélection de tags.

    Si cette option est activée, les appareils sans tags sélectionnés seront inclus dans le profil de stratégie. Si l'option est désactivée, les critères ne sont pas appliqués.

    Cette option est Inactif par défaut.

- Règles d'utilisation d'Active Directory

Cochez la case pour configurer les règles d'activation du profil de stratégie sur l'appareil en fonction du placement de l'appareil dans une division Active Directory ou de l'appartenance de l'appareil ou du propriétaire de l'appareil au groupe de sécurité Active Directory.

Définissez cette option à l'étape suivante :

- Appartenance du propriétaire de l'appareil au groupe de sécurité Active Directory

  Si l'option est activée, le profil de stratégie est activé sur l'appareil dont le propriétaire est membre du groupe de sécurité indiqué. Si l'option est désactivée, les critères d'activation du profil ne sont pas appliqués. Cette option est Inactif par défaut.

- Appartenance de l'appareil au groupe de sécurité Active Directory

  Si cette option est activée, le profil de stratégie est activé sur l'appareil. Si l'option est désactivée, les critères d'activation du profil ne sont pas appliqués. Cette option est Inactif par défaut.

- Placement de l'appareil dans une unité organisationnelle Active Directory

  Si cette option est activée, le profil de stratégie est activé sur l'appareil figurant dans la sous-division Active Directory indiquée. Si l'option est désactivée, les critères d'activation du profil ne sont pas appliqués.

  Cette option est Inactif par défaut.

Le nombre de pages supplémentaires de l'assistant dépend des paramètres que vous sélectionnez à la première étape. Vous pouvez modifier les règles d'activation du profil de stratégie plus tard.

6. Consultez la liste des paramètres configurés. Si la liste est correcte, cliquez sur **Créer**.

Le profil est enregistré. Le profil sera activé sur l'appareil lors de l'application des règles d'activation.

Les règles d'activation du profil de stratégie créées pour le profil s'affichent dans les propriétés du profil de stratégie sous l'onglet **Règles d'activation**. Vous pouvez modifier ou supprimer la règle de l'activation du profil de stratégie.

Il est possible d'exécuter simultanément plusieurs règles d'activation.

Suppression d'un profil de stratégie

Pour supprimer un profil de stratégie, procédez comme suit :

1. Passez à la liste des profils d'une stratégie que vous voulez.

   La liste des profils de la stratégie s'ouvre.

2. Sous l'onglet **Profils de stratégie**, cochez la case en regard du profil de stratégie que vous souhaitez supprimer, puis cliquez sur **Supprimer**.

3. Dans la fenêtre qui s'ouvre, cliquez une nouvelle fois sur **Supprimer ;**.

Le profil de stratégie est supprimé. Si la stratégie est héritée d'un groupe de niveau inférieur, le profil reste dans ce groupe, mais devient le profil de la stratégie de ce groupe. Cela permet d'éliminer les changements importants au niveau des paramètres des applications administrées installées sur les appareils des groupes de niveau inférieur.

Chiffrement et protection des données

Le chiffrement des données diminue les risques de fuite d'informations en cas de vol ou de perte d'un ordinateur portable ou d'un disque dur, ou en cas d'accès aux données par des utilisateurs et des applications non autorisés.

L'utilisation du chiffrement est prise en charge par les applications suivantes de Kaspersky :

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Mac

Vous pouvez afficher ou masquer certains des éléments d'interface liés à la fonction de gestion du chiffrement à l'aide des paramètres de l'interface utilisateur.

Chiffrement des données dans Kaspersky Endpoint Security for Windows

Vous pouvez administrer la technologie Chiffrement de disque BitLocker sur les appareils fonctionnant sous le système d'exploitation Windows pour les serveurs ou les postes de travail.

À l'aide de ces modules de Kaspersky Endpoint Security for Windows, vous pouvez, par exemple, activer ou désactiver le chiffrement, consulter la liste des disques chiffrés ou générer et consulter des rapports sur le chiffrement.

Vous configurez le chiffrement en définissant les stratégies de Kaspersky Endpoint Security for Windows dans Kaspersky Security Center Cloud Console. Kaspersky Endpoint Security for Windows effectue le chiffrement et le déchiffrement conformément à la stratégie active. Les instructions détaillées sur la configuration des règles et la description des fonctionnalités de chiffrement sont disponibles dans l'aide de Kaspersky Endpoint Security for Windows.

Chiffrement des données dans Kaspersky Endpoint Security for Mac

Vous pouvez utiliser le chiffrement FileVault sur les appareils exécutant macOS. Lorsque vous travaillez avec Kaspersky Endpoint Security for Mac, vous pouvez activer ou désactiver ce chiffrement.

Vous configurez le chiffrement en définissant les stratégies de Kaspersky Endpoint Security for Mac dans Kaspersky Security Center Cloud Console. Kaspersky Endpoint Security for Mac effectue le chiffrement et le déchiffrement conformément à la stratégie active. Pour obtenir la description détaillée des fonctionnalités de chiffrement, consultez l'aide de Kaspersky Endpoint Security for Mac.

Consultation de la liste des disques chiffrés

Dans Kaspersky Security Center Cloud Console, vous pouvez afficher les détails des disques chiffrés et des appareils chiffrés au niveau du lecteur. Une fois que les informations sur le disque sont déchiffrées, celui-ci sera automatiquement supprimé de la liste.

Pour consulter la liste des disques chiffrés,

Dans le menu principal, accédez à **Opérations → Chiffrement et protection des données → Disques chiffrés**.

Si la section ne figure pas dans le menu, cela signifie qu'elle est masquée. Dans les paramètres de l'interface utilisateur, activez l'option **Afficher le chiffrement et la protection des données** pour afficher la section.

Vous pouvez exporter la liste des disques chiffrés dans un fichier CSV ou TXT. Pour ce faire, cliquez sur le bouton **Exporter vers un fichier CSV** ou **Exporter vers un fichier TXT**.

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 et rapports → Rapports**. Vous pouvez également générer les rapports de chiffrement suivants dans la section **Opérations → Chiffrement et protection des données** :

- Rapport de l'état de chiffrement des appareils de stockage 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 le menu principal, accédez à **Opérations → Chiffrement et protection des données**.

3. Ouvrez la section **Disques chiffrés** pour générer le rapport sur l'état du chiffrement des appareils de stockage de masse ou le rapport sur les droits d'accès aux disques chiffrés.

4. Cliquez sur le nom du rapport que vous souhaitez générer.

La création du rapport démarre.

Accorder l'accès à un disque chiffré en mode déconnecté

Un utilisateur peut demander l'accès à un appareil chiffré, par exemple, lorsque Kaspersky Endpoint Security for Windows n'est pas installé sur l'appareil administré. Après avoir reçu la demande, vous pouvez créer un fichier de clé d'accès et l'envoyer à l'utilisateur. Tous les cas d'utilisation et les instructions détaillées sont fournis dans l'aide de Kaspersky Endpoint Security for Windows.

Pour accorder l'accès à un disque chiffré en mode déconnecté, procédez comme suit :

1. Obtenez une demande d'accès au fichier d'un utilisateur (fichier avec l'extension FDERTC). Suivez les instructions de l'aide de Kaspersky Endpoint Security for Windows pour générer le fichier dans Kaspersky Endpoint Security for Windows.

2. Dans le menu principal, accédez à **Opérations → Chiffrement et protection des données → Disques chiffrés**.

   Une liste des disques chiffrés s'affiche.

3. Sélectionnez le disque pour lequel l'utilisateur a demandé l'accès.

4. Cliquez sur le bouton **Autoriser l'accès à l'appareil en mode déconnecté**.

5. Dans la fenêtre qui s'ouvre, sélectionnez le plug-in correspondant à l'application Kaspersky utilisée pour chiffrer le disque sélectionné.

   > Si un disque est chiffré avec une application Kaspersky non prise en charge par Kaspersky Security Center Cloud Console, utilisez la Console d'administration Microsoft Management Console pour accorder l'accès en mode déconnecté.

6. Suivez les instructions fournies dans l'aide de Kaspersky Endpoint Security for Windows (voir les blocs d'extension à la fin de la section).

Après cela, l'utilisateur applique le fichier reçu pour accéder au disque chiffré et lire les données stockées sur le disque.

Utilisateurs et rôles d'utilisateurs

Cette section décrit les utilisateurs et les rôles d'utilisateurs et explique comment les créer et les modifier, comment affecter des rôles et des groupes à des utilisateurs et comment associer des profils de stratégie à des rôles.

À propos des comptes utilisateurs

Kaspersky Security Center Cloud Console permet d'administrer les comptes utilisateurs et groupes de comptes. L'application prend en charge trois types de comptes utilisateur :

- Comptes utilisateur pour les employés de l'entreprise. Le Serveur d'administration reçoit les données relatives aux comptes utilisateur de ces utilisateurs de domaine lors du balayage du controleur de domaine de l'entreprise.
- Comptes des utilisateurs locaux. Les comptes locaux des appareils administrés, ainsi que les comptes locaux de l'appareil sur lequel le Serveur d'administration est installé.
- Comptes des utilisateurs internes de Kaspersky Security Center Cloud Console. Vous pouvez créer des comptes d'utilisateurs internes. Ces comptes sont utilisés uniquement dans Kaspersky Security Center Cloud Console.

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. Par défaut, le tableau ouvert est filtré en fonction des colonnes **Sous-type** ou **Possède des rôles**. Le tableau affiche les utilisateurs ou groupes internes auxquels des rôles ont été attribués.

Si vous souhaitez consulter le tableau avec uniquement les comptes des utilisateurs locaux, définissez les critères de filtre du **Sous-type** sur **Local**.

Si vous passez au Serveur d'administration secondaire 14.2 ou antérieure et que vous ouvrez la liste des utilisateurs ou des groupes de sécurité, le tableau ouvert sera filtré uniquement en fonction de la colonne **Sous-type**. Le filtre selon la colonne **Possède des rôles** ne sera pas appliqué par défaut. Le tableau filtré contiendra tous les utilisateurs ou groupes de sécurité internes avec et sans le rôle attribué.

Ajout d'un compte d'un utilisateur interne

Si vous le voulez, vous pouvez ajouter des utilisateurs internes de votre espace de travail sur le portail. Après avoir ajouté un utilisateur interne, vous pouvez lui attribuer un rôle dans Kaspersky Security Center Cloud Console.

À propos des rôles d'utilisateurs

Un *rôle d'utilisateur* (ou un *rôle*) est un objet qui contient un ensemble de privilèges. Un rôle peut être associé aux paramètres des applications de Kaspersky installées sur l'appareil de l'utilisateur. Vous pouvez attribuer un rôle à un ensemble d'utilisateurs ou à un ensemble de groupes de sécurité à n'importe quel niveau de la hiérarchie des groupes d'administration, des Serveurs d'administration ou au niveau d'objets spécifiques.

Si vous administrez les appareils via une hiérarchie de Serveurs d'administration comprenant des Serveurs d'administration virtuels, notez que vous ne pouvez créer, modifier ou supprimer des rôles d'utilisateur qu'à partir d'un Serveur d'administration physique. Ensuite, vous pouvez propager les rôles d'utilisateurs sur les Serveurs d'administration secondaires, y compris les serveurs virtuels.

Vous pouvez associer des rôles d'utilisateurs aux profils des stratégies. Si un rôle est attribué à un utilisateur, cet utilisateur obtient les paramètres de sécurité dont il a besoin pour remplir ses fonctions.

Un rôle d'utilisateur peut être associé à des utilisateurs d'appareils dans un groupe d'administration défini.

Portée du rôle d'utilisateur

La *portée du rôle d'utilisateur* est un ensemble d'utilisateurs et de groupes d'administration. Les paramètres associés à un rôle d'utilisateur s'appliquent uniquement aux appareils qui appartiennent aux utilisateurs qui ont ce rôle et uniquement si ces appareils appartiennent aux groupes associés à ce rôle, y compris les groupes enfant.

Avantage de l'utilisation de rôles

Un des avantages liés à l'utilisation de rôles est qu'il n'est pas nécessaire de définir les paramètres de sécurité pour chacun des appareils administrés ou pour chaque utilisateur individuellement. Le nombre d'utilisateurs et d'appareils au sein d'une entreprise peut être relativement élevé, mais le nombre de différentes fonctions qui requièrent différents paramètres de sécurité est quant à lui considérablement plus réduit.

Différences par rapport à l'utilisation de profils des stratégies

Les profils des stratégies désignent des propriétés d'une stratégie qui est créée pour chaque application de Kaspersky séparément. Un rôle est associé à de nombreux profils des stratégies créés pour différentes applications. Par conséquent, un rôle est une manière de réunir en un endroit les paramètres pour un certain type d'utilisateur.

Configuration des droits d'accès aux fonctionnalités de l'application. Restriction d'accès selon un rôle

Kaspersky Security Center Cloud Console fournit des possibilités d'accès selon un rôle aux fonctionnalités de Kaspersky Security Center Cloud Console et des applications Kaspersky administrées.

Vous pouvez configurer les droits d'accès aux fonctionnalités de l'application pour les utilisateurs de Kaspersky Security Center Cloud Console 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 Cloud Console avec les droits d'accès pour gérer les tâches associées, les rapports, les paramètres et effectuer les actions utilisateur associées.

Pour exécuter les actions utilisateur répertoriées dans le tableau, un utilisateur doit avoir le droit spécifié en regard de l'action.

Les droits de **lecture**, d'**écriture** et d'**exécution** s'appliquent à toute tâche, rapport ou paramètre. En plus de ces droits, un utilisateur doit disposer du droit **Effectuer des opérations sur les sélections d'appareils** pour gérer les tâches, les rapports ou les paramètres sur les sélections d'appareils.

La zone fonctionnelle **Fonctionnalités générales** : **Accéder aux objets quel que soit leur ACL** est conçue à des fins d'audit. Lorsque les utilisateurs disposent des droits de **lecture** dans cette zone fonctionnelle, ils bénéficient d'un accès complet en **lecture** à tous les objets et peuvent exécuter toutes les tâches créées sur une sélection d'appareils connectés au Serveur d'administration via l'Agent d'administration avec des privilèges d'administrateur local (root pour Linux). Nous vous recommandons d'octroyer ces droits avec précaution et à un nombre limité d'utilisateurs qui en ont besoin pour l'accomplissement de leurs tâches officielles.

Toutes les tâches, rapports, paramètres et paquets d'installation qui manquent dans le tableau appartiennent à la zone fonctionnelle **Fonctionnalités générales : Fonctionnalité de base**.

Droits d'accès aux fonctionnalités de l'application

Zone fonctionnelle	Droit	Action utilisateur : droit requis pour exécuter l'action	Tâche	Rapport	Autres
Caractéristiques générales : **Gestion des groupes d'administration**	**Écrire**	• Ajouter un appareil à un groupe d'administration : **Écrire** • Supprimer un appareil d'un groupe d'administration : **Écrire** • Ajouter un groupe d'administration à un autre groupe d'administration : **Écrire** • Supprimer un groupe d'administration d'un autre groupe d'administration : **Écrire**	Aucun	Aucun	Aucun
Caractéristiques générales : **Accéder aux objets, quel que soit leur ACL**	**Lecture**	Obtenir un accès en lecture à tous les objets : **Lire**	Aucun	Aucun	L'accès est accordé indépendamment des autres droits, même s'ils interdisent l'accès en lecture à des objets particuliers.
Caractéristiques générales : **Fonctionnalité de base**	• **Lecture** • **Écrire** • **Exécuter** • **Effectuer des opérations sur les sélections d'appareils**	• Règles de déplacement des appareils (création, modification ou suppression) pour le Serveur virtuel : **Écrire**, **Effectuer des opérations sur les sélections d'appareils** • Certificat personnalisé du protocole Get Mobile (LWNGT) : **Lire**	• " Télécharger les mises à jour dans le stockage du Serveur d'administration " • "Livrer des rapports" • "Diffusion du paquet d'installation"	• "Rapport sur l'état de la protection" • "Rapport sur les menaces" • "Rapport sur les appareils les plus infectés"	Aucun

		• Définir le certificat personnalisé du protocole mobile (LWNGT) : **Écrire** • Obtenir la liste des réseaux définis par NLA : **Lire** • Ajouter, modifier ou supprimer une liste de réseaux définie par NLA : **Écrire** • Afficher la liste de contrôle d'accès des groupes : **Lire** • Afficher le journal des événements Kaspersky : **Lire**	• "Installation des applications sur les Serveurs d'administration secondaires à distance"	• "Rapport sur l'état des bases antivirus" • "Rapport sur les erreurs" • "Rapport sur les attaques réseau" • " Rapport de synthèse sur les applications de sécurité des systèmes de messagerie installées " • " Rapport de synthèse sur les applications de défense de périmètre installés " • "Rapport de synthèse sur les types d'application installés" • " Rapport sur les utilisateurs des appareils infectés " • " Rapport sur les problèmes de sécurité " • " Rapport sur les événements " • " Rapport de fonctionnement des Points de distribution " • " Rapport sur les Serveurs d'administration secondaires " • " Rapport sur les événements du Contrôle des appareils " • "Rapport sur les vulnérabilités" • "Rapport sur les applications interdites" • "Rapport sur le fonctionnement du Contrôle Internet" • " Rapport de l'état de chiffrement des appareils administrés "	

				• " Rapport de l'état de chiffrement des appareils de stockage de masse " • " Rapport sur les erreurs de chiffrement des fichiers " • " Rapport sur le blocage de l'accès aux fichiers chiffrés " • " Rapport sur les privilèges d'accès aux appareils chiffrés " • " Rapport sur les droits effectifs de l'utilisateur " • "Rapport sur les privilèges"	
Caractéristiques générales : **Objets supprimés**	• **Lecture** • **Écrire**	• Afficher les objets supprimés dans la corbeille : **Lire** • Supprimer des objets de la corbeille : **Écrire**	Aucun	Aucun	Aucun
Caractéristiques générales : **Traitement des événements**	• **Supprimer des événements** • **Modifier les paramètres de notification d'événement** • **Modifier les paramètres de journalisation des événements** • **Écrire**	• Modifier les paramètres d'enregistrement des événements : **Modifier les paramètres de journalisation des événements** • Modifier les paramètres de notification d'événements **Modifier les paramètres de notification d'événements** • Supprimer des événements : **Supprimer des événements**	Aucun	Aucun	Paramètres : • Paramètres de propagation de virus : nombre de détections de virus nécessaires pour créer un événement d'épidémie virale • Paramètres de propagation de virus : période de temps pour l'évaluation des détections de virus • Le nombre maximal d'événements stockés dans la base de données • Période de stockage des événements

					des appareils supprimés
Caractéristiques générales : **Déploiement de logiciels 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 "
Fonctionnalités générales : **Gestion des clés de licence**	• **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 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**	Aucun	Aucun	Aucun

		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	" Rapport sur les résultats de l'installation des mises à jour du logiciel tiers "	Aucun
Caractéristiques générales : Gestion des clés de chiffrement	**Écrire**	Importer les clés de chiffrement : **Écrire**	Aucun	Aucun	Aucun
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 : **Inventaire matériel**	• **Lecture** • **Écrire** • **Exécuter**	• Obtenir ou exporter un objet d'inventaire matériel : **Lire** • Ajouter, définir ou supprimer un objet	Aucun	• " Rapport sur le registre du matériel " • " Rapport sur les changements	Aucun

	• **Effectuer des opérations sur les sélections d'appareils**	d'inventaire matériel : **Écrire**		de configuration " • " Rapport sur le matériel "	
Gestion du système : **Contrôle d'accès au réseau**	• **Lecture** • **Écrire**	• Afficher les paramètres CISCO : **Lire** • Modifier les paramètres CISCO : **Écrire**	Aucun	Aucun	Aucun
Gestion du système : **Déploiement du système d'exploitation**	• **Déploiement des serveurs PXE** • **Lecture** • **Écrire** • **Exécuter** • **Effectuer des opérations sur les sélections d'appareils**	• Déployer les serveurs PXE : **Déployer les serveurs PXE** • Afficher une liste de serveurs PXE : **Lire** • Démarrer ou arrêter le processus d'installation sur les clients PXE : **Exécuter** • Gérer les pilotes pour WinPE et les images du système d'exploitation : **Écrire**	" Créer un paquet d'installation sur l'image du système d'exploitation de l'appareil de référence "	Aucun	Paquet d'installation : " OS Image "
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**	• " Synchronisation de Windows Update " • " Installer les mises à jour de Windows Update " • " Corriger les vulnérabilités " • "Installation des mises à jour requises et correction des vulnérabilités"	"Rapport sur les mises à jour des logiciels"	Aucun
Gestion du système : **Installation à distance**	• **Lecture** • **Écrire** • **Exécuter** • **Effectuer des opérations sur les sélections d'appareils**	• Afficher les propriétés du paquet d'installation tiers basé sur la gestion des vulnérabilités et des correctifs : **Lire** • Modifier les propriétés du paquet d'installation tiers basé sur la gestion des vulnérabilités et des correctifs : **Écrire**	Aucun	Aucun	Paquets d'installation : • " Application personnalisée " • " Paquet VAPM "
Gestion du système : **Inventaire des logiciels**	• **Lecture** • **Écrire** • **Exécuter** • **Effectuer des opérations sur les sélections d'appareils**	Aucun	Aucun	• " Rapport sur les applications installées " • " Rapport sur l'historique du registre des applications " • " Rapport sur l'état des	Aucun

				groupes des applications sous licence " • " Rapport sur les clés de licence des applications tierces "	

À propos des rôles d'utilisateurs prédéfinis

Les rôles d'utilisateurs attribués aux utilisateurs de Kaspersky Security Center Cloud Console 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 et configurer vous-même les droits requis. Certains des rôles d'utilisateurs prédéfinis disponibles dans Kaspersky Security Center Cloud Console peuvent être associés à des fonctions spécifiques, par exemple, **Auditeur**, **Responsable de la sécurité**, **Superviseur** (ces rôles sont présents dans Kaspersky Security Center Cloud Console à partir de la version 11). Les droits d'accès de ces rôles sont préconfigurés conformément aux tâches standard et à l'étendue des tâches des fonctions associées. Le tableau ci-dessous montre comment les rôles suivants peuvent être associés à des fonctions spécifiques.

Exemples de rôles pour des fonctions particulières

Rôle	Commentaire
Auditeur	Ceci autorise toutes les opérations avec tous les types de rapports, toutes les opérations de visualisation, y compris la visualisation des objets supprimés (accorde les droits de **Lire** et **Écrire** dans la zone **Objets supprimés**). Ceci n'autorise pas les autres opérations. Vous pouvez attribuer ce rôle à une personne qui réalise un audit de votre organisation.
Superviseur	Autorise toutes les opérations d'affichage, n'autorise pas les autres opérations. Vous pouvez attribuer ce rôle à un responsable de la sécurité et à d'autres responsables chargé de la sécurité de l'information dans votre organisation.
Responsable de la sécurité	Autorise toutes les informations de consultation, autorise la gestion des rapports, octroie des permissions restreintes dans les domaines **Administration du système** : **Connectivité**. Vous pouvez attribuer ce rôle à la personne chargée de la sécurité de l'information dans votre organisation.

Le tableau ci-dessous montre les droits d'accès attribués à chaque rôle d'utilisateur prédéfini.

Droits d'accès des rôles utilisateur prédéfinis

Rôle	Description

Administrateur du Serveur d'administration	Permet toutes les opérations dans les domaines fonctionnels suivants :
	• **Caractéristiques générales** :
	  • **Fonctionnalité de base**
	  • **Traitement des événements**
	  • **Hiérarchie des Serveurs d'administration**
	  • **Serveurs d'administration virtuels**
	• **Administration du système :**
	  • **Connectivité**
	  • **Inventaire du matériel**

	• **Inventaire des applications** Accorde les droits de **lecture** et d'**écriture** dans la zone fonctionnelle **Caractéristiques générales : Gestion des clés de chiffrement**.

Opérateur du Serveur d'administration	Accorde les droits de **lecture** et d' **exécution** dans tous les domaines fonctionnels suivants :
	• **Caractéristiques générales** :
	  • **Fonctionnalité de base**
	  • **Serveurs d'administration virtuels**
	• **Administration du système :**
	  • **Connectivité**
	  • **Inventaire du matériel**
	  • **Inventaire des applications**

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 :
	• **Caractéristiques générales** :
	  • **Fonctionnalité de base**
	  • **Déploiement de logiciels Kaspersky**
	  • **Gestion des clés de licence**
	• **Administration du système :**
	  • **Déploiement du système d'exploitation**
	  • **Gestion des vulnérabilités et des correctifs**
	  • **Installation à distance**
	  • **Inventaire des applications**
	
	Accorde les droits de **lecture** et d'**exécution** dans la zone fonctionnelle **Fonctionnalités générales : Serveurs d'administration virtuelle**.

Opérateur d'installation	Accorde les droits de **lecture** et d' **exécution** dans tous les domaines fonctionnels suivants :
	• **Caractéristiques générales** :
	  • **Fonctionnalité de base**
	  • **Déploiement de logiciels Kaspersky** (accorde également les **correctifs Manage Kaspersky** directement dans cette zone)
	  • **Serveurs d'administration virtuels**
	• **Administration du système :**
	  • **Déploiement du système d'exploitation**
	  • **Gestion des vulnérabilités et des correctifs**
	  • **Installation à distance**
	  • **Inventaire des applications**

Administrateur	Permet toutes les opérations dans les domaines fonctionnels suivants :

Kaspersky Endpoint Security	• **Caractéristiques générales : fonctionnalité de base** • Zone Kaspersky Endpoint Security, y compris toutes les fonctionnalités Accorde les droits de **lecture** et d'**écriture** dans la zone fonctionnelle **Caractéristiques générales : Gestion des clés de chiffrement**.
Opérateur Kaspersky Endpoint Security	Accorde les droits de **lecture** et d' **exécution** dans tous les domaines fonctionnels suivants : • **Caractéristiques générales : fonctionnalité de base** • Zone Kaspersky Endpoint Security, y compris toutes les fonctionnalités
Administrateur principal	Permet toutes les opérations dans les domaines fonctionnels, *à l'exception* des zones suivantes dans **Fonctions générales** : • **Accéder aux objets quel que soit leur ACL** • **Administration des rapports mise en œuvre** Accorde les droits de **lecture** et d'**écriture** dans la zone fonctionnelle **Caractéristiques générales : Gestion des clés de chiffrement**.

Opérateur principal	Accorde les droits de **lecture** et d' **exécution** (le cas échéant) dans tous les domaines fonctionnels suivants :
	• **Caractéristiques générales** :
	  • **Fonctionnalité de base**
	  • **Objets supprimés**
	  • **Opérations sur le Serveur d'administration**
	  • **Déploiement de l'application Kaspersky**
	  • **Serveurs d'administration virtuels**
	• **Administration des appareils mobiles : généralités**
	• **Gestion du système**, y compris toutes les fonctionnalités
	• Zone Kaspersky Endpoint Security, y compris toutes les fonctionnalités

Administrateur Administration des appareils mobiles	Permet toutes les opérations dans les domaines fonctionnels suivants : • **Caractéristiques générales : fonctionnalité de base** • **Administration des appareils mobiles : généralités**
Opérateur Administration des appareils mobiles	Accorde les droits de **lecture** et d'**exécution** dans la zone fonctionnelle **Fonctionnalités générales** : **Fonctionnalité de base**. Accorde des commandes de **lecture** et d'**envoi uniquement d'informations aux appareils mobiles** dans la zone fonctionnelle **Administration des appareils mobiles** : **Général**.
Responsable de la sécurité	Autorise toutes les opérations dans les domaines fonctionnels suivants, dans **Fonctions générales** : • **Accéder aux objets quel que soit leur ACL** • **Administration des rapports mise en œuvre** Accorde les droits **Lire**, **Écrire**, **Exécuter**, **Enregistrer les fichiers des appareils sur le poste de travail de l'administrateur** et **Réaliser des opérations sur les sélections d'appareils** dans la zone fonctionnelle **Administration du système : Connectivité**. Vous pouvez attribuer ce rôle à la personne chargée de la sécurité de l'information dans votre organisation.
Analyste de sécurité principal	Accorde les droits de **lecture** dans la zone fonctionnelle **Fonctionnalités générales** : **Fonctionnalité de base**. Accorde les droits **Lire**, **Écrire**, **Exécuter**, **Enregistrer les fichiers des appareils sur le poste de travail de l'administrateur** et **Réaliser des opérations sur les sélections d'appareils dans la zone fonctionnelle Administration du système** : **Connectivité**. Accorde les droits d'accès à la solution Kaspersky Endpoint Detection and Response Expert.
Utilisateur du Self Service Portal	Autorise toutes les opérations dans la zone fonctionnelle **Administration des appareils mobiles : Self Service Portal**. Cette fonctionnalité n'est pas prise en charge par Kaspersky Security Center 11 ni par les versions ultérieures.

Superviseur	Accorde le droit de **lecture** dans les **fonctionnalités générales** : **objets d'accès quelles que soient leurs ACL** et **fonctionnalités générales** : **Administration des rapports mise en œuvre**. Vous pouvez attribuer ce rôle à un responsable de la sécurité et à d'autres responsables chargé de la sécurité de l'information dans votre organisation.
Administrateur de gestion des vulnérabilités et des correctifs	Permet toutes les opérations dans les zones fonctionnelles **Fonctionnalités générales** : **Fonctionnalité de base** et **Gestion du système** (y compris toutes les fonctionnalités).
Opérateur de gestion des vulnérabilités et des correctifs	Accorde les droits de **lecture** et d'**exécution** (le cas échéant) dans les zones fonctionnelles **Fonctionnalités générales** : **Fonctionnalités de base** et **Gestion du système** (y compris toutes les fonctionnalités).

Attribution de droits d'accès à des objets spécifiques

Outre l'attribution de droits d'accès au niveau du serveur, vous pouvez configurer l'accès à des objets spécifiques, par exemple, à une tâche spécifique. L'application permet de définir les droits d'accès aux types d'objets suivants :

- Groupes d'administration
- Tâches
- Rapports
- Sélections d'appareils
- Sélections d'événements

Pour attribuer des droits d'accès à un objet spécifique, procédez comme suit :

1. Selon le type d'objet, dans le menu principal, accédez à la section correspondante :
   - **Ressources (Appareils) → Hiérarchie des groupes**
   - **Ressources (Appareils) → Tâches**
   - **Surveillance et rapports → Rapports**
   - **Ressources (Appareils) → Sélections d'appareils**
   - **Surveillance et rapports → Sélections d'événements**
2. Ouvrez les propriétés de l'objet pour lequel vous souhaitez configurer les droits d'accès.

   Pour ouvrir la fenêtre des propriétés d'un groupe d'administration ou d'une tâche, cliquez sur le nom de l'objet. Les propriétés d'autres objets peuvent être ouvertes à l'aide du bouton de la barre d'outils.
3. Dans la fenêtre des propriétés, ouvrez la section **Privilèges d'accès**.

   La liste des utilisateurs s'ouvre. Les utilisateurs et les groupes de sécurité répertoriés disposent de droits d'accès à l'objet. Par défaut, si vous utilisez une hiérarchie de groupes d'administration ou de Serveurs, la liste et les droits d'accès sont hérités du groupe d'administration parent ou du Serveur primaire.
4. Pour pouvoir modifier la liste, activez l'option **Utiliser des autorisations personnalisées**.
5. Configurez les droits d'accès :
   - Utilisez les boutons **Ajouter** et **Supprimer** pour modifier la liste.

- Spécifiez les droits d'accès pour un utilisateur ou un groupe de sécurité. Exécutez une des actions suivantes :

  - Si vous souhaitez définir les droits d'accès manuellement, sélectionnez l'utilisateur ou le groupe de sécurité, cliquez sur le bouton **Privilèges d'accès**, puis indiquez les droits d'accès.

  - Si vous souhaitez attribuer un rôle utilisateur à l'utilisateur ou au groupe de sécurité, sélectionnez l'utilisateur ou le groupe de sécurité, cliquez sur le bouton **Rôles**, puis sélectionnez le rôle à attribuer.

6. Cliquez sur le bouton **Enregistrer**.

Les droits d'accès à l'objet sont configurés.

Attribution de droits d'accès aux utilisateurs et aux groupes de sécurité

Vous pouvez octroyer aux utilisateurs et aux groupes de sécurité des droits d'accès pour utiliser différentes fonctionnalités du Serveur d'administration, par exemple, Kaspersky Endpoint Security for Linux.

Pour attribuer des droits d'accès à un utilisateur ou à un groupe de sécurité :

1. Dans le menu principal, cliquez sur l'icône des paramètres ( ) en regard du nom du Serveur d'administration requis.

   La fenêtre des propriétés du Serveur d'administration s'ouvre.

2. Sous l'onglet **Privilèges d'accès**, cochez la case en regard du nom de l'utilisateur ou du groupe de sécurité auquel attribuer des droits, puis cliquez sur le bouton **Privilèges d'accès**.

   Vous ne pouvez pas sélectionner plusieurs utilisateurs ou groupes de sécurité en même temps. Si vous sélectionnez plusieurs éléments, le bouton **Privilèges d'accès** sera désactivé.

3. Configurez l'ensemble des droits pour l'utilisateur ou le groupe :

   a. Développez le nœud avec les fonctionnalités du Serveur d'administration ou d'une autre application Kaspersky.

   b. Cochez la case **Autoriser** ou **Interdire** en regard de la fonctionnalité ou du droit d'accès souhaité.

      Exemple 1: cochez la case **Autoriser** en regard du nœud **Intégration des applications** pour accorder tous les droits d'accès disponibles à la fonctionnalité d'intégration d'application (**Lecture**, **Écriture** et **Exécution**) pour un utilisateur ou un groupe.

      Exemple 2: développez le nœud **Gestion des clés de chiffrement**, puis cochez la case **Autoriser** en regard de l'autorisation d'**écriture** pour accorder le droit d'accès en **écriture** à la fonctionnalité de gestion des clés de chiffrement pour un utilisateur ou un groupe.

4. Après avoir configuré l'ensemble des droits d'accès, cliquez sur **OK**.

L'ensemble des privilèges pour les utilisateurs ou les groupes d'utilisateurs sont alors configurés.

Les permissions du Serveur d'administration (ou du groupe d'administration) sont réparties dans les catégories suivantes :

- Fonctions générales :

  - Administration des groupes d'administration

- Accéder aux objets quel que soit leur ACL
- Fonctionnalité de base
- Objets supprimés
- Gestion des clés de chiffrement
- Traitement des événements
- Opérations 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 un droit d'accès, ce droit est considérée comme *non défini* : il persiste tant qu'il n'a pas été explicitement autorisé ou interdit pour l'utilisateur.

Les privilèges d'un utilisateur sont la somme des éléments suivants :

- Propres privilèges de l'utilisateur
- Privilèges de tous les rôles attribués à cet utilisateur
- Privilèges de tous les groupe de sécurité auxquels l'utilisateur appartient
- Les privilèges de tous les rôles attribués aux groupes de sécurité auxquels l'utilisateur appartient

Si au moins un de ces ensembles de privilèges a la valeur **Interdire** pour une permission, celle-ci n'est pas accordée à l'utilisateur, même si d'autres ensembles l'autorisent ou ne la définissent pas.

Vous pouvez également ajouter des utilisateurs et des groupes de sécurité à la portée d'un rôle d'utilisateur pour utiliser les différentes fonctionnalités du Serveur d'administration. Les paramètres associés à un rôle d'utilisateur s'appliqueront uniquement aux appareils qui appartiennent aux utilisateurs qui ont ce rôle et uniquement si ces appareils appartiennent aux groupes associés à ce rôle, y compris les groupes enfant.

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**.

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 le bouton **Enregistrer** afin d'enregistrer les modifications.

Le nouveau rôle apparaît dans la liste des rôles des utilisateurs.

Modification d'un rôle d'utilisateur

Pour modifier un rôle d'utilisateur, procédez comme suit :

1. Dans le menu principal, accédez à **Utilisateurs et rôles** → **Rôles**.
2. Cliquez sur le nom du rôle que vous souhaitez modifier.
3. Dans la fenêtre des propriétés du rôle qui s'ouvre, modifiez les paramètres du rôle :
   - Sous l'onglet **Général**, modifiez le nom du rôle.
     Il est impossible de modifier le nom d'un rôle système.
   - Sous l'onglet **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 le bouton **Enregistrer** afin d'enregistrer les modifications.

Le rôle mis à jour apparaît dans la liste des rôles des utilisateurs.

Modification de la zone d'action d'un rôle d'utilisateur

La *portée du rôle d'utilisateur* est un ensemble d'utilisateurs et de groupes d'administration. Les paramètres associés à un rôle d'utilisateur s'appliquent uniquement aux appareils qui appartiennent aux utilisateurs qui ont ce rôle et uniquement si ces appareils appartiennent aux groupes associés à ce rôle, y compris les groupes enfant.

Pour ajouter des utilisateurs, des groupes d'utilisateurs 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 d'utilisateurs 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 d'utilisateurs 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. Fermez la fenêtre des propriétés du rôle.

Les utilisateurs ou groupes d'utilisateurs sélectionnés et le groupe d'administration sélectionné sont ajoutés à la portée du rôle d'utilisateur.

Méthode 3 :

1. Dans le menu principal, cliquez sur l'icône des paramètres ( ) en regard du nom du Serveur d'administration requis.

   La fenêtre des propriétés du Serveur d'administration s'ouvre.

2. Sous l'onglet **Privilèges d'accès**, cochez la case en regard du nom de l'utilisateur ou du groupe de sécurité que vous souhaitez ajouter à la portée du rôle de l'utilisateur, puis cliquez sur le bouton **Rôles**.

   Vous ne pouvez pas sélectionner plusieurs utilisateurs ou groupes de sécurité en même temps. Si vous sélectionnez plusieurs éléments, le bouton **Rôles** sera désactivé.

3. Dans la fenêtre **Rôles**, sélectionnez le rôle d'utilisateur que vous souhaitez attribuer, puis cliquez sur **OK** pour enregistrer les modifications.

   Les utilisateurs ou les groupes de sécurité sélectionnés sont ajoutés à la portée du rôle d'utilisateur.

Suppression d'un rôle d'utilisateur

Pour supprimer un rôle d'utilisateur, procédez comme suit :

1. Dans le menu principal, accédez à **Utilisateurs et rôles** → **Rôles**.
2. Cochez la case en regard du nom du rôle que vous souhaitez supprimer.
3. Cliquez sur **Supprimer**.
4. Dans la fenêtre qui s'ouvre, cliquez sur **OK**.

Le rôle d'utilisateur est supprimé.

Association des profils des stratégies aux rôles

Vous pouvez associer des rôles d'utilisateurs aux profils des stratégies. Dans ce cas, la règle d'activation pour ce profil de stratégie repose sur le rôle : le profil de stratégie devient actif pour un utilisateur qui a le rôle indiqué.

Par exemple, la stratégie interdit les logiciels de navigation GPS pour tous les appareils du groupe d'administration. Les applications de navigation urbaine sont seulement nécessaires au fonctionnement d'un appareil de l'utilisateur jouant le rôle de livreur, dans le groupe d'administration " Utilisateurs ". Dans ce cas, vous pouvez attribuer un rôle de " messager " à son propriétaire, puis créer un profil de stratégie qui autorise l'exécution d'un logiciel de navigation par satellite uniquement sur les appareils dont les propriétaires ont reçu le rôle " Messager ". Tous les autres paramètres de la stratégie sont préservés. Seul l'utilisateur qui a reçu le rôle " Messager " pourra exécuter un logiciel de navigation par satellite. Ensuite, si un autre employé reçoit le rôle " Messager ", il pourra également exécuter le logiciel de navigation sur l'appareil de votre entreprise. L'exécution d'un logiciel de navigation par satellite sera toujours interdite sur les autres appareils au sein du même groupe d'administration.

Pour associer un rôle à un profil de stratégie :

1. Dans le menu principal, accédez à **Utilisateurs et rôles** → **Rôles**.
2. Cliquez sur le nom d du rôle que vous souhaitez associer à un profil de stratégie.

   La fenêtre des propriétés du rôle s'ouvre à l'onglet **Général**.
3. Sélectionnez l'onglet **Configuration** et passez à la section **Stratégies et profils**.
4. Cliquez sur **Modifier**.
5. Pour associer le rôle à :

   - **Un profil de stratégie existant** : Cliquez sur l'icône de chevron (>) en regard du nom de la stratégie requise, puis cochez la case en regard du profil auquel vous souhaitez associer le rôle.
   - **Un nouveau profil de stratégie** :

a. Cochez la case en regard de la stratégie pour laquelle vous souhaitez créer un profil.

b. Cliquez sur **Nouveau profil de stratégie**.

c. Indiquez un nom pour le nouveau profil et configurez les paramètres du profil.

d. Cliquez sur le bouton **Enregistrer**.

e. Cochez la case en regard du nouveau profil.

6. Cliquez sur **Attribuer au rôle**.

Le profil est associé au rôle et apparaît dans les propriétés du rôle. Le profil s'applique alors automatiquement à tout appareil dont le propriétaire possède ce rôle.

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 **Créer un groupe**.

3. Dans la fenêtre **Créer un groupe**, définissez les paramètres suivants pour le nouveau groupe de sécurité :

   - **Nom**

   - **Description**

4. Cliquez sur le bouton **OK** afin d'enregistrer les modifications.

Un nouveau groupe de sécurité est ajouté à la liste des groupes de sécurité.

Modification d'un groupe de sécurité

Pour modifier un groupe de sécurité, procédez comme suit :

1. Dans le menu principal, accédez à **Utilisateurs et rôles** → **Utilisateurs et groupes**, puis sélectionnez l'onglet **Groupes**.

2. Cliquez sur le nom du groupe de sécurité que vous souhaitez modifier.

3. Dans la fenêtre des paramètres de groupe qui s'ouvre, modifiez les paramètres du groupe de sécurité :

   - Sous l'onglet **Général**, vous pouvez modifier les paramètres **Nom** et **Description**. Ces paramètres sont disponibles uniquement pour les groupes de sécurité internes.

   - L'onglet **Utilisateurs** permet d'ajouter des utilisateurs au groupe de sécurité. Ce paramètre est disponible uniquement pour les utilisateurs internes et les groupes de sécurité internes.

- Sous l'onglet **Rôles**, vous pouvez attribuer le rôle au groupe de sécurité.

4. Cliquez sur le bouton **Enregistrer** afin d'enregistrer les modifications.

Les modifications sont appliquées au groupe de sécurité.

Ajout de comptes utilisateurs à un groupe interne

Vous ne pouvez ajouter des comptes utilisateurs internes qu'à un groupe interne.

Pour ajouter des comptes utilisateurs à un groupe 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.
3. Cliquez sur le bouton **Attribuer un groupe**.
4. Dans la fenêtre **Attribuer un groupe** qui s'ouvre, sélectionnez le groupe auquel vous voulez ajouter des comptes utilisateurs.
5. Cliquez sur le bouton **Désigner**.

Les comptes utilisateurs sont ajoutés au groupe. Vous pouvez également ajouter des utilisateurs internes à un groupe à l'aide des paramètres du groupe.

Suppression d'un groupe de sécurité

Vous ne pouvez supprimer que les groupes de sécurité internes.

Pour supprimer un groupe d'utilisateur, procédez comme suit :

1. Dans le menu principal, accédez à **Utilisateurs et rôles** → **Utilisateurs et groupes**, puis sélectionnez l'onglet **Groupes**.
2. Cochez les cases en regard du groupe d'utilisateur que vous souhaitez supprimer.
3. Cliquez sur **Supprimer**, puis confirmez la suppression dans la fenêtre ouverte.

Le groupe d'utilisateur est supprimé.

Configuration de l'intégration ADFS

Pour permettre aux utilisateurs enregistrés dans Active Directory (AD) au sein de votre organisation de se connecter à Kaspersky Security Center Cloud Console, vous devez configurer l'intégration avec Active Directory Federation Services (AD FS).

Kaspersky Security Center Cloud Console prend en charge AD FS 3 (Windows Server 2016) ou une version ultérieure. AD FS doit être publié et disponible sur Internet. En tant que service, le certificat de communication AD FS utilise un certificat de confiance publique.

Pour modifier les paramètres d'intégration AD FS, vous devez disposer du droit d'accès vous permettant de modifier les autorisations des utilisateurs.

Avant de continuer, assurez-vous d'avoir terminé le sondage Active Directory.

Pour configurer l'intégration d'AD FS, procédez comme suit :

1. Dans le menu principal, cliquez sur l'icône des paramètres ( ) à côté du nom du Serveur d'administration.

   La fenêtre des propriétés du Serveur d'administration s'ouvre.

2. Sous l'onglet **Général**, sélectionnez la section **Paramètres d'intégration ADFS**.

3. Copiez l'URL de rappel.

   Vous aurez besoin de cette URL pour configurer l'intégration dans AD FS Management Console.

4. Dans AD FS Management Console, ajoutez un nouveau groupe d'applications, puis ajoutez une nouvelle application en sélectionnant le modèle **Application serveur** (les noms des éléments de l'interface Microsoft sont fournis en anglais.).

   AD FS Management Console génère un identifiant de client pour la nouvelle application. Vous aurez besoin de l'identifiant de client pour configurer l'intégration dans Kaspersky Security Center Cloud Console.

5. En tant qu'URI de redirection, indiquez l'URL de rappel que vous avez copiée dans la fenêtre des propriétés du Serveur d'administration.

6. Générez un secret de client. Vous aurez besoin du secret de client pour configurer l'intégration dans Kaspersky Security Center Cloud Console.

7. Enregistrez les propriétés de l'application ajoutée.

8. Ajoutez une nouvelle application au groupe d'applications créé. Cette fois, sélectionnez le modèle **API Web**.

9. Sous l'onglet **Identifiants**, ajoutez l'identifiant de client de l'application de serveur que vous avez ajoutée auparavant à la liste **Identifiants de partie de confiance**.

10. Sous l'onglet **Autorisations des clients**, dans la liste **Zones autorisées**, sélectionnez les zones **allatclaims** et **openid**.

11. Sous l'onglet **Règles de transformation d'émission**, ajoutez une nouvelle règle en sélectionnant le modèle **Envoyer les attributs LDAP en tant que revendications** :

    a. Attribuez un nom à la règle. Par exemple, vous pouvez la nommer " Groupe SID ".

    b. Sélectionnez **Active Directory** en tant que magasin d'attributs, puis mappez **Groupes de jetons en tant que SID** en tant qu'attribut LDAP à " Groupe SID " en tant que type de revendication sortante.

12. Sous l'onglet **Règles de transformation d'émission**, ajoutez une nouvelle règle en sélectionnant le modèle **Envoyer des revendications à l'aide d'une règle personnalisée** :

    a. Attribuez un nom à la règle. Par exemple, vous pouvez la nommer " ActiveDirectoryUserSID ".

    b. Dans le champ **Règle personnalisée**, saisissez ce qui suit :

    ```
    c:[Type ==
    "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname",
    Issuer == "AD AUTHORITY"] => issue(store = "Active Directory", types =
    ("http://schemas.microsoft.com/ws/2008/06/identity/claims/primarysid"), query =
    ";objectSID;{0}", param = c.Value);
    ```

13. Dans Kaspersky Security Center Cloud Console, ouvrez de nouveau la section **Paramètres d'intégration ADFS**.

14. Basculez le commutateur sur **Intégration ADFS Activé**.

15. Cliquez sur le lien **Paramètres**, puis indiquez le fichier qui contient le certificat ou plusieurs certificats pour le serveur de fédération.

16. Cliquez sur le lien **Paramètres d'intégration ADFS**, puis définissez les paramètres suivants :

- URL de l'émetteur

  L'URL du serveur de fédération fonctionnant dans votre organisation.

  Kaspersky Security Center Cloud Console ajoute notamment " /.well-known/openid-configuration " à l'URL de l'émetteur et essaie d'ouvrir l'URL résultante (issuer_URL/.well-known/openid-configuration) pour découvrir la configuration de l'émetteur automatiquement.

- ID du client

  Identifiant de client généré par le serveur de fédération pour identifier Kaspersky Security Center Cloud Console. Vous pouvez trouver l'identifiant de client dans AD FS Management Console, dans la fenêtre des propriétés de l'application de serveur qui correspond à Kaspersky Security Center Cloud Console.

- Secret du client

  Vous générez un secret de client dans AD FS Management Console lorsque vous définissez les propriétés de l'application de serveur qui correspond à Kaspersky Security Center Cloud Console.

- Domaine à partir duquel authentifier les utilisateurs

  Les membres du domaine que vous sélectionnez pourront se connecter à Kaspersky Security Center Cloud Console avec leurs identifiants du compte de domaine. Les noms de domaine s'affichent dans la liste une fois que le sondage du réseau est terminé.

- Nom du champ pour le SID de l'utilisateur dans le jeton d'identification

  Nom du champ qui fait référence au SID de l'utilisateur dans le jeton d'identification. Le nom du champ est obligatoire pour identifier l'utilisateur dans Kaspersky Security Center Cloud Console. Par défaut, ce champ dans le jeton d'identification est appelé " primarysid ".

- Nom du champ pour le tableau des SID des groupes de l'utilisateur dans le jeton d'identification

  Nom du champ qui fait référence à l'ensemble de SID des groupes de sécurité Active Directory dans lequel l'utilisateur est inclus. Par défaut, ce champ dans le jeton d'identification est appelé " groupsid ".

17. Cliquez sur le bouton **Enregistrer**.

L'intégration avec AD FS est terminée. Pour vous connecter à Kaspersky Security Center Cloud Console à l'aide des identifiants d'un compte AD, utilisez le lien fourni dans la section **Paramètres d'intégration ADFS** (**Lien de connexion à Kaspersky Security Center Cloud Console avec ADFS**).

Lorsque vous vous connectez à Kaspersky Security Center Cloud Console via AD FS pour la première fois, la console peut réagir avec un certain retard.

Configuration de l'intégration avec Microsoft Entra ID

Vous devez configurer l'intégration avec Microsoft Entra ID pour permettre aux utilisateurs de votre organisation de se connecter à Kaspersky Security Center Cloud Console à l'aide des identifiants de leur compte Microsoft Entra ID.

L'intégration avec Microsoft Entra ID est disponible uniquement pour le Serveur d'administration principal. Vous ne pouvez pas configurer l'intégration pour les Serveurs d'administration virtuels ou secondaires.

Pour configurer l'intégration avec Microsoft Entra ID, procédez comme suit :

1. Dans le menu principal, cliquez sur l'icône des paramètres ( ) à côté du nom du Serveur d'administration.

   La fenêtre des propriétés du Serveur d'administration s'ouvre.

2. Sous l'onglet **Général**, sélectionnez la section **Microsoft Entra ID**.

3. Activez le commutateur **Intégration de Microsoft Entra ID**.

4. Copiez les liens des champs suivants :

   - **URL de rappel**
   - **URL de déconnexion du canal frontal**

     Vous aurez besoin de ces URL pour enregistrer Kaspersky Security Center Cloud Console dans le locataire Microsoft Entra ID.

   - **URL de connexion**

     Vous aurez besoin de cette URL pour permettre aux utilisateurs de se connecter à l'espace de travail de Kaspersky Security Center Cloud Console avec leurs identifiants Microsoft Entra ID une fois l'intégration avec Microsoft Entra ID terminée.

5. Connectez-vous au centre d'administration Microsoft Entra, puis sélectionnez le locataire de votre organisation.

Vous devez disposer du rôle Administrateur général ou Administrateur des applications pour le locataire.

6. Dans le menu principal, sélectionnez **Identité** → **Applications** → **Inscriptions d'applications**, puis cliquez sur le bouton **Nouvelle inscription**.

7. Dans la fenêtre qui s'ouvre, procédez comme suit :

   - Définissez un nom pour l'application Kaspersky Security Center Cloud Console.
   - Dans la section **Types de comptes pris en charge**, sélectionnez l'option **Comptes dans ce répertoire de l'organisation uniquement (<nom_locataire> uniquement – locataire unique)**.
   - Dans la section **URL de redirection**, sélectionnez **Internet** dans la liste déroulante, puis saisissez l'URL de rappel que vous avez copiée depuis Kaspersky Security Center Cloud Console à l'étape 4.

8. Cliquez sur le bouton **Enregistrer**.

   L'application Kaspersky Security Center Cloud Console est enregistrée dans Microsoft Entra ID et la page de présentation de l'application s'ouvre.

9. Si nécessaire, ajoutez Kaspersky Security Center Cloud Console à la liste des applications.

   Les utilisateurs pourront ouvrir Kaspersky Security Center Cloud Console en cliquant sur son nom dans la liste des applications dans Mes applications et le lanceur Office 365 sans utiliser l'URL de connexion.

10. Copiez l'**identifiant de l'application (client)** et l'**identifiant du répertoire (locataire)**, et enregistrez-les de la manière qui vous convient le mieux.

    Vous en aurez besoin pour remplir les champs obligatoires dans Kaspersky Security Center Cloud Console à l'étape 14.

11. Dans le menu de l'application Kaspersky Security Center Cloud Console, accédez à la section **Authentification**, puis saisissez les URL que vous avez copiées depuis Kaspersky Security Center Cloud Console à l'étape 4 :

    - Dans la section **Web**, cliquez sur le bouton **Ajouter une URI**, puis saisissez l'URL de connexion.
    - Dans la section **URL de déconnexion de la chaîne principale**, saisissez l'URL de déconnexion de la chaîne principale.

12. Dans le menu de l'application Kaspersky Security Center Cloud Console, accédez à la section **Certificats et secrets**, puis procédez comme suit :

    a. Accédez à l'onglet **Secrets client**, puis cliquez sur le bouton **Nouveau secret client**.

    b. Dans la fenêtre qui s'ouvre, indiquez une toute description nécessaire pour le secret client, puis sélectionnez la période à l'issue de laquelle le secret expirera.

    Nous vous recommandons de copier la date d'expiration du secret, de la manière qui vous convient le mieux, afin d'assurer l'alternance des secrets en temps utile.

    a. Cliquez sur le bouton **Ajouter**.

    Le secret créé s'affiche dans l'onglet **Secrets client**.

    b. Copiez les informations de la colonne **Valeur**.

Nous vous recommandons vivement de copier les informations immédiatement après la création du secret client.

13. Dans le menu de l'application Kaspersky Security Center Cloud Console, accédez à la section **Configuration du jeton**, puis procédez comme suit :

    - Ajoutez la revendication facultative **onprem_sid** :

      a. Cliquez sur le bouton **Ajouter une revendication facultative**.

      b. Dans la fenêtre qui s'ouvre, sélectionnez le type de jeton **Identifiant**, puis dans la colonne **Revendication**, cochez la case en regard de **onprem_sid**.

      c. Cliquez sur le bouton **Ajouter**.

      La requête facultative **onprem_sid** s'affiche sur la page **Revendications facultatives**.

    - Ajoutez la revendication facultative **favorite_username** :

      a. Cliquez sur le bouton **Ajouter une revendication facultative**.

      b. Dans la fenêtre qui s'ouvre, sélectionnez le type de jeton **Accès**, puis dans la colonne **Revendication**, cochez la case en regard de **favorite_username**.

      c. Cliquez sur le bouton **Ajouter**.

      La revendication facultative **favorite_username** s'affiche sur la page **Revendications facultatives**.

14. Dans le menu de l'application Kaspersky Security Center Cloud Console, accédez à la section **Autorisations API**, puis ajoutez les autorisations :

    - **User.Read.All**
    - **User.Export.All**
    - **GroupMember.Read.All**
    - **Directory.Read.All**

    Pour ajouter une autorisation, procédez comme suit :

    a. Cliquez sur le bouton **Ajouter une autorisation**, puis sélectionnez l'onglet **API Microsoft**.

    b. Sélectionnez **Graphique Microsoft → Autorisations de l'application**, puis sélectionnez l'autorisation que vous souhaitez ajouter.

    c. Cliquez sur le bouton **Ajouter une autorisation**.

    Les quatre autorisations sont ajoutées et affichées sur la page **Autorisations configurées**.

    d. Cliquez sur le **bouton Accorder le consentement de l'administrateur pour <tenant_name>**, puis dans la fenêtre qui s'ouvre, cliquez sur **Oui** pour confirmer l'octroi des autorisations que vous avez ajoutées.

15. Revenez à Kaspersky Security Center Cloud Console et, dans l'onglet **Général**, remplissez les champs obligatoires suivants :

- **ID du locataire**. L'**identifiant du répertoire (locataire)** que vous avez copié à l'étape 10.
- **ID du client**. L'**identifiant de l'application (client)** que vous avez copié à l'étape 10.
- **Secret du client**. La valeur que vous avez copiée à l'étape 12.

16. Cliquez sur le bouton **Analyser la connexion** pour vérifier si les paramètres sont corrects, puis après l'affichage de l'état **Connecté**, cliquez sur le bouton **Enregistrer**.

Les paramètres d'intégration sont enregistrés et l'intégration avec Microsoft Entra ID est configurée.

Une fois que vous avez configuré l'intégration avec Microsoft Entra ID, vous devez effectuer les opérations suivantes :

1. Dans le menu principal de Kaspersky Security Center Cloud Console, accédez à **Utilisateurs et rôles** → **Utilisateurs et groupes** pour vous assurer que les utilisateurs et les groupes de Microsoft Entra ID sont bien ajoutés à Kaspersky Security Center Cloud Console.

   Si les utilisateurs et les groupes de votre client Microsoft Entra ID sont synchronisés à partir d'Active Directory dans votre organisation et que le sondage Active Directory est configuré, les utilisateurs et les groupes ont déjà été ajoutés à Kaspersky Security Center Cloud Console à la suite du sondage Active Directory.

   Dans le cas contraire, vous devez activer et exécuter le sondage Microsoft Entra ID pour ajouter les utilisateurs et les groupes de votre locataire Microsoft Entra ID à Kaspersky Security Center Cloud Console.

2. Attribuez les rôles nécessaires aux utilisateurs et aux groupes.

   Lors de l'attribution de rôles à un utilisateur sur un Serveur d'administration virtuel, dans le menu principal, accédez à **Utilisateurs et rôles** → **Utilisateurs et groupes**, puis sélectionnez l'onglet **Utilisateurs**. Si vous sélectionnez l'onglet **Groupes**, puis que vous attribuez des rôles au groupe dont l'utilisateur est membre, l'utilisateur ne pourra pas se connecter à Kaspersky Security Center Cloud Console.

3. Envoyez l'URL de connexion que vous avez copiée à l'étape 4 aux utilisateurs. Ils saisiront cette URL pour **se connecter à l'espace de travail Kaspersky Security Center Cloud Console à l'aide de leurs identifiants Microsoft Entra ID**.

   Lorsque un utilisateur se déconnecte du compte Microsoft Entra ID qu'il a utilisé pour s'authentifier dans Kaspersky Security Center Cloud Console et que Kaspersky Security Center Cloud Console est ouvert dans un autre onglet ou dans une autre fenêtre du même navigateur, la session se termine également pour Kaspersky Security Center Cloud Console, et l'utilisateur se déconnecte automatiquement de la console.

   Si Kaspersky Security Center Cloud Console est ouvert dans un autre navigateur ou sur différents appareils, la session se poursuit lorsque l'utilisateur se déconnecte du compte Microsoft Entra ID.

Pour se connecter à Kaspersky Security Center Cloud Console avec les identifiants du compte Microsoft Entra ID, l'utilisateur doit pouvoir se connecter à son compte Microsoft Entra ID.

Activation du sondage Microsoft Entra ID

Vous devez activer le sondage Microsoft Entra ID pour ajouter des utilisateurs à partir de Microsoft Entra ID vers Kaspersky Security Center Cloud Console.

Pour activer le sondage Microsoft Entra ID, procédez comme suit :

1. Dans le menu principal, cliquez sur l'icône des paramètres ( ) à côté du nom du Serveur d'administration.

   La fenêtre des propriétés du Serveur d'administration s'ouvre.

2. Sous l'onglet **Général**, sélectionnez la section **Microsoft Entra ID**.

3. Dans la section **Découverte des utilisateurs**, activez le commutateur **Sondage Microsoft Entra ID**.

4. Si vous souhaitez modifier la planification par défaut du sondage, cliquez sur le bouton **Paramètres de la programmation**, indiquez la fréquence et l'heure du sondage dans la fenêtre qui s'ouvre, puis cliquez sur le bouton **Enregistrer**.

   Le sondage Microsoft Entra ID s'exécutera selon la planification que vous avez configurée.

5. Si vous souhaitez lancer immédiatement le sondage Microsoft Entra ID, cliquez sur le bouton **Exécuter maintenant**.

   Le chargement du fichier utilisateurs est en cours. Lorsque les utilisateurs sont chargés, le sondage Microsoft Entra ID est terminé.

6. Cliquez sur **Enregistrer**.

Le sondage Microsoft Entra ID est terminé, et les utilisateurs de Microsoft Entra ID sont ajoutés à Kaspersky Security Center Cloud Console.

Ajout de Kaspersky Security Center Cloud Console à la liste des applications

Vous pouvez autoriser l'utilisateur à ouvrir Kaspersky Security Center Cloud Console en cliquant sur son nom dans la liste des applications sans saisir l'URL de connexion. La liste des applications est disponible dans Mes applications et le lanceur Office 365.

Pour ajouter Kaspersky Security Center Cloud Console à la liste des applications, procédez comme suit :

1. Dans le menu principal du centre d'administration Microsoft Entra, accédez à **Identité** → **Applications** → **Inscriptions d'applications**, puis sous l'onglet **Toutes les applications**, sélectionnez l'application Kaspersky Security Center Cloud Console que vous avez déjà enregistrée dans Microsoft Entra ID.

2. Dans le menu de Kaspersky Security Center Cloud Console, sélectionnez la section Image de **Marque et propriétés**, puis procédez comme suit :

   a. Dans le champ **URL de la page d'accueil**, saisissez l'URL de connexion.

   b. Le cas échéant, ajoutez, dans le champ **Charger le nouveau logo**, une image qui servira d'icône de l'application dans la liste des applications.

   c. Cliquez sur **Enregistrer**.

3. Dans le menu principal du centre d'administration Microsoft Entra, accédez à **Identité** → **Applications** → **Applications d'entreprise**, puis sélectionnez Kaspersky Security Center Cloud Console.

   La page de présentation de l'application s'ouvre.

4. Dans le menu de Kaspersky Security Center Cloud Console, sélectionnez la section **Propriétés**, puis procédez comme suit :

   a. Définissez les options suivantes sur **Oui** :

   - **Connexion permise pour les utilisateurs ?**

     Cette action est nécessaire uniquement si l'option n'est pas définie sur **Oui** par défaut.

   - **Visible par les utilisateurs ?**

   b. Cliquez sur **Enregistrer**.

5. Dans le menu de Kaspersky Security Center Cloud Console, sélectionnez la section **Utilisateurs et groupes**, puis procédez comme suit :

   a. Cliquez sur le bouton **Ajouter un utilisateur/groupe**, puis sur le lien en dessous de **Utilisateurs et groupes**.

   b. Dans la fenêtre qui s'ouvre, sélectionnez les utilisateurs et les groupes, puis cliquez sur le bouton **Enregistrer**.

   La fenêtre se ferme.

   c. Cliquez sur le bouton **Attribuer**.

Kaspersky Security Center Cloud Console est disponible dans Mes applications et le lanceur Office 365 pour les utilisateurs sélectionnés. Les utilisateurs peuvent ouvrir Kaspersky Security Center Cloud Console en cliquant sur son nom dans la liste sans saisir l'URL de connexion.

Désignation d'un utilisateur en tant que propriétaire de l'appareil

Pour obtenir plus d'informations sur l'attribution d'un utilisateur en tant que propriétaire de l'appareil mobile, consultez l'aide de Kaspersky Security for Mobile.

Pour désigner un utilisateur en tant que propriétaire de l'appareil, procédez comme suit :

1. Si vous souhaitez désigner le propriétaire d'un appareil connecté à un Serveur d'administration virtuel, basculez d'abord sur le Serveur d'administration virtuel :

   a. Dans le menu principal, cliquez sur l'icône en forme de chevron (›) à droite du nom actuel du Serveur d'administration.

   b. Sélectionnez le Serveur d'administration requis.

2. Dans le menu principal, accédez à **Utilisateurs et rôles** → **Utilisateurs et groupes**, puis sélectionnez l'onglet **Utilisateurs**.

   Une liste d'utilisateurs s'ouvre. Si vous êtes actuellement connecté à un Serveur d'administration virtuel, la liste comprend les utilisateurs du Serveur d'administration virtuel actuel et du Serveur d'administration principal.

3. Cliquez sur le nom du compte utilisateur que vous souhaitez désigner comme propriétaire de l'appareil.

4. Dans la fenêtre des paramètres utilisateur qui s'ouvre, sélectionnez l'onglet **Appareils**.

5. Cliquez sur **Ajouter**.

6. Dans la liste des appareils, sélectionnez l'appareil que vous voulez attribuer à l'utilisateur.

7. Cliquez sur le bouton **OK**.

L'appareil sélectionné est ajouté à la liste des appareils attribués à l'utilisateur.

Vous pouvez effectuer la même opération dans **Ressources (Appareils)** → **Appareils administrés**, en cliquant sur le nom de l'appareil que vous voulez attribuer, puis en cliquant sur le lien **Administrer le propriétaire de l'appareil**.

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 Cloud 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.

L'utilisateur sera enregistré en tant que propriétaire de l'appareil.

Utilisation des révisions des objets

Cette section contient les informations sur l'utilisation des révisions des objets. Kaspersky Security Center Cloud Console permet de suivre les modifications des objets. Chaque enregistrement de modification dans une objet entraîne la création d'une *révision*. Chaque révision possède un numéro.

Voici les objets 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 Cloud Console avec laquelle l'objet a été modifié.
- **Action** – l'action exécutée avec l'objet.
- **Description** – la description de la révision de modification des paramètres de l'objet.

  Par défaut, la description de la révision de l'objet n'est pas remplie. Pour ajouter une description de la révision, choisissez la révision requise, puis cliquez sur le bouton **Modifier la description**. Dans la fenêtre qui s'ouvre, saisissez un texte correspondant à la description de la révision.

Restauration des modifications

En cas de besoin, vous pouvez restaurer les modifications de l'objet. Par exemple, il peut être nécessaire de rétablir les paramètres de la stratégie à leur état à la date définie.

Pour restaurer les modifications d'un objet, procédez comme suit :

1. Dans la fenêtre des propriétés de l'objet, ouvrez l'onglet **Historique des révisions**.
2. Dans la liste des révisions de l'objet, sélectionnez le numéro de la révision pour laquelle il faut restaurer les modifications.
3. Cliquez sur le bouton **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.

Ajout d'une description de la révision

Vous pouvez ajouter une description de la révision afin de pouvoir la retrouver facilement dans la liste à l'avenir.

Pour ajouter une description de la révision, procédez comme suit :

1. Dans la fenêtre des propriétés de l'objet, ouvrez l'onglet **Historique des révisions**.
2. Dans la liste des révisions de l'objet, sélectionnez la révision pour laquelle vous souhaitez ajouter une description.
3. Cliquez sur le bouton **Modifier la description**.

   La fenêtre **Description** s'ouvrira.
4. Dans la fenêtre **Description**, saisissez un texte correspondant à la description de la révision.

   Par défaut, la description de la révision de l'objet n'est pas remplie.
5. Enregistrez la description de la révision.

La description est ajoutée pour la révision de l'objet.

Affichage et enregistrement d'une révision de la stratégie

Kaspersky Security Center Cloud Console permet de consulter les modifications apportées à une stratégie au cours d'une période donnée et d'enregistrer les informations sur ces modifications dans un fichier.

L'affichage et l'enregistrement d'une révision de la stratégie sont disponibles si le plug-in Internet d'administration correspondant prend en charge cette fonctionnalité.

Pour consulter la révision d'une stratégie, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Stratégies et profils**.
2. Cliquez sur la stratégie de la révision que vous souhaitez consulter, puis passez à la section **Historique des révisions**.

3. Dans la liste des révisions de la stratégie, cliquez sur le numéro de la révision que vous souhaitez consulter.

   Si la taille de la révision est supérieure à 10 Mo, vous ne pourrez pas la consulter à l'aide de Kaspersky Security Center Cloud Console. Vous serez invité à enregistrer la révision sélectionnée dans un fichier JSON.

   Si la taille de la révision ne dépasse pas 10 Mo, un rapport au format HTML avec les paramètres de la révision de la stratégie sélectionnée s'affiche. Comme le rapport s'affiche dans une fenêtre contextuelle, assurez-vous que les fenêtres contextuelles sont autorisées dans votre navigateur.

Pour enregistrer une révision de la stratégie dans un fichier JSON, procédez comme suit :

Dans la liste des révisions de la stratégie, sélectionnez la révision que vous souhaitez enregistrer, puis cliquez sur **Enregistrer dans le fichier**.

La révision est enregistrée dans un fichier JSON.

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 permet de recevoir des informations sur les applications installées sur les appareils clients. Ces informations se trouvent dans les bases de réputation de Kaspersky.

Si vous participez à KSN, vous acceptez de transmettre automatiquement à Kaspersky les informations relatives au fonctionnement des applications de Kaspersky installées sur les appareils clients administrés par Kaspersky Security Center Cloud Console. 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.

L'application propose de vous connecter à KSN lors de l'exécution de l'assistant de démarrage rapide 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 jour ou mettez à niveau le 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 Cloud Console vérifie si les serveurs KSN sont accessibles. Si l'accès aux serveurs via le DNS système n'est pas possible, l'application utilise les serveurs DNS publics. Cela est nécessaire pour garantir le maintien du niveau de sécurité des appareils administrés.

Les appareils clients administrés par le Serveur d'administration interagissent avec KSN à l'aide du serveur proxy KSN. Le serveur proxy KSN fournit les possibilités suivantes :

- Les appareils clients peuvent exécuter les demandes à KSN 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 activer le serveur proxy KSN du côté du point de distribution pour que l'appareil agisse comme le serveur proxy KSN. Dans ce cas, le service KSN proxy (ksnproxy) est exécuté sur l'appareil.

Activation et désactivation de KSN

Pour activer KSN, procédez comme suit :

1. Dans le menu principal, cliquez sur l'icône des paramètres ( ) en regard du nom du Serveur d'administration requis.

   La fenêtre des propriétés du Serveur d'administration s'ouvre.

2. Sous l'onglet **Général**, sélectionnez la section **Paramètres KSN**.

3. Basculez le commutateur sur la position **Utiliser Kaspersky Security Network Activé**.

   Le KSN est activé.

   Si le commutateur est activé, les appareils clients transmettent les résultats de l'installation des correctifs à Kaspersky. Une fois que vous avez le commutateur, vous devez lire et accepter les Conditions de la Déclaration KSN.

4. Cliquez sur le bouton **Enregistrer**.

Pour désactiver KSN, procédez comme suit :

1. Dans le menu principal, cliquez sur l'icône des paramètres ( ) en regard du nom du Serveur d'administration requis.

   La fenêtre des propriétés du Serveur d'administration s'ouvre.

2. Sous l'onglet **Général**, sélectionnez la section **Paramètres KSN**.

3. Basculez le commutateur sur la position **Utiliser Kaspersky Security Network Désactivé**.

   Le KSN est désactivé.

   Si le commutateur est désactivé, les appareils clients ne transmettent pas les résultats de l'installation des correctifs à Kaspersky.

4. Cliquez sur le bouton **Enregistrer**.

Affichage de la Déclaration KSN acceptée

Lorsque vous activez Kaspersky Security Network (KSN), vous devez lire et accepter la Déclaration KSN. Vous pouvez consulter à tout moment la déclaration KSN.

Pour afficher la Déclaration KSN acceptée, procédez comme suit :

1. Dans le menu principal, cliquez sur l'icône des paramètres ( ) à côté du nom du Serveur d'administration.

   La fenêtre des propriétés du Serveur d'administration s'ouvre.

2. Sous l'onglet **Général**, sélectionnez la section **Paramètres de 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 automatiquement lorsque vous ouvrez Kaspersky Security Center Cloud Console. 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. Vous pouvez consulter et accepter la Déclaration KSN mise à jour 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 qui fonctionne comme un point de distribution, vous pouvez activer le serveur proxy KSN. Un appareil administré fonctionne comme un serveur proxy KSN lorsque le service ksnproxy est exécuté sur l'appareil. Vous pouvez vérifier, activer ou désactiver ce service sur l'appareil localement.

Vous pouvez désigner un appareil Windows ou Linux comme point de distribution. La méthode de vérification du point de distribution dépend du système d'exploitation de ce point de distribution.

Pour vérifier si le point de distribution basé sur Windows fonctionne comme serveur proxy KSN, procédez comme suit :

1. Sur l'appareil du point de distribution, sous Windows, ouvrez **Services** (**Tous les programmes** → **Outils d'administration** → **Services**).

2. Dans la liste des services, vérifiez si le service ksnproxy est en cours d'exécution.

   Si le service ksnproxy est en cours d'exécution, l'Agent d'administration de l'appareil participe à Kaspersky Security Network et fonctionne comme serveur proxy KSN pour les appareils administrés inclus dans la zone d'action du point de distribution.

Si vous le souhaitez, vous pouvez désactiver le service ksnproxy. Dans ce cas, l'Agent d'administration sur le point de distribution cesse de participer à Kaspersky Security Network. Cela requiert des autorisations d'administrateur local.

Pour vérifier si le point de distribution basé sur Linux fonctionne comme serveur proxy KSN, procédez comme suit :

1. Sur l'appareil du point de distribution, affichez la liste des processus en cours d'exécution.

2. Dans la liste des processus en cours d'exécution, vérifiez si le processus `/opt/kaspersky/ksc64/sbin/ksnproxy` est en cours d'exécution.

Si le processus `/opt/kaspersky/ksc64/sbin/ksnproxy` est en cours d'exécution, l'Agent d'administration de l'appareil participe à Kaspersky Security Network et fonctionne comme serveur proxy KSN pour les appareils administrés inclus dans la zone d'action du point de distribution.

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

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 Cloud Console 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 souhaite supprimer le(s) appareil(s)** dans la fenêtre de confirmation qui s'ouvre lorsque vous supprimez de tels appareils (soit du groupe **Appareils non définis**, soit du groupe **Appareils administrés**), cela signifie que vous êtes au courant de la suppression des données ultérieure.

  Pour déchiffrer le disque, les conditions suivantes doivent être remplies :

  - L'appareil est reconnecté au Serveur d'administration pour restaurer les données nécessaires au déchiffrement du disque.
  - L'utilisateur de l'appareil se souvient du mot de passe de déchiffrement.
  - L'application de sécurité utilisée pour chiffrer le disque, par exemple, Kaspersky Endpoint Security for Windows, est toujours installée sur l'appareil.

  Si le disque a été chiffré à l'aide de la technologie Kaspersky Disk Encryption, vous pouvez également essayer de récupérer les données à l'aide de l'utilitaire de restauration FDERT.

Lorsque vous supprimez manuellement un appareil du groupe Appareils non définis, l'application supprime l'appareil de la liste. Après la suppression de l'appareil, les applications Kaspersky installées (le cas échéant) restent sur l'appareil. Ensuite, si l'appareil est toujours visible pour le Serveur d'administration et que vous avez configuré le sondage du réseau régulier, Kaspersky Security Center Cloud Console 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.

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 composants et les applications de sécurité de Kaspersky Security Center Cloud Console

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 Configuration de la protection du réseau, vous devez maintenir la fiabilité du système de protection. Cette maintenance garantit que la protection des appareils administrés reste ferme contre une série de menaces, notamment les virus, les attaques réseau et les attaques de phishing.

Vous pouvez utiliser plusieurs schémas pour installer les mises à jour des composants et des applications de sécurité de Kaspersky Security Center Cloud Console. Choisissez le schéma ou plusieurs schémas qui répondent le mieux aux exigences de votre réseau.

Le scénario ci-dessous décrit le schéma de mise à jour qui implique le téléchargement de mises à jour dans les stockages de points de distribution. Si les appareils administrés ne sont pas connectés aux points de distribution, envisagez de mettre à jour manuellement les bases de données, les modules logiciels et les applications ou directement à partir des serveurs de mise à jour de Kaspersky.

Lorsque vous terminez ce scénario, les résultats suivants se produisent :

- Les composants de Kaspersky Security Center Cloud Console sont mis à jour automatiquement ou uniquement lorsque vous affectez l'état *Approuvé* aux mises à jour.
- Les applications de sécurité Kaspersky, les bases de données Kaspersky et les modules logiciels sont mis à jour conformément au calendrier que vous avez spécifié. Par défaut, les applications de sécurité Kaspersky installent uniquement les mises à jour que vous avez approuvées.

Vous pouvez configurer le processus de mise à jour pour télécharger et installer les mises à jour de deux façons différentes :

- Automatiquement

  Dans ce cas, vous ne devez exécuter ce scénario qu'une seule fois. Vous devrez programmer la tâche *Téléchargement des mises à jour sur les stockages des points de distribution* (le cas échéant), et les tâches de mise à jour pour les applications de sécurité Kaspersky et conserver les paramètres de mise à jour par défaut dans les propriétés de l'Agent d'administration.

- Mode manuel

Vous pouvez configurer le processus de mise à jour pour exécuter la tâche *Téléchargement des mises à jour sur les stockages des points de distribution* (le cas échéant) et les tâches de mise à jour pour les applications de sécurité Kaspersky manuellement. Vous pouvez également configurer l'Agent d'administration pour installer les mises à jour des composants de Kaspersky Security Center Cloud Console uniquement lorsque vous affectez l'état *Approuvé* aux mises à jour.

Prérequis

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 Cloud Console. Lors de l'exécution de ce scénario, vous avez affecté la quantité de points de distribution appropriée en fonction du nombre d'appareils administrés et de la topologie du réseau.

2. Créé et configuré l'ensemble des stratégies, profils de stratégie et tâches obligatoire selon le scénario de configuration de la protection du réseau.

Étapes

La configuration des mises à jour régulières des bases de données et des applications de Kaspersky s'effectue par étapes :

1. **Création de la tâche de téléchargement des mises à jour dans les stockages des points de distribution**

   Créez la tâche *Téléchargement des mises à jour sur les stockages des points de distribution*. Une fois cette tâche exécutée, Kaspersky Security Center Cloud Console télécharge les mises à jour des points de distribution directement à partir des serveurs de mises à jour de Kaspersky.

   Instructions pour : Création de la tâche de téléchargement des mises à jour sur les stockages des points de distribution

2. **Configuration des points de distribution**

   Assurez-vous que l'option **Déployer les mises à jour** est activée dans les propriétés de tous les points de distribution requis. Lorsque cette option est désactivée pour un point de distribution, les appareils inclus dans son périmètre ne peuvent télécharger les mises à jour qu'à partir d'une ressource locale ou directement à partir des serveurs de mises à jour de Kaspersky.

   Si vous souhaitez que les appareils administrés reçoivent des mises à jour uniquement à partir des points de distribution, activez l'option **Distribuer les fichiers uniquement via les points de distribution** dans la stratégie de l'Agent d'administration.

3. **Optimisation du processus de mise à jour à l'aide de fichiers diff (facultatif)**

   L'activation de cette fonctionnalité entraîne une diminution du trafic entre 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 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

4. **Définition des mises à jour à installer**

   Par défaut, les mises à jour du logiciel téléchargées sont à l'état *Non défini*. Affectez à l'état la valeur *Approuvé* ou *Rejeté* pour définir si cette mise à jour doit être installée sur des appareils en réseau. Les mises à jour confirmées sont toujours installées. Les mises à jour non définies peuvent uniquement être installées sur l'Agent d'administration et sur les autres composants de Kaspersky Security Center Cloud Console conformément aux paramètres de stratégie de l'Agent d'administration. Les mises à jour auxquelles vous avez attribué l'état *Rejetée* ne seront pas installées sur les appareils.

Instructions pour :

- À propos des statuts de mise à jour
- Approbation et refus des mises à jour du logiciel

5. **Configuration de l'installation automatique des mises à jour et des correctifs des composants de Kaspersky Security Center Cloud Console**

   Par défaut, les mises à jour et les correctifs téléchargés pour l'Agent d'administration et les autres composants de la Kaspersky Security Center Cloud Console sont installés automatiquement. Si vous n'avez pas laissé l'option **Installer automatiquement les mises à jour et les correctifs nécessaires pour les modules dont l'état est Non défini** activée dans les propriétés de l'Agent d'administration, toutes les mises à jour seront installées automatiquement après leur téléchargement dans le stockage (ou plusieurs stockages). Si l'option est désactivée, les correctifs de Kaspersky chargés avec l'état *Non défini* sont installés après que l'administrateur a modifié leur état pour qu'il soit *Approuvé*.

   Instructions pour : Activation et désactivation de la mise à jour automatique et de l'installation automatique des correctifs pour les composants de Kaspersky Security Center Cloud Console

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 applications, des modules logiciels et des bases de données Kaspersky, et notamment des bases antivirus. Nous vous recommandons de sélectionner l'option **Lors du téléchargement des mises à jour dans le stockage** pendant la configuration de la programmation de la tâche. Cela garantira que les nouvelles mises à jour sont installées dès que possible.

   Par défaut, les mises à jour des applications administrées ne sont installées que lorsque vous avez affecté à l'état de la mise à jour la valeur *Approuvé*. Pour Kaspersky Endpoint Security for Windows, vous pouvez modifier les paramètres de mise à jour dans la tâche de mise à jour.

   Si une mise à jour nécessite une révision et l'acceptation des termes du Contrat de licence utilisateur final, vous devez d'abord les accepter. Ensuite, la mise à jour peut être propagée sur les appareils administrés.

   Instructions pour : Installation automatique des mises à jour pour Kaspersky Endpoint Security sur les appareils

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 de sécurité a été installée précédemment, Kaspersky Security Center Cloud Console 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 Cloud Console et des plug-ins Web d'administration n'est pas prise en charge.

   Instructions pratiques : approbation et refus de mises à jour

Une fois le scénario terminé, vous pouvez contrôler 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 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 Cloud Console 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 antivirus sont mises à jour et que le niveau de sécurité est maintenu pour les appareils administrés.

- Applications de Kaspersky installées, y compris les composants et les applications de sécurité de Kaspersky Security Center Cloud Console

  Kaspersky Security Center Cloud Console 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 Cloud 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 :

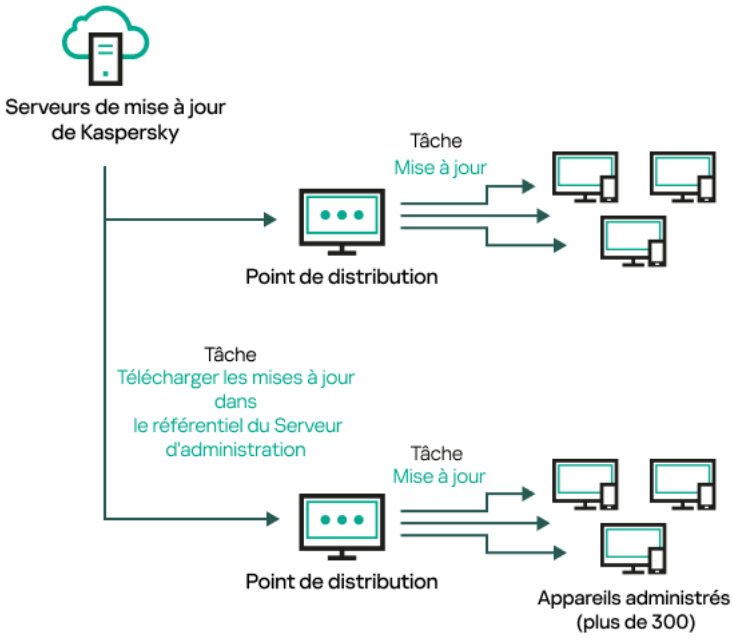
- En utilisant la tâche *Téléchargement des mises à jour sur les stockages des points de distribution*
- Manuellement via un dossier local, un dossier partagé ou un serveur FTP
- Directement à partir des serveurs de mise à jour de Kaspersky vers les applications de sécurité sur les appareils administrés

Utilisation de la tâche Téléchargement des mises à jour sur les stockages des points de distribution

Dans ce schéma, Kaspersky Security Center Cloud Console télécharge les mises à jour via la tâche *Téléchargement des mises à jour sur 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 à partir du stockage du point de distribution (voir la figure ci-dessous).

Les appareils de points de distribution exécutant macOS ne peuvent pas télécharger les mises à jour à partir des serveurs de mises à jour de Kaspersky.

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



Mise à jour en utilisant la tâche Téléchargement des mises à jour sur les stockages des points de distribution

Lorsque la tâche *Téléchargement des mises à jour sur les stockages des points de distribution* est terminée, les mises à jour suivantes sont téléchargées dans le stockage du point de distribution :

- Bases de données et modules logiciels de Kaspersky pour les applications de sécurité sur les appareils administrés

  Ces mises à jour sont installées via la tâche de mise à jour pour Kaspersky Endpoint Security for Windows.

- Mises à jour des composants de Kaspersky Security Center Cloud Console

  Par défaut, ces mises à jour sont installées automatiquement. Vous pouvez modifier les paramètres dans la stratégie de l'Agent d'administration.

- Mises à jour des applications de sécurité

  Par défaut, Kaspersky Endpoint Security for Windows installe uniquement les mises à jour que vous approuvez. Les mises à jour sont installées via la tâche de mise à jour et peuvent être configurées dans les propriétés de cette tâche.

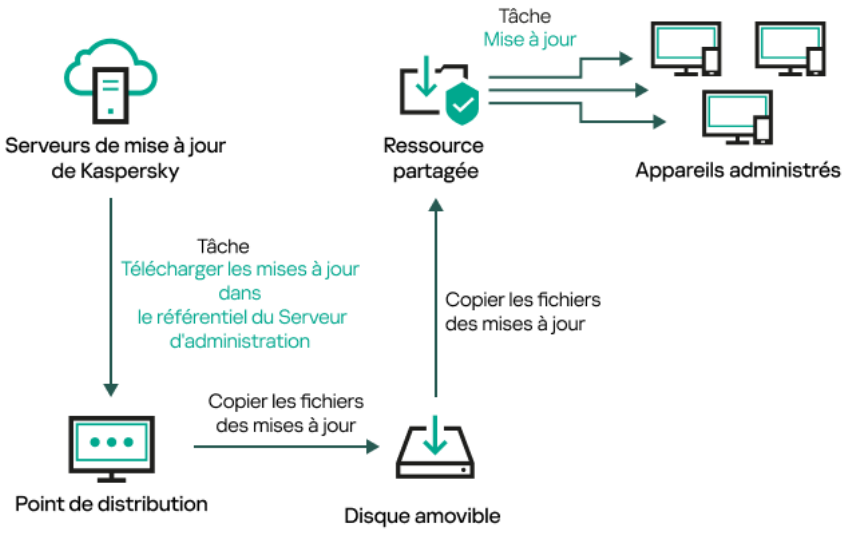
Chaque application de Kaspersky sollicite les mises à jour requises au serveur d'administration. Le Serveur d'administration accumule ces requêtes et télécharge sur les stockages des points de distribution uniquement les mises à jour requises par n'importe quelle application. Cela évite de télécharger 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 les stockages des points de distribution*, 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 :

- Identifiant et version de l'application
- Identifiant d'installation de l'application
- ID de la clé active
- ID de l'exécution de la tâche de téléchargement

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.

Manuellement via un dossier local, un dossier partagé ou un serveur FTP

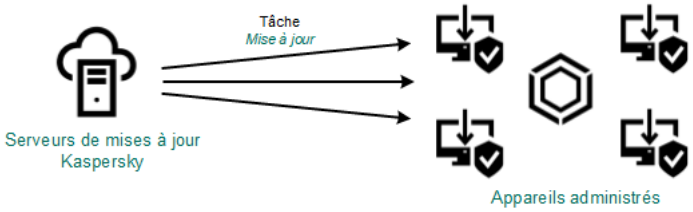
Si les appareils client ne disposent pas d'une connexion à un point de distribution, vous pouvez utiliser un dossier local ou une ressource partagée comme source de mise à jour des bases de données, des modules logiciels et des applications de Kaspersky. Dans ce schéma, vous devez copier les mises à jour nécessaires du stockage du point de distribution sur un disque amovible, puis copier les mises à jour dans le dossier local ou dans la ressource spécifiée comme source de mises à jour dans les paramètres de Kaspersky Endpoint Security for Windows (voir figure ci-dessous).



Mise à jour via un dossier local, un dossier partagé ou un serveur FTP

Directement à partir des serveurs de mise à jour de Kaspersky vers Kaspersky Endpoint Security for Windows sur les appareils administrés

Sur les appareils administrés, vous pouvez configurer Kaspersky Endpoint Security for Windows 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 Cloud Console. Pour recevoir directement les mises à jour à partir des serveurs de mise à jour de Kaspersky, spécifiez ces derniers comme source de mises à jour dans l'interface de l'application de sécurité. Pour obtenir une description complète de ces paramètres, consultez la documentation de Kaspersky Endpoint Security for Windows.

Création de la tâche de téléchargement des mises à jour dans les stockages des points de distribution

Les appareils de points de distribution exécutant macOS ne peuvent pas télécharger les mises à jour à partir des serveurs de mises à jour de Kaspersky.

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

Vous pouvez créer la tâche *Téléchargement des 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.

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 composants Kaspersky Security Center Cloud Console
- Mises à jour des applications de sécurité Kaspersky

Une fois téléchargées, les mises à jour peuvent être propagées vers les appareils administrés.

*Pour créer la tâche **Téléchargement des mises à jour sur les stockages des points de distribution** pour un groupe d'administration sélectionné, procédez comme suit :*

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Tâches**.
2. Cliquez sur le bouton **Ajouter**.

   Ceci permet de lancer l'assistant de création d'une tâche. Suivez les étapes de l'assistant.
3. Pour l'application Kaspersky Security Center Cloud Console, dans le champ **Type de tâche**, sélectionnez **Téléchargement des mises à jour sur les stockages des points de distribution**.
4. Spécifiez le nom de la tâche créée. Le nom de la tâche ne peut pas contenir plus de 100 symboles et contenir de symboles spéciaux ("*<>?\:|).
5. Sélectionnez un bouton d'option pour spécifier le groupe d'administration, la sélection d'appareils ou les appareils auxquels la tâche s'applique.
6. À l'étape **Fin de la création de la tâche**, si vous activez l'option **Ouvrir les détails de la tâche à la fin de la création**, vous pouvez modifier les paramètres de la tâche par défaut. Si vous n'activez pas cette tâche, la tâche est créée selon les paramètres par défaut. Vous pourrez modifier ces paramètres par défaut plus tard, à tout moment.
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.

- Serveur d'administration principal

  Cette ressource s'applique aux tâches créées pour un Serveur d'administration virtuel ou secondaire.

- Dossier local ou réseau

  Un dossier local ou de réseau qui contient les mises à jour les plus récentes. Un dossier de réseau peut être un serveur FTP ou HTTP ou un dossier partagé SMB. Si un dossier réseau nécessite une authentification, seul le protocole SMB est pris en charge. Lors de la sélection du dossier local, il faut indiquer le dossier sur l'appareil avec le Serveur d'administration installé.

  Un serveur FTP ou http ou un dossier de réseau utilisé par une source des mises à jour doit contenir une structure de dossiers (avec les mises à jour) qui correspond à la structure créée lors de l'utilisation des serveurs de mise à jour de Kaspersky.

- **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**

Kaspersky Security Center Cloud Console télécharge les mises à jour des bases de données et des modules logiciels en utilisant le nouveau schéma. Pour que l'application télécharge les mises à jour à l'aide du nouveau schéma, la source de mise à jour doit contenir les fichiers de mise à jour avec les métadonnées compatibles avec le nouveau schéma. Si la source de mise à jour contient les fichiers de mise à jour avec les métadonnées compatibles avec l'ancien schéma uniquement, activez l'option **Télécharger les mises à jour en utilisant l'ancien système**. Sinon, la tâche de téléchargement de la mise à jour échouera.

Par exemple, vous devez activer cette option lorsqu'un dossier local ou réseau est spécifié comme source de mise à jour et que les fichiers de mise à jour de ce dossier ont été téléchargés par l'une des applications suivantes :

- Kaspersky Update Utility

  Cet utilitaire télécharge les mises à jour en utilisant l'ancien schéma.

- Kaspersky Security Center 13.2 ou version antérieure

Par exemple, un point de distribution est configuré pour prendre les mises à jour d'un dossier local ou réseau. Dans ce cas, vous pouvez télécharger les mises à jour à l'aide d'un Serveur d'administration doté d'une connexion Internet, puis placer les mises à jour dans le dossier local du point de distribution. Si le Serveur d'administration dispose de la version 13.2 ou antérieure, activez l'option **Télécharger les mises à jour en utilisant l'ancien système** dans la tâche *Télécharger les mises à jour dans les stockages des points de distribution*.

Cette option est Inactif par défaut.

10. Créez une programmation pour le démarrage de la tâche. Le cas échéant, configurez les paramètres suivants :

- Démarrer la tâche

  Sélectionnez la programmation de l'exécution de la tâche, puis configurez la programmation sélectionnée.

  - 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.

- **Toutes les N semaines**

  La tâche s'exécute régulièrement, selon l'intervalle défini en semaines, le jour indiqué de la semaine et à l'heure indiquée.

  La tâche s'exécute par défaut chaque lundi à l'heure système actuelle.

- **Chaque jour (passage à l'heure d'été non pris en charge)**

  La tâche s'exécute régulièrement, selon l'intervalle défini en jours. Cette programmation ne tient pas compte du passage à l'heure d'été. Cela signifie que lorsque les horloges sont avancées ou reculées d'une heure au début ou à la fin de l'été, l'heure de lancement réelle de la tâche ne change pas.

  Nous déconseillons d'adopter cette programmation. Elle est requise pour la rétrocompatibilité avec Kaspersky Security Center Cloud Console.

  La tâche démarre par défaut chaque jour à l'heure système actuelle.

- **Chaque semaine**

  La tâche s'exécute chaque semaine, le jour défini et à l'heure indiquée.

- **Selon les jours de la semaine**

  La tâche s'exécute régulièrement les jours définis de la semaine, à l'heure indiquée.

  Par défaut, la tâche s'exécute chaque vendredi à 18h00.

- **Chaque mois**

  La tâche s'exécute régulièrement le jour du mois défini, à l'heure indiquée.

  Si le jour en question ne figure pas dans le mois, la tâche s'exécute le dernier jour.

  La tâche s'exécute par défaut le premier jour de chaque mois, à l'heure système actuelle.

- **Mensuellement, les jours indiqués des semaines sélectionnées**

  La tâche s'exécute régulièrement les jours du mois définis, à l'heure indiquée.

  Par défaut, aucun jour du mois n'est sélectionné. L'heure de début par défaut est 18:00.

- **Lors de la détection d'une propagation de virus**

La tâche s'exécute après un événement *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. Ce paramètre 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.

Configuration des appareils administrés pour recevoir les mises à jour uniquement à partir de points de distribution

Les appareils administrés peuvent récupérer les mises à jour des bases de données Kaspersky, des modules logiciels et des applications Kaspersky à partir de différentes sources : directement à partir de serveurs de mises à jour de points de distribution, ou d'un dossier local ou réseau. Vous pouvez spécifier des points de distribution comme source unique de mises à jour possible.

Pour configurer les appareils administrés de manière à recevoir les mises à jour uniquement à partir de points de distribution :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Stratégies et profils**.
2. Cliquez sur la stratégie de l'Agent d'administration.

3. Dans la fenêtre des propriétés de la stratégie, ouvrez l'onglet **Paramètres de l'application**.

4. Dans la section **Paramètres**, activez le commutateur **Distribuer les fichiers uniquement via les points de distribution**.

5. Fermez le cadenas (🔒) de ce bouton à bascule.

6. Cliquez sur le bouton **Enregistrer**.

La stratégie sera appliquée aux appareils sélectionnés et ceux-ci recevront les mises à jour uniquement des points de distribution.

Activation et désactivation de l'installation automatique des mises à jour et des correctifs pour les composants de Kaspersky Security Center Cloud Console

L'installation automatique des mises à jour et des correctifs pour les composants de Kaspersky Security Center Cloud Console est activée par défaut lors de l'installation de l'Agent d'administration sur l'appareil. Vous pouvez le désactiver lors de l'installation de l'Agent d'administration ou ultérieurement en utilisant une stratégie.

Pour désactiver l'installation automatique des mises à jour et des correctifs pour les composants de Kaspersky Security Center Cloud Console lors de l'installation locale de l'Agent d'administration sur l'appareil, procédez comme suit :

1. Lancez l'installation locale de l'Agent d'administration sur l'appareil.

2. À l'étape **Paramètres complémentaires**, décochez la case **Installer automatiquement les mises à jour et les correctifs applicables aux composants dont la case à cocher de statut est Non défini**.

3. Suivez les instructions de l'assistant.

L'Agent d'administration s'installe sur l'appareil sans l'option d'installer des mises à jour et des correctifs pour les composants de Kaspersky Security Center Cloud Console. Vous pouvez activer l'installation automatique des mises à jour et des correctifs plus tard à l'aide d'une stratégie.

Pour désactiver l'installation automatique des mises à jour et des correctifs pour les composants de Kaspersky Security Center Cloud Console lors de l'installation de l'Agent d'administration sur l'appareil à l'aide d'un paquet d'installation, procédez comme suit :

1. Dans le menu principal, accédez à **Opérations → Stockages → Paquets d'installation**.

2. Cliquez sur le paquet **Agent d'administration de Kaspersky Security Center <numéro de version>**.

3. Dans la fenêtre des propriétés, ouvrez l'onglet **Paramètres**.

4. Désactivez le commutateur **Installer automatiquement les mises à jour et les correctifs nécessaires pour les modules dont l'état est Non défini**.

L'Agent d'administration est installé depuis ce paquet avec l'option d'installation automatique des mises à jour et des correctifs pour les composants de Kaspersky Security Center Cloud Console désactivée. Vous pouvez activer l'installation automatique des mises à jour et des correctifs plus tard à l'aide d'une stratégie.

Si la case à cocher à l'étape 4 a été activée (ou désactivée) lors de l'installation de l'Agent d'administration sur l'appareil, vous pouvez par la suite activer (ou désactiver) la mise à jour automatique à l'aide de la stratégie d'Agent d'administration.

Pour activer ou désactiver l'installation automatique des mises à jour et les correctifs pour les composants de Kaspersky Security Center Cloud Console à l'aide d'une stratégie de l'Agent d'administration, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Stratégies et profils**.
2. Cliquez sur la stratégie de l'Agent d'administration.
3. Dans la fenêtre des propriétés de la stratégie, sélectionnez l'onglet **Paramètres de l'application**.
4. Dans la section **Administration des correctifs et des mises à jour**, désactivez le commutateur **Installer automatiquement les mises à jour et les correctifs nécessaires pour les modules dont l'état est Non défini** pour activer ou désactiver respectivement l'installation automatique des mises à jour et des correctifs.
5. Assurez-vous de définir le bouton bascule sur (**Appliquer**) pour le verrou ( ).

   La stratégie est appliquée aux appareils sélectionnés et l'installation automatique des mises à jour et des correctifs pour les composants de Kaspersky Security Center Cloud Console est activée (désactivée) sur ces appareils.

Installation automatique des mises à jour pour Kaspersky Endpoint Security for Windows

Vous pouvez configurer les mises à jour automatiques des bases de données et des modules logiciels Kaspersky Endpoint Security for Windows sur les appareils clients.

Pour configurer le téléchargement et l'installation automatique des mises à jour de Kaspersky Endpoint Security for Windows sur les appareils, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Tâches**.
2. Cliquez sur le bouton **Ajouter**.

   Ceci permet de lancer l'assistant de création d'une tâche. Suivez les étapes de l'assistant.
3. Pour l'application Kaspersky Endpoint Security for Windows, sélectionnez **Mise à jour** comme sous-type de tâche.
4. Spécifiez le nom de la tâche créée. Le nom de la tâche ne peut pas contenir plus de 100 symboles et contenir de symboles spéciaux ("*<>?\:|).
5. Choisissez la zone d'action de la tâche.
6. Spécifiez le groupe d'administration, la sélection d'appareils ou les appareils auxquels la tâche s'applique.
7. À l'étape **Fin de la création de la tâche**, si vous activez l'option **Ouvrir les détails de la tâche à la fin de la création**, vous pouvez modifier les paramètres de la tâche par défaut. Si vous n'activez pas cette tâche, la tâche est créée selon les paramètres par défaut. Vous pourrez modifier ces paramètres par défaut plus tard, à tout moment.

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** : Les paramètres de cet onglet définissent la manière dont l'appareil reçoit les mises à jour une fois la connexion entre l'appareil et le Serveur d'administration établie.

    - **Mode mobile** : Les paramètres de cet onglet définissent la manière dont l'appareil reçoit les mises à jour lorsqu'aucune connexion n'est établie entre Kaspersky Security Center Cloud Console et l'appareil (par exemple, lorsque 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 à l'aide des 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.

    Quand Kaspersky Security Center Cloud Console est défini comme une source de mises à jour, les mises à jour sont téléchargées à partir d'un stockage de point de distribution et non à partir du stockage du Serveur d'administration. Vérifiez que vous avez assigné des points de distribution et créé la tâche *Téléchargement des mises à jour sur les stockages des points de distribution*.

12. Activez l'option **Installer les mises à jour des modules de l'application approuvés** pour télécharger et installer simultanément les mises à jour des modules logiciels avec les bases de l'application.

    Si l'option est activée, Kaspersky Endpoint Security for Windows informe l'utilisateur des mises à jour de module logiciel disponibles et les inclut dans le paquet de mise à jour lors de l'exécution de la tâche de mise à jour. Kaspersky Endpoint Security for Windows installe uniquement les mises à jour pour lesquelles vous avez défini le statut *Approuvé*. Ils seront installés localement via l'interface de l'application ou via Kaspersky Security Center Cloud Console.

    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 des statuts de mise à jour

L'état est un attribut des mises à jour du logiciel qui définit si une mise à jour du logiciel particulière doit être installée sur un appareil en réseau.

Une mise à jour peut avoir les états suivants :

- *Indéfini*

  Par défaut, les mises à jour du logiciel téléchargées sont à l'état *Non défini*. Les mises à jour non définies peuvent uniquement être installées sur l'Agent d'administration et sur les autres composants de Kaspersky Security Center Cloud Console conformément aux paramètres de stratégie de l'Agent d'administration.

- *Approuvé*

  Les mises à jour confirmées sont toujours installées. Si une mise à jour nécessite une révision et l'acceptation des termes du Contrat de licence utilisateur final, vous devez d'abord les accepter.

- *Rejeté*

  Les mises à jour auxquelles vous avez attribué l'état *Rejetée* ne seront pas installées sur les appareils.

Vous pouvez modifier les états des mises à jour pour les logiciels suivants :

- Agent d'administration et autres composants de Kaspersky Security Center Cloud Console

  Par défaut, les mises à jour et les correctifs téléchargés pour les composants de Kaspersky Security Center Cloud Console sont installés automatiquement. Si vous n'avez pas laissé l'option **Installer automatiquement les mises à jour et les correctifs nécessaires pour les modules dont l'état est Non défini** activée dans les propriétés de l'Agent d'administration, toutes les mises à jour seront installées automatiquement après leur téléchargement dans le stockage (ou plusieurs stockages). Si l'option est désactivée, les correctifs de Kaspersky chargés avec l'état *Non défini* sont installés après que l'administrateur a modifié leur état pour qu'il soit *Approuvé*.

  Les mises à jour des composants de Kaspersky Security Center Cloud Console ne peuvent pas être désinstallées, même si vous définissez une mise à jour sur l'état *Rejeté*.

- Applications de sécurité Kaspersky

  Par défaut, les mises à jour des applications administrées ne sont installées que lorsque vous avez affecté à l'état de la mise à jour la valeur *Approuvé*. Si une mise à jour rejetée pour une application de sécurité a été installée précédemment, Kaspersky Security Center Cloud Console essaiera de la désinstaller de tous les appareils.

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 et Linux. La mise à jour transparente du Serveur d'administration, de Kaspersky Security Center Cloud 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 Cloud Console 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.

Utilisation de fichiers diff pour la mise à jour des bases de données et des modules logiciels Kaspersky

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 limite le trafic sur le 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 fonctionnalité de *téléchargement de fichiers diff* est activée sur un point de distribution, les fichiers diff sont enregistrés sur ce point de distribution. Par conséquent, les appareils qui effectuent des mises à jour à partir de ce point de distribution peuvent utiliser les fichiers diff enregistrés pour mettre à jour leurs bases de données et leurs modules logiciels.

Pour optimiser l'utilisation des fichiers diff, nous vous recommandons de synchroniser le calendrier de mise à jour des appareils avec le calendrier de mise à jour du point de distribution à partir duquel les appareils effectuent les mises à jour. Toutefois, le trafic peut être enregistré même si les appareils sont mis à jour moins souvent que le point de distribution à partir duquel ils sont mis à jour.

Les points de distribution n'utilisent pas la multidiffusion IP pour distribuer automatiquement les fichiers diff.

Pour activer la fonction de téléchargement des fichiers diff :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Tâches**.
2. Cliquez sur la tâche *Téléchargement des mises à jour sur les stockages des points de distribution* pour ouvrir les propriétés de la tâche.
3. Sous l'onglet **Paramètres de l'application**, activez l'option **Télécharger les fichiers diff**.
4. Cliquez sur le bouton **Enregistrer**.

   La fonctionnalité de téléchargement des fichiers diff est activée. Les fichiers diff des mises à jour seront téléchargés en plus des fichiers de mise à jour chaque exécution de la tâche *Téléchargement des mises à jour sur les stockages des points de distribution*.

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.

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 les stockages des points de distribution.

Lorsque vous devez mettre à jour les bases de données et les modules logiciels sur un appareil (ou un groupe d'appareils) non connecté 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 sources suivantes :

- Point de distribution.

Pour garantir que le stockage de point de distribution contient les mises à jour nécessaires à l'application de sécurité installée sur un appareil déconnecté, au moins un des appareils connectés administrés se trouvant dans la zone d'action du point de distribution doit avoir la même application de sécurité installée. Cette application doit être configurée pour recevoir les mises à jour du stockage de point de distribution via la tâche *Téléchargement des mises à jour sur les stockages des points de distribution*.

- Tout appareil ayant la même application de sécurité installée et configuré pour recevoir les mises à jour à partir 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 mises à jour des bases de données et des modules logiciels par copie à partir d'un stockage de point de distribution.

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 du point de distribution.
2. Copiez les fichiers de mises à jour sur le disque amovible.

   Par défaut, les mises à jour se trouvent à l'emplacement suivant : %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1103\Updates.
3. Sur les appareils déconnectés, configurez l'application de sécurité (par exemple, Kaspersky Endpoint Security for Windows) pour recevoir les mises à jour à partir d'un dossier local ou d'une ressource partagée, comme un serveur FTP ou un dossier partagé.
4. Copiez les fichiers de mise à jour du disque amovible dans le dossier local ou dans la ressource partagée à utiliser comme source de mise à jour.
5. Sur l'appareil déconnecté qui nécessite l'installation des mises à jour, démarrez la tâche de mise à jour de Kaspersky Endpoint Security for Windows.

Une fois que la tâche de mise à jour est terminée, les bases de données et les modules logiciels de Kaspersky sont à jour sur l'appareil.

Mise à jour des bases de données de Kaspersky Security for Windows Server

Vous pouvez installer Kaspersky Security for Windows Server sur des appareils administrés, et il pourrait être préférable de lancer la tâche de protection des fichiers en temps réel de cette application. Cependant, l'application est livrée sans les bases de données qui sont nécessaires à son bon fonctionnement. Les bases de données sont téléchargées sur l'appareil administré uniquement une fois la tâche de *téléchargement des mises à jour vers les stockages des points de distribution* terminée.

Si vous souhaitez démarrer la tâche de protection des fichiers en temps réel sur un appareil administré juste après l'installation de Kaspersky Security for Windows Server, vous devez vous assurer que les bases de données de cette application sont téléchargées et à jour. Dans le cas contraire, la tâche risque de ne pas fonctionner correctement.

Pour vous assurer que les bases de données de Kaspersky Security for Windows Server sont à jour :

1. Assurez-vous que la tâche *Téléchargement des mises à jour sur les stockages des points de distribution* est terminée sur le Serveur d'administration.
2. Exécutez une des actions suivantes :

- Dans les paramètres de la tâche de protection des fichiers en temps réel, définissez le début sur **Au démarrage de l'application**, puis redémarrez l'appareil administré.

- Dans les paramètres de la tâche Protection des fichiers en temps réel, définissez manuellement l'heure de lancement sur l'heure souhaitée.

La tâche de protection des fichiers en temps réel dans Kaspersky Security for Windows Server peut maintenant fonctionner correctement.

Gestion des applications tierces sur les appareils client

Cette section décrit les fonctions de Kaspersky Security Center Cloud Console associées à la gestion des applications tierces installées sur les appareils client.

Limitations de la fonctionnalité Gestion des vulnérabilités et des correctifs

La fonctionnalité de la gestion des vulnérabilités et des correctifs présente un certain nombre de limitations, en fonction de la licence que vous utilisez et du mode dans lequel Kaspersky Security Center Cloud Console fonctionne.

Les licences suivantes ne prennent pas en charge la fonctionnalité de la gestion des vulnérabilités et des correctifs :

- Kaspersky Endpoint Security for Business Select
- Kaspersky Hybrid Cloud Security

Les licences suivantes prennent en charge la fonctionnalité de la gestion des vulnérabilités et des correctifs :

- Kaspersky Endpoint Security for Business Advanced
- Kaspersky Endpoint Detection and Response Optimum
- Kaspersky Total Security for Business
- Kaspersky Hybrid Cloud Security Enterprise

Le tableau ci-dessous compare les limitations de Kaspersky Security Center Cloud Console en mode d'évaluation, sous les licences ne prenant pas en charge la fonctionnalité de la gestion des vulnérabilités et des correctifs et sous les licences la prenant en charge.

Limitations de la fonctionnalité Gestion des vulnérabilités et des correctifs

Restrictions	Mode d'évaluation	Mode commercial : licences qui ne prennent pas en charge la fonctionnalité de la gestion des vulnérabilités et des correctifs	Mode commercial : licences qui prennent en charge la fonctionnalité de la gestion des vulnérabilités et des correctifs
Nombre maximum de tâches *Installation des mises à jour Windows Update* ou *Corriger les vulnérabilités*	4	4	0 (aucune nouvelle tâche de ce type ne peut être créée)
Nombre maximal de tâches *Installation des mises à jour requises et correction des vulnérabilités*	2	Non pris en charge	4
Nombre maximal de règles dans toutes les tâches *Installation des mises à jour requises et correction des vulnérabilités*	10	Non pris en charge	50
Nombre maximal de mises à jour du logiciel pouvant avoir l'état *Approuvée* en même temps, sur tous les serveurs, y compris les serveurs virtuels	100	Non pris en charge	1000
Nombre maximal de mises à jour logicielles pouvant être ajoutées manuellement à une tâche, sur tous les serveurs, y compris les serveurs virtuels	500	1000	1000
Nombre maximal de vulnérabilités dans les applications pouvant être ajoutées manuellement à	500	1000	1000

une tâche, sur tous les serveurs, y compris les serveurs virtuels			

Disponibilité des fonctionnalités de la gestion des vulnérabilités et des correctifs en mode d'essai et commercial et sous diverses options de licence

La disponibilité des fonctionnalités de la gestion des vulnérabilités et des correctifs dans Kaspersky Security Center Cloud Console varie selon que vous l'utilisez en mode d'essai ou commercial, ainsi que selon l'option de licence que vous avez sélectionnée. Utilisez le tableau pour vérifier les fonctionnalités de la gestion des vulnérabilités et des correctifs disponibles.

Disponibilité des fonctionnalités de la gestion des vulnérabilités et des correctifs

Fonctionnalité Gestion des vulnérabilités et des correctifs	Mode d'évaluation	Mode commercial : Kaspersky Endpoint Security for Business Select	Mode commercial : Kaspersky Endpoint Security for Business Advanced, Kaspersky Endpoint Detection and Response Optimum, Kaspersky Total Security for Business
Correction manuelle des vulnérabilités dans les applications Microsoft sur les appareils administrés fonctionnant sous Windows Création de la tâche *Corriger les vulnérabilités*	✓	✓	–
Installation manuelle des mises à jour des logiciels Microsoft sur les appareils administrés fonctionnant sous Windows Installation de mises à jour du logiciel tiers à l'aide de la tâche *Installation des mises à jour Windows Update*	–	✓	✓
Installation automatique basée sur des règles de mises à jour du logiciel tiers et correction des vulnérabilités dans les applications tierces Création de la tâche *Installation des mises à jour requises et correction des vulnérabilités* et installation des mises à jour Ajout de règles pour l'installation de la mise à jour	✓	–	✓

À propos des applications tierces

Kaspersky Security Center Cloud Console peut vous aider à mettre à jour les logiciels tiers installés sur les appareils clients, ainsi qu'à corriger les vulnérabilités dans les applications tierces. Kaspersky Security Center Cloud Console peut mettre à jour les logiciels tiers de la version actuelle à la dernière version uniquement.

La liste des logiciels tiers peut être mise à jour et étendue avec de nouvelles applications. Vous pouvez vérifier si vous pouvez mettre à jour le logiciel tiers (installé sur les appareils des utilisateurs) avec Kaspersky Security Center Cloud Console en consultant la liste des mises à jour disponibles dans Kaspersky Security Center Cloud 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 Cloud Console. 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 Cloud Console, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Tâches**.
2. Cliquez sur **Ajouter**.

   Ceci permet de lancer l'assistant de création d'une tâche. Parcourez les étapes de l'assistant à l'aide du bouton **Suivant**.
3. À l'étape **Paramètres de nouvelle tâche** de l'assistant, spécifiez les paramètres suivants :

   a. Dans la liste déroulante **Application**, sélectionnez **Kaspersky Security Center Cloud Console**.

   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.

Mises à jour du logiciel tiers

Kaspersky Security Center Cloud Console permet d'administrer les mises à jour des logiciels tiers installés sur les appareils administrés et de corriger les vulnérabilités dans les applications de Microsoft et d'autres éditeurs du logiciel à l'aide de l'installation des mises à jour nécessaires.

Kaspersky Security Center Cloud Console recherche des mises à jour par la tâche *Recherche de vulnérabilités et de mises à jour requises*. Une fois cette tâche terminée, le Serveur d'administration reçoit la liste des vulnérabilités détectées et des mises à jour requises pour les logiciels tiers installés sur les appareils que vous avez spécifiés dans les propriétés de la tâche. Après la consultation des informations sur les mises à jour disponibles, vous pouvez exécuter l'installation des mises à jour sur les appareils.

La mise à jour de certaines applications Kaspersky Security Center Cloud Console s'effectue par la suppression de la version précédente de l'application et par l'installation d'une nouvelle version.

Une interaction utilisateur peut être requise lorsque vous mettez à jour une application tierce ou corrigez une vulnérabilité dans une application tierce sur un appareil administré. Par exemple, l'utilisateur peut être invité à fermer l'application tierce si elle est actuellement ouverte.

Pour des raisons de sécurité, toutes les mises à jour du logiciel tiers que vous installez à l'aide de la fonction de la gestion des vulnérabilités et des correctifs sont automatiquement analysées à la recherche d'applications malveillantes par les technologies de Kaspersky. Ces technologies sont utilisées pour la vérification automatique des fichiers et incluent la recherche de virus, l'analyse statique, l'analyse dynamique, l'analyse comportementale dans l'environnement sandbox et machine learning.

Les experts de Kaspersky n'effectuent pas d'analyse manuelle des mises à jour du logiciel tiers pouvant être installées par la fonction de la gestion des vulnérabilités et des correctifs. De plus, les experts de Kaspersky ne recherchent pas de vulnérabilités (connues ou inconnues) ou de fonctionnalités non documentées dans ces mises à jour, et n'effectuent pas d'autres types d'analyse des mises à jour que ceux indiqués dans le paragraphe ci-dessus.

Tâches pour l'installation des mises à jour du logiciel tiers

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 les tâches suivantes :

- La tâche *Installation des mises à jour requises et correction des vulnérabilités*

  Cette tâche 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.

  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 Cloud Console 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.

- Tâche *Installation des mises à jour Windows Update*

  Cette tâche peut être utilisée uniquement pour installer les mises à jour Windows Update.

  Lorsque cette tâche est terminée, seules les mises à jour spécifiées dans les propriétés de la tâche sont installées. À l'avenir, si vous souhaitez installer de nouvelles mises à jour, vous devez ajouter les mises à jour requises à la liste des mises à jour de la tâche existante ou créer une nouvelle tâche *Installation des mises à jour Windows Update*.

Les tâches d'installation de mise à jour du logiciel intègrent un certain nombre de limitations. Ces limitations dépendent de la licence sous laquelle vous utilisez Kaspersky Security Center Cloud Console et du mode de fonctionnement de Kaspersky Security Center Cloud Console.

Scénario : mise à jour des logiciels tiers

Cette section fournit un scénario pour la mise à jour des logiciels tiers installés sur les appareils client. Les logiciels tiers comprennent des applications de Microsoft et d'autres fournisseurs de logiciels. Les mises à jour des applications de Microsoft sont fournies par le service Windows Update.

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 Cloud Console 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 démarrage rapide du Serveur d'administration. Si vous n'avez pas exécuté l'assistant, créez la tâche ou exécutez l'assistant de démarrage rapide de l'application maintenant.

Instructions pour :

- Création de la tâche Recherche de vulnérabilités et de mises à jour requises
- La tâche Recherche de vulnérabilités et de mises à jour requises est créée

2. **Analyser la liste des mises à jour trouvées**

Consultez la liste des **Mises à jour du logiciel** et décidez des mises à jour que vous souhaitez installer. Pour consulter les informations détaillées de chaque mise à jour, cliquez sur le nom de la mise à jour dans la liste. Pour chaque mise à jour de la liste, vous pouvez consulter les statistiques de mise à jour sur les appareils administrés. Par exemple, vous pouvez afficher le nombre d'appareils sur lesquels la mise à jour sélectionnée n'est pas installée, doit être installée ou sur lesquels l'installation de la mise à jour a échoué.

Instructions : consultation des informations sur les mises à jour du logiciel tiers disponibles

3. **Configuration de l'installation des mises à jour**

Une fois que Kaspersky Security Center Cloud Console a reçu la liste des mises à jour du logiciel tiers, vous pouvez les installer sur les appareils clients à l'aide de la tâche *Installation des mises à jour requises et correction des vulnérabilités* ou de la tâche *Installation des mises à jour Windows Update*. Créez une de ces tâches. Vous pouvez créer ces tâches sous l'onglet **Tâches** ou à l'aide de la liste **Mises à jour du logiciel**.

La tâche *Installation des mises à jour requises et correction des vulnérabilités* est utilisée pour installer les mises à jour des applications de Microsoft, y compris les mises à jour fournies par le service Windows Update et les mises à jour des logiciels d'autres fournisseurs.

La tâche *Installation des mises à jour Windows Update* peut être utilisée uniquement pour installer les mises à jour Windows Update.

Les tâches d'installation de mise à jour du logiciel intègrent un certain nombre de limitations. Ces limitations dépendent de la licence sous laquelle vous utilisez Kaspersky Security Center Cloud Console et du mode de fonctionnement de Kaspersky Security Center Cloud Console.

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 du logiciel ne sera pas installée.

Instructions pour :

- Création de la tâche Installation des mises à jour requises et correction des vulnérabilités
- Création de la tâche Installation des mises à jour Windows Update
- Consultation des informations sur les mises à jour du logiciel tiers disponibles

4. **Planification des tâches**

Pour vous assurer que la liste des mises à jour est toujours d'actualité, planifiez la tâche *Recherche de vulnérabilités et de mises à jour requises* pour exécuter automatiquement la tâche de temps à autre. La fréquence moyenne par défaut est 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 *Installation des mises à jour Windows Update*, notez que vous devez définir la liste des mises à jour chaque fois avant de démarrer cette tâche.

Lors de la planification des tâches, assurez-vous qu'une tâche pour corriger la vulnérabilité démarre une fois que la tâche *Recherche de vulnérabilités et de mises à jour requises* est terminée.

Instructions pratiques : Paramètres de la tâche générale

5. **Approbation et refus des mises à jour du logiciel (facultatif)**

   Si vous avez créé la tâche *Installation des mises à jour requises et correction des vulnérabilités*, vous pouvez spécifier des règles pour l'installation des mises à jour dans les propriétés de la tâche. Si vous avez créé la tâche *Installation des mises à jour Windows Update*, ne tenez pas compte de cette étape.

   Pour chaque règle, vous pouvez définir les mises à jour à installer en fonction de l'état de la mise à jour : *Non défini*, *Approuvé* ou *Rejeté*. Par exemple, vous pouvez créer une tâche spécifique pour les serveurs et définir une règle pour cette tâche afin de n'autoriser l'installation que des mises à jour de Windows Update et uniquement celles qui disposent de l'état *Approuvé*. Ensuite, vous définissez manuellement l'état *Approuvé* pour les mises à jour que vous souhaitez installer. Dans ce cas, les mises à jour Windows Update qui disposent de l'état *Non défini* ou *Rejeté* ne seront pas installées sur les serveurs que vous avez spécifiés dans la tâche.

   Par défaut, les mises à jour du logiciel téléchargées sont à l'état *Non défini*. Vous pouvez modifier l'état en *Approuvé* ou *Rejeté* dans la liste **Mises à jour du logiciel** (**Opérations** → **Gestion des correctifs** → **Mises à jour du logiciel**).

   Instructions pratiques : approbation et refus de mises à jour du logiciel tiers

6. **Exécution d'une tâche d'installation des mises à jour**

   Lancez la tâche *Installation des mises à jour requises et correction des vulnérabilités* ou la tâche *Installation des mises à jour Windows Update*. Lorsque vous démarrez ces tâches, les mises à jour sont téléchargées et installées sur les appareils administrés. Une fois la tâche terminée, assurez-vous qu'elle possède le statut *Terminée* dans la liste des tâches.

   Instructions pour : Lancer une tâche manuellement

7. **Création du rapport des résultats de l'installation des mises à jour du logiciel tiers (facultatif)**

   Pour vous assurer que la tâche est créée et que les mises à jour sont installées, créez le **Rapport sur les résultats de l'installation des mises à jour du logiciel tiers** et affichez des statistiques détaillées sur l'installation de la mise à jour dans ce rapport.

   Instructions : génération et affichage d'un rapport

Installation des mises à jour du logiciel tiers

Vous pouvez installer des mises à jour du logiciel tiers sur des appareils administrés en utilisant et en exécutant l'une des tâches suivantes :

- *Installation des mises à jour requises et correction des vulnérabilités*

  Vous pouvez utiliser cette tâche pour installer les mises à jour Windows Update fournies par Microsoft et les mises à jour des logiciels d'autres fournisseurs.

- *Installation des mises à jour Windows Update*

  Vous pouvez utiliser cette tâche pour installer uniquement les mises à jour Windows Update.

Les tâches d'installation de mise à jour du logiciel intègrent un certain nombre de limitations. Ces limitations dépendent de la licence sous laquelle vous utilisez Kaspersky Security Center Cloud Console et du mode de fonctionnement de Kaspersky Security Center Cloud Console.

Une interaction utilisateur peut être requise lorsque vous mettez à jour une application tierce ou corrigez une vulnérabilité dans une application tierce sur un appareil administré. Par exemple, l'utilisateur peut être invité à fermer l'application tierce si elle est actuellement ouverte.

Vous pouvez également créer une tâche pour installer les mises à jour requises comme suit :

- En ouvrant la liste des mises à jour et en définissant les mises à jour à installer.

  En conséquence, une nouvelle tâche d'installation des mises à jour sélectionnées est créée. En option, vous pouvez ajouter les mises à jour sélectionnées à une tâche existante.

- En exécutant l'assistant d'installation des mises à jour.

  La disponibilité de l'assistant d'installation des mises à jour dépend du mode de Kaspersky Security Center Cloud Console et de votre licence actuelle.

  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 l'une des listes des mises à jour :

   - Pour ouvrir la liste générale des mises à jour, dans le menu principal, accédez à **Opérations → Gestion des correctifs → Mises à jour du logiciel**.
   - Pour ouvrir la liste des mises à jour d'un appareil administré, dans le menu principal, accédez à **Ressources (Appareils) → Appareils administrés → <nom de l'appareil> → Avancé → Mises à jour non installées**.
   - Pour ouvrir la liste des mises à jour d'une application en particulier, dans le menu principal, accédez à **Opérations → Applications tierces → Registre des applications → <nom de l'application> → Mises à jour 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**.

   Pour installer certaines mises à jour du logiciel, vous devez accepter le Contrat de licence utilisateur final (CLUF). Si vous refusez le CLUF, la mise à jour du logiciel ne sera pas installée.

4. Sélectionnez l'une des options ci-dessous :

   - **Nouvelle tâche**

     Ceci permet de lancer l'assistant de création d'une tâche. La tâche *Installation des mises à jour requises et correction des vulnérabilités* ou la tâche *Installation des mises à jour Windows Update* est présélectionnée, en fonction du mode de Kaspersky Security Center Cloud Console et de votre licence actuelle. 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. Sélectionnez une tâche *Installation des mises à jour requises et correction des vulnérabilités* ou une tâche *Installation des mises à jour Windows Update*. Si vous sélectionnez une tâche *Installation des mises à jour requises et correction des vulnérabilités*, une nouvelle règle pour installer les mises à jour sélectionnées sera automatiquement ajoutée à la tâche sélectionnée. Si vous sélectionnez une tâche *Installation des mises à jour Windows Update*, les mises à jour sélectionnées seront ajoutées aux propriétés de la tâche.

La fenêtre de propriétés de la tâche s'affiche. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications.

Si vous avez choisi de créer une tâche, la tâche est créée et affichée dans la liste des tâches à l'endroit suivant : **Ressources (Appareils)** → **Tâches**. Si vous avez choisi d'ajouter les mises à jour à une tâche existante, les mises à jour sont enregistrées dans les propriétés de la tâche.

Pour installer des mises à jour de logiciel tiers, démarrez la tâche *Installation des mises à jour requises et correction des vulnérabilités* ou la tâche *Installation des mises à jour Windows Update*. Vous pouvez lancer n'importe laquelle de ces tâches manuellement ou spécifier des paramètres de planification dans les propriétés de la tâche que vous lancez. Lorsque vous définissez la planification de la tâche, assurez-vous que la tâche d'installation de la mise à jour est lancée une fois que la tâche *Recherche de vulnérabilités et de mises à jour requises* est terminée.

Installation de mises à jour du logiciel tiers à l'aide de l'assistant d'installation des mises à jour

La disponibilité de cette fonctionnalité dépend du mode de Kaspersky Security Center Cloud Console et de votre licence actuelle.

Pour créer une tâche d'installation des mises à jour du logiciel tiers à l'aide de l'assistant d'installation des mises 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 des mises à jour démarre. La page **Sélection de la tâche d'installation de la mise à jour** affiche la liste de toutes les tâches existantes des types suivants :

   - *Installation des mises à jour requises et correction des vulnérabilités*
   - *Installation des mises à jour Windows Update*
   - *Corriger les vulnérabilités*

   Vous ne pouvez pas modifier les tâches des deux derniers types pour installer de nouvelles mises à jour. Pour installer de nouvelles mises à jour, vous ne pouvez utiliser que les tâches *Installation des mises à jour requises et correction des vulnérabilités*.

4. Si vous souhaitez que l'assistant affiche uniquement les tâches qui installent la mise à jour que vous avez sélectionnée, activez l'option **Afficher uniquement les tâches d'installation de mise à jour**.

5. Choisissez la manière dont vous voulez procéder :

   - Pour démarrer une tâche, cochez la case en regard du nom de la tâche, puis cliquez sur le bouton **Démarrer**.

- Pour ajouter une nouvelle règle à une tâche existante :

  a. Cochez la case en regard du nom de la tâche, puis cliquez sur le bouton **Ajouter une règle**.

  b. Sur la page qui s'ouvre, configurez la nouvelle règle :

  - Règle d'installation 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.

  - Règle d'installation pour les mises à jour de ce niveau d'importance selon MSRC (disponible uniquement pour les mises à jour Windows Update)

    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 (disponible uniquement pour les mises à jour Windows), les mises à jour corrigent uniquement les vulnérabilités dont le niveau de gravité tel que défini par Microsoft Security Response Center (MSRC) est égal ou supérieur à la valeur sélectionnée dans la liste (**Bas**, **Moyen**, **Élevé** ou **Critique**). Les vulnérabilités dont le niveau de gravité est inférieur à la valeur sélectionnée ne sont pas corrigées.

    Si cette option est désactivée, les mises à jour corrigent toutes les vulnérabilités, quel que soit le niveau de gravité.

    Cette option est Inactif par défaut.

  - Règle d'installation des mises à jour de cet éditeur (disponible uniquement pour les mises à jour d'applications tierces)

    Cette option est disponible uniquement pour les mises à jour d'applications tierces. Kaspersky Security Center Cloud Console installe uniquement les mises à jour relatives aux applications créées par le même fournisseur que la mise à jour sélectionnée. Les mises à jour et les mises à jour refusées pour des applications créées par d'autres fournisseurs ne sont pas installées.

    Cette option est Inactif par défaut.

  - **Règle d'installation des mises à jour de type**

  - **Règle d'installation 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 le bouton **Ajouter**.

- Pour créer une tâche, procédez comme suit :

  a. Cliquez sur le bouton **Nouvelle tâche**.

  b. Sur la page qui s'ouvre, configurez la nouvelle règle :

  - Règle d'installation 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.

  - Règle d'installation pour les mises à jour de ce niveau d'importance selon MSRC (disponible uniquement pour les mises à jour Windows Update)

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 (disponible uniquement pour les mises à jour Windows), les mises à jour corrigent uniquement les vulnérabilités dont le niveau de gravité tel que défini par Microsoft Security Response Center (MSRC) est égal ou supérieur à la valeur sélectionnée dans la liste (**Bas**, **Moyen**, **Élevé** ou **Critique**). Les vulnérabilités dont le niveau de gravité est inférieur à la valeur sélectionnée ne sont pas corrigées.

Si cette option est désactivée, les mises à jour corrigent toutes les vulnérabilités, quel que soit le niveau de gravité.

Cette option est Inactif par défaut.

- **Règle d'installation des mises à jour de cet éditeur** (disponible uniquement pour les mises à jour d'applications tierces)

  Cette option est disponible uniquement pour les mises à jour d'applications tierces. Kaspersky Security Center Cloud Console installe uniquement les mises à jour relatives aux applications créées par le même fournisseur que la mise à jour sélectionnée. Les mises à jour et les mises à jour refusées pour des applications créées par d'autres fournisseurs ne sont pas installées.

  Cette option est Inactif par défaut.

- **Règle d'installation des mises à jour de type**

- **Règle d'installation 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 le bouton **Ajouter**.

Si vous avez choisi de démarrer une tâche, vous pouvez fermer l'assistant. La tâche se poursuivra en mode arrière-plan. Il n'y a rien d'autre à faire.

Si vous avez choisi d'ajouter une règle à une tâche existante, la fenêtre des propriétés de la tâche s'ouvre. La nouvelle règle est déjà ajoutée aux propriétés de la tâche. Vous pouvez afficher ou modifier la règle ou d'autres paramètres de tâche. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications.

Si vous avez choisi de créer une tâche, vous continuez à créer la tâche dans l'assistant de création d'une tâche. La nouvelle règle que vous avez ajoutée dans l'assistant d'installation des mises à jour s'affiche dans l'assistant de création d'une tâche. Lorsque vous terminez l'assistant de création d'une tâche, la tâche *Installation des mises à jour requises et correction des vulnérabilités* est ajoutée à la liste des tâches.

Création de la tâche Recherche de vulnérabilités et des mises à jour requises

Grâce à la tâche Recherche de vulnérabilités et de mises à jour requises, Kaspersky Security Center Cloud Console reçoit la liste des vulnérabilités détectées et des mises à jour requises pour les logiciels tiers installés sur les appareils administrés.

La tâche Recherche de vulnérabilités et de mises à jour requises est créée automatiquement lorsque l'assistant de démarrage rapide de l'application est en cours d'exécution. Si vous n'aviez pas exécuté l'assistant, vous pouvez créer la tâche manuellement.

Pour créer la tâche Recherche de vulnérabilités et de mises à jour requises, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Tâches**.
2. Cliquez sur **Ajouter**.

   Ceci permet de lancer l'assistant de création d'une tâche. Suivez les étapes de l'assistant.
3. Pour l'application Kaspersky Security Center Cloud Console, sélectionnez le type de tâche **Recherche de vulnérabilités et de mises à jour requises**.
4. Spécifiez le nom de la tâche créée. Le nom de la tâche ne peut pas contenir plus de 100 symboles et contenir de symboles spéciaux ("*<>?\:|).
5. Sélectionnez les appareils auxquels les tâches seront affectées.
6. Si vous souhaitez modifier les paramètres de la tâche par défaut, activez l'option **Ouvrir les détails de la tâche à la fin de la création** sur la page **Fin de la création de la tâche**. Si vous n'activez pas cette tâche, la tâche est créée selon les paramètres par défaut. Vous pourrez modifier ces paramètres par défaut plus tard, à tout moment.
7. Cliquez sur le bouton **Créer**.

   La tâche est créée et s'affiche dans la liste des tâches.
8. Cliquez sur le nom de la tâche créée pour ouvrir la fenêtre de propriétés de la tâche.
9. Dans la fenêtre des propriétés de la tâche, indiquez les paramètres généraux de la tâche.
10. Dans l'onglet **Paramètres de l'application**, indiquez les paramètres suivants :

    - **Rechercher les vulnérabilités et les mises à jour indiquées par Microsoft**

Lors de la recherche de vulnérabilités et de mises à jour, Kaspersky Security Center Cloud Console utilise les informations sur les mises à jour Microsoft applicables à partir de la source des mises à jour Microsoft disponibles à ce moment là.

Par exemple, pensez à désactiver cette option si vous avez différentes tâches avec différents paramètres pour les mises à jour Microsoft et les mises à jour d'applications tierces.

Cette option est activée par défaut.

Les informations sur les mises à jour facultatives de Microsoft Windows Update ne sont pas envoyées au Serveur d'administration.

- Se connecter au serveur de mise à jour pour mettre à jour les données

L'Agent de mises à jour Windows sur un appareil administré se connecte à la source des mises à jour Microsoft. Les serveurs suivants peuvent servir de source de mises à jour Microsoft :

- Serveur d'administration de Kaspersky Security Center Cloud Console (voir les paramètres de stratégie de l'Agent d'administration)
- Serveur Windows sur lequel Microsoft Windows Server Update Services (WSUS) est déployé dans le réseau de votre organisation
- Serveurs de mises à jour Microsoft

Si cette option est activée, l'Agent de mises à jour Windows sur un appareil administré se connecte à la source de mise à jour Microsoft pour actualiser les informations relatives aux mises à jour Microsoft Windows applicables.

Si cette option est désactivée, l'Agent de mises à jour Windows sur un appareil administré utilise les informations relatives aux mises à jour Microsoft Windows obtenues antérieurement auprès de la source des mises à jour Microsoft.

La connexion à la source des mises à jour Microsoft peut requérir beaucoup de ressources. Pensez à désactiver cette option si vous définissez une connexion régulière à cette source de mises à jour dans une autre tâche ou dans les propriétés de la stratégie de l'Agent d'administration, dans la section **Mises à jour et vulnérabilités du logiciel**. Si vous ne souhaitez pas désactiver cette option, pour réduire la surcharge, vous pouvez configurer la planification des tâches pour randomiser le délai de démarrage des tâches dans les 360 minutes.

Cette option est activée par défaut.

La combinaison des options suivantes des paramètres de la stratégie de l'Agent d'administration définit le mode d'obtention des mises à jour :

- L'Agent de mises à jour Windows sur un appareil administré se connecte au Serveur de mises à jour pour obtenir les mises à jour uniquement si l'option **Se connecter au serveur de mise à jour pour mettre à jour les données** est activée dans les propriétés de la tâche *Recherche de vulnérabilités et de mises à jour requises* et si l'option **Mode de recherche des mises à jour Windows Update** est définie sur **Actif** dans les paramètres de la stratégie de l'Agent d'administration.
- Si vous n'avez pas besoin de l'Agent d'administration pour établir une connexion à la source des mises à jour Microsoft Windows et télécharger les mises à jour lors de l'exécution de la tâche *Recherche de vulnérabilités*, vous pouvez définir l'option **Mode de recherche des mises à jour Windows Update** sur **Passif**, tandis que l'option **Se connecter au serveur de mise à jour pour mettre à jour les données** doit rester activée. Cela vous permet d'économiser des ressources et d'utiliser les mises à jour de Windows déjà reçues pour vérifier la présence de vulnérabilités. Vous pouvez utiliser le mode passif si vous configurez la réception des mises à jour Microsoft Windows différemment. Si la réception des mises à jour Microsoft Windows n'est pas configurée d'une autre manière, ne définissez pas l'option du **Mode de recherche des mises à jour Windows Update** sur **Passif**, car dans ce cas, les informations sur les mises à jour ne seront jamais reçues.
- Quel que soit l'état de l'option **Se connecter au serveur de mise à jour pour mettre à jour les données** (activé ou désactivé), si l'option **Mode de recherche des mises à jour Windows Update** est définie sur **Désactivé**, Kaspersky Security Center Cloud Console ne demande aucune information sur les mises à jour.

- Rechercher les vulnérabilités et les mises à jour de tiers indiquées par Kaspersky

Si cette option est activée, Kaspersky Security Center Cloud Console 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 Cloud Console ne recherche pas les vulnérabilités et les mises à jour requises pour les applications tiers. Par exemple, pensez à désactiver cette option si vous avez différentes tâches avec différents paramètres pour les mises à jour Microsoft Windows et les mises à jour d'applications tierces.

Cette option est activée par défaut.

- **Indiquez les chemins d'accès pour la recherche avancée des applications dans le système de fichiers**

  Les dossiers dans lesquels Kaspersky Security Center Cloud Console 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. La liste est vide par défaut.

- **Activer le diagnostic avancé**

  Quand cette fonction est activée, l'Agent d'administration enregistre les traces même si le traçage est désactivé pour l'agent d'administration dans l'utilitaire de diagnostic à distance Kaspersky Security Center Cloud Console. 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 Cloud Console. Aucune trace complémentaire n'est écrite.

  Lors de la création d'une tâche, il n'est pas nécessaire d'activer le diagnostic avancé. Par contre, vous pouvez activer cette fonction plus tard si, par exemple, une tâche échoue sur certains appareils et que vous souhaitez obtenir des informations complémentaires lors d'une autre exécution de la tâche.

  Cette option est Inactif par défaut.

- **Taille maximale (Mo) des fichiers de diagnostic avancé**

  La valeur par défaut est de 100 Mo, mais elle peut se situer entre 1 et 2 048 Mo. Il peut arriver qu'un expert du Support Technique de Kaspersky vous demande de modifier la valeur par défaut lorsque les informations reprises dans les fichiers de diagnostic avancés que vous avez envoyés ne suffisent pas pour résoudre le problème.

11. Cliquez sur le bouton **Enregistrer**.

La tâche est créée et configurée.

Si les résultats de la tâche contiennent un avertissement concernant l'erreur 0x80240033 " Erreur de l'agent de mise à jour Windows 80240033 (" Les conditions de licence n'ont pas pu être téléchargées ") ", vous pouvez résoudre ce problème via le registre Windows.

La tâche Recherche de vulnérabilités et de mises à jour requises est créée

La tâche *Recherche de vulnérabilités et de mises à jour requises* est créée automatiquement lorsque l'assistant de démarrage rapide de l'application est en cours d'exécution. Si vous n'aviez pas exécuté l'assistant, vous pouvez créer la tâche manuellement.

En plus des paramètres de la tâche générale, vous pouvez indiquer les paramètres suivants lors de la création de la tâche *Recherche de vulnérabilités et de mises à jour requises*, ou plus tard, lorsque vous configurez les propriétés de la tâche créée :

- **Rechercher les vulnérabilités et les mises à jour indiquées par Microsoft**

  Lors de la recherche de vulnérabilités et de mises à jour, Kaspersky Security Center Cloud Console utilise les informations sur les mises à jour Microsoft applicables à partir de la source des mises à jour Microsoft disponibles à ce moment là.

  Par exemple, pensez à désactiver cette option si vous avez différentes tâches avec différents paramètres pour les mises à jour Microsoft et les mises à jour d'applications tierces.

  Cette option est activée par défaut.

  Les informations sur les mises à jour facultatives de Microsoft Windows Update ne sont pas envoyées au Serveur d'administration.

- **Se connecter au serveur de mise à jour pour mettre à jour les données**

L'Agent de mises à jour Windows sur un appareil administré se connecte à la source des mises à jour Microsoft. Les serveurs suivants peuvent servir de source de mises à jour Microsoft :

- Serveur d'administration de Kaspersky Security Center Cloud Console (voir les paramètres de stratégie de l'Agent d'administration)
- Serveur Windows sur lequel Microsoft Windows Server Update Services (WSUS) est déployé dans le réseau de votre organisation
- Serveurs de mises à jour Microsoft

Si cette option est activée, l'Agent de mises à jour Windows sur un appareil administré se connecte à la source de mise à jour Microsoft pour actualiser les informations relatives aux mises à jour Microsoft Windows applicables.

Si cette option est désactivée, l'Agent de mises à jour Windows sur un appareil administré utilise les informations relatives aux mises à jour Microsoft Windows obtenues antérieurement auprès de la source des mises à jour Microsoft.

La connexion à la source des mises à jour Microsoft peut requérir beaucoup de ressources. Pensez à désactiver cette option si vous définissez une connexion régulière à cette source de mises à jour dans une autre tâche ou dans les propriétés de la stratégie de l'Agent d'administration, dans la section **Mises à jour et vulnérabilités du logiciel**. Si vous ne souhaitez pas désactiver cette option, pour réduire la surcharge, vous pouvez configurer la planification des tâches pour randomiser le délai de démarrage des tâches dans les 360 minutes.

Cette option est activée par défaut.

La combinaison des options suivantes des paramètres de la stratégie de l'Agent d'administration définit le mode d'obtention des mises à jour :

- L'Agent de mises à jour Windows sur un appareil administré se connecte au Serveur de mises à jour pour obtenir les mises à jour uniquement si l'option **Se connecter au serveur de mise à jour pour mettre à jour les données** est activée dans les propriétés de la tâche *Recherche de vulnérabilités et de mises à jour requises* et si l'option **Mode de recherche des mises à jour Windows Update** est définie sur **Actif** dans les paramètres de la stratégie de l'Agent d'administration.
- Si vous n'avez pas besoin de l'Agent d'administration pour établir une connexion à la source des mises à jour Microsoft Windows et télécharger les mises à jour lors de l'exécution de la tâche *Recherche de vulnérabilités*, vous pouvez définir l'option **Mode de recherche des mises à jour Windows Update** sur **Passif**, tandis que l'option **Se connecter au serveur de mise à jour pour mettre à jour les données** doit rester activée. Cela vous permet d'économiser des ressources et d'utiliser les mises à jour de Windows déjà reçues pour vérifier la présence de vulnérabilités. Vous pouvez utiliser le mode passif si vous configurez la réception des mises à jour Microsoft Windows différemment. Si la réception des mises à jour Microsoft Windows n'est pas configurée d'une autre manière, ne définissez pas l'option du **Mode de recherche des mises à jour Windows Update** sur **Passif**, car dans ce cas, les informations sur les mises à jour ne seront jamais reçues.
- Quel que soit l'état de l'option **Se connecter au serveur de mise à jour pour mettre à jour les données** (activé ou désactivé), si l'option **Mode de recherche des mises à jour Windows Update** est définie sur **Désactivé**, Kaspersky Security Center Cloud Console ne demande aucune information sur les mises à jour.

- Rechercher les vulnérabilités et les mises à jour de tiers indiquées par Kaspersky

Si cette option est activée, Kaspersky Security Center Cloud Console 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 Cloud Console ne recherche pas les vulnérabilités et les mises à jour requises pour les applications tiers. Par exemple, pensez à désactiver cette option si vous avez différentes tâches avec différents paramètres pour les mises à jour Microsoft Windows et les mises à jour d'applications tierces.

Cette option est activée par défaut.

- **Indiquez les chemins d'accès pour la recherche avancée des applications dans le système de fichiers**

  Les dossiers dans lesquels Kaspersky Security Center Cloud Console 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. La liste est vide par défaut.

- **Activer le diagnostic avancé**

  Quand cette fonction est activée, l'Agent d'administration enregistre les traces même si le traçage est désactivé pour l'agent d'administration dans l'utilitaire de diagnostic à distance Kaspersky Security Center Cloud Console. 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 Cloud Console. Aucune trace complémentaire n'est écrite.

  Lors de la création d'une tâche, il n'est pas nécessaire d'activer le diagnostic avancé. Par contre, vous pouvez activer cette fonction plus tard si, par exemple, une tâche échoue sur certains appareils et que vous souhaitez obtenir des informations complémentaires lors d'une autre exécution de la tâche.

  Cette option est Inactif par défaut.

- **Taille maximale (Mo) des fichiers de diagnostic avancé**

  La valeur par défaut est de 100 Mo, mais elle peut se situer entre 1 et 2 048 Mo. Il peut arriver qu'un expert du Support Technique de Kaspersky vous demande de modifier la valeur par défaut lorsque les informations reprises dans les fichiers de diagnostic avancés que vous avez envoyés ne suffisent pas pour résoudre le problème.

Recommandations sur la planification des tâches

Lors de la planification de la tâche *Recherche de vulnérabilités et de mises à jour requises*, assurez-vous que les deux options **Lancer les tâches non exécutées** et **Adopter un décalage aléatoire automatique pour les lancements de tâche** sont activées.

Par défaut, la tâche *Recherche de vulnérabilités et de mises à jour requises* est configurée pour démarrer manuellement. Si le règlement de travail de la société prévoit la désactivation des appareils à ce moment, la tâche *Recherche de vulnérabilités et de mises à jour requises* est lancée après l'activation de l'appareil, c'est-à-dire le matin du lendemain. Ce comportement est à éviter car la recherche de vulnérabilités peut augmenter la charge sur le processeur et le sous-système de disque de l'appareil. Vous devez configurer une programmation optimale de cette tâche sur la base du règlement de travail adopté par l'entreprise.

Création de la tâche Installer les mises à jour requises et corriger les vulnérabilités

La disponibilité de la tâche *Installation des mises à jour requises et correction des vulnérabilités* dépend du mode de Kaspersky Security Center Cloud Console et de votre licence actuelle.

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.

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.

Les tâches d'installation de mise à jour du logiciel intègrent un certain nombre de limitations. Ces limitations dépendent de la licence sous laquelle vous utilisez Kaspersky Security Center Cloud Console et du mode de fonctionnement de Kaspersky Security Center Cloud Console.

Pour créer une tâche Installation des mises à jour requises et correction des vulnérabilités :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Tâches**.
2. Cliquez sur **Ajouter**.

   Ceci permet de lancer l'assistant de création d'une tâche. Suivez les étapes de l'assistant.
3. Pour l'application Kaspersky Security Center Cloud Console, sélectionnez le type de tâche **Installation des mises à jour requises et correction des vulnérabilités**.
4. Spécifiez le nom de la tâche créée. Le nom de la tâche ne peut pas contenir plus de 100 symboles et contenir de symboles spéciaux ("*<>?\:|).
5. Sélectionnez les appareils auxquels les tâches seront affectées.
6. Indiquez les règles d'installation des mises à jour, puis définissez les paramètres suivants :
   - **Commencer l'installation au moment du redémarrage ou de l'arrêt de l'appareil**

Si cette option est activée, les mises à jour sont installées lors du redémarrage ou de l'arrêt de l'appareil. Dans le cas contraire, les mises à jour sont installées selon la programmation.

Utilisez cette option si l'installation des mises à jour peut avoir un impact sur les performances de l'appareil.

Cette option est Inactif par défaut.

- **Installer les modules système général requis**

  Si cette option est activée, l'application, avant d'installer une mise à jour, installe automatiquement tous les composants généraux système (prérequis) requis pour l'installation de la mise à jour. Par exemple, il peut s'agir des mises à jour du système d'exploitation.

  Si cette option est désactivée, vous devrez peut-être installer les prérequis manuellement.

  Cette option est Inactif par défaut.

- **Autoriser l'installation de nouvelles versions de l'application lors des mises à jour**

  Si cette option est activée, les mises à jour sont autorisées lorsqu'elles entraînent l'installation d'une nouvelle version d'un logiciel.

  Si cette option est désactivée, le logiciel n'est pas mis à jour. Vous pouvez alors installer les nouvelles versions du logiciel manuellement ou via un autre tâche. Par exemple, vous pouvez utiliser cette option si l'infrastructure de votre entreprise n'est pas prise en charge par une nouvelle version du logiciel ou si vous souhaitez vérifier une mise à jour dans une infrastructure d'essai.

  Cette option est activée par défaut.

  La mise à jour d'une application peut provoquer un dysfonctionnement des applications dépendantes installées sur les appareils clients.

- **Télécharger les mises à jour sur l'appareil sans les installer**

  Quand cette option est activée, l'application télécharge les mises à jour sur l'appareil, mais ne les installe pas automatiquement. Vous pouvez installer les mises à jour manuellement par la suite.

  Les mises à jour Microsoft sont téléchargées dans le stockage Windows système. Les mises à jour des produits tiers (applications développées par des éditeurs d'application autres que Kaspersky et Microsoft) sont téléchargées dans le dossier indiqué dans le champ **Télécharger les mises à jour sur**.

  Si cette option est désactivée, les mises à jour sont installées automatiquement sur l'appareil.

  Cette option est Inactif par défaut.

- **Télécharger les mises à jour sur**

  Ce dossier est utilisé dans le cadre du téléchargement des mises à jour de produits tiers (applications développées par des éditeurs de logiciels autres que Kaspersky et Microsoft).

- **Activer le diagnostic avancé**

Quand cette fonction est activée, l'Agent d'administration enregistre les traces même si le traçage est désactivé pour l'agent d'administration dans l'utilitaire de diagnostic à distance Kaspersky Security Center Cloud Console. 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 Cloud Console. Aucune trace complémentaire n'est écrite.

Lors de la création d'une tâche, il n'est pas nécessaire d'activer le diagnostic avancé. Par contre, vous pouvez activer cette fonction plus tard si, par exemple, une tâche échoue sur certains appareils et que vous souhaitez obtenir des informations complémentaires lors d'une autre exécution de la tâche.

Cette option est Inactif par défaut.

- Taille maximale (Mo) des fichiers de diagnostic avancé

  La valeur par défaut est de 100 Mo, mais elle peut se situer entre 1 et 2 048 Mo. Il peut arriver qu'un expert du Support Technique de Kaspersky vous demande de modifier la valeur par défaut lorsque les informations reprises dans les fichiers de diagnostic avancés que vous avez envoyés ne suffisent pas pour résoudre le problème.

7. Définissez les paramètres de redémarrage du système d'exploitation :

- Ne pas redémarrer l'appareil

  Les appareils clients ne redémarrent pas automatiquement après l'opération. Pour arrêter le fonctionnement, il faut redémarrer l'appareil (par exemple, manuellement ou à l'aide d'une tâche d'administration des appareils). Les informations sur la nécessité du redémarrage sont enregistrées dans les résultats de la tâche et dans l'état de l'appareil. Cette option convient aux tâches d' sur les serveurs et autres appareils pour lesquels la continuité des opérations est critique.

- Redémarrer l'appareil

  Dans ce cas, le redémarrage des appareils clients est toujours exécuté automatiquement, si celui-ci est requis pour terminer l'opération. Cette option convient aux tâches d' sur des appareils pour lesquels des interruptions périodiques sont admises (débranchement, redémarrage).

- Confirmer l'action auprès de l'utilisateur

  Le message qui signale que l'appareil client doit être redémarré manuellement s'affiche sur l'écran de l'appareil. Pour cette option, il est possible de configurer des paramètres avancés : le texte du message pour l'utilisateur, la fréquence du message, ainsi que le délai à l'issue duquel le redémarrage sera forcé (sans confirmation de l'utilisateur). Cette option convient le mieux pour les postes de travail sur lesquels les utilisateurs doivent pouvoir sélectionner l'heure de redémarrage qui leur convient le mieux.

  Cette option est sélectionnée par défaut.

- Répéter la demande toutes les (min.)

Quand cette option est activée, l'application invite l'utilisateur à redémarrer le système d'exploitation selon la fréquence indiquée.

Cette option est activée par défaut. L'intervalle par défaut est de 5 minutes. La valeur peut être comprise entre 1 et 1 440 minutes.

Si cette option est désactivée, l'invite est affichée une seule fois.

- **Redémarrer le système au bout de (min.)**

  Après avoir averti l'utilisateur, l'application force le redémarrage du système d'exploitation à l'issue de l'intervalle défini.

  Cette option est activée par défaut. Le délai par défaut est de 30 minutes. La valeur peut être comprise entre 1 et 1 440 minutes.

- **Délai d'attente avant la fermeture forcée des ap&plications dans les sessions bloquées (min)**

  Arrêt forcé des applications lorsque l'appareil de l'utilisateur est verrouillé (arrêt manuel ou automatique après une période d'inactivité).

  Si cette option est activée, les applications en cours sur l'appareil verrouillé seront fermées de force à la fin du délai indiqué dans le champ situé à côté de la case.

  Si cette option est activée, les applications en cours sur l'appareil verrouillé ne seront pas fermées.

  Cette option est Inactif par défaut.

8. Si sur la page **Fin de la création de la tâche** vous activez l'option **Ouvrir les détails de la tâche à la fin de la création**, vous pouvez modifier les paramètres de la tâche par défaut. Si vous n'activez pas cette tâche, la tâche est créée selon les paramètres par défaut. Vous pourrez modifier ces paramètres par défaut plus tard, à tout moment.

9. Cliquez sur le bouton **Terminer**.

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

10. Cliquez sur le nom de la tâche créée pour ouvrir la fenêtre de propriétés de la tâche.

11. Dans la fenêtre des propriétés de la tâche, indiquez les paramètres généraux de la tâche en fonction de vos besoins.

12. Cliquez sur le bouton **Enregistrer**.

    La tâche est créée et configurée.

Si les résultats de la tâche contiennent un avertissement concernant l'erreur 0x80240033 " Erreur de l'agent de mise à jour Windows 80240033 (" Les conditions de licence n'ont pas pu être téléchargées ") ", vous pouvez résoudre ce problème via le registre Windows.

Ajout de règles pour l'installation de la mise à jour

La disponibilité de cette fonctionnalité dépend du mode de Kaspersky Security Center Cloud Console et de votre licence actuelle.

Lors de l'installation de mises à jour du logiciel ou de la correction de la vulnérabilité dans les applications à l'aide de la tâche *Installation des mises à jour requises et correction des vulnérabilités*, vous devez définir les règles pour l'installation de la mise à jour. Ces règles déterminent les mises à jour à installer et les vulnérabilités à corriger.

Les paramètres exacts dépendent de l'objet pour lequel vous ajoutez une règle : pour toutes les mises à jour, pour les mises à jour Windows Update ou pour les mises à jour d'applications tierces (applications développées par des éditeurs autres que Kaspersky et Microsoft). Lors de l'ajout d'une règle pour des mises à jour Windows Update ou des mises à jour d'applications tierces, vous pouvez sélectionner des applications spécifiques et les versions de l'application pour lesquelles vous souhaitez installer les mises à jour. Lors de l'ajout d'une règle pour toutes les mises à jour, vous pouvez sélectionner les mises à jour spécifiques que vous souhaitez installer et les vulnérabilités que vous souhaitez éliminer via l'installation des mises à jour.

Vous pouvez ajouter une règle pour l'installation de la mise à jour comme suit :

- En ajoutant une règle lors de la création d'une nouvelle tâche Installation des mises à jour requises et correction des vulnérabilités.
- En ajoutant une règle sous l'onglet **Paramètres de l'application** dans la fenêtre des propriétés d'une tâche *Installation des mises à jour requises et correction des vulnérabilités* existante.
- Via l'assistant d'installation des mises à jour ou l'assistant de correction des vulnérabilités.

Pour ajouter une nouvelle règle pour toutes les mises à jour, procédez comme suit :

1. Cliquez sur le bouton **Ajouter**.

   L'Assistant de création de règles se lance. Parcourez les étapes de l'assistant à l'aide du bouton **Suivant**.

2. Sur la page **Type de règle**, sélectionnez **Règle pour toutes les mises à jour**.

3. Sur la page **Critères généraux**, utilisez les listes déroulantes pour définir les paramètres suivants :

   - **Définir les mises à jour à installer**

     Sélectionnez les mises à jour qui doivent être installées sur les appareils clients :

     - **Installer uniquement les mises à jour confirmées**. Cette option installe uniquement les mises à jour confirmées.
     - **Installer toutes les mises à jour (sauf les mises à jour rejetées)**. Cette option installe les mises à jour avec l'état *Approuvé* ou *Non défini*.
     - **Installer toutes les mises à jour (y compris les mises à jour rejetées)**. Ceci installe toutes les mises à jour, quel que soit leur état d'approbation. Sélectionnez cette option avec prudence. Par exemple, utilisez cette option si vous souhaitez vérifier l'installation de certaines mises à jour rejetées dans une infrastructure d'essai.

   - **Corriger les vulnérabilités de niveau de gravité égal ou supérieur à**

Parfois, les mises à jour du logiciel peuvent nuire à l'expérience de l'utilisateur. Dans ce cas, il se peut que vous décidiez d'installer uniquement les mises à jour critiques au fonctionnement du logiciel et d'ignorer les autres.

Quand cette option est activée, les mises à jour corrigent uniquement les vulnérabilités dont le niveau de gravité tel que défini par Kaspersky est égal ou supérieur à la valeur sélectionnée dans la liste (**Moyenne**, **Élevé** ou **Critique**). Les vulnérabilités dont le niveau de gravité est inférieur à la valeur sélectionnée ne sont pas corrigées.

Si cette option est désactivée, les mises à jour corrigent toutes les vulnérabilités, quel que soit le niveau de gravité.

Cette option est Inactif par défaut.

4. Sur la page **Mises à jour**, sélectionnez les mises à jour à installer :

- **Installer toutes les mises à jour convenables**

  Installez toutes les mises à jour du logiciel qui répondent aux critères définis à la page **Critères généraux** de l'assistant. Sélectionné par défaut.

- **Installer uniquement les mises à jour depuis la liste**

  Installer uniquement les mises à jour du logiciel que vous sélectionnez manuellement dans la liste. Cette liste contient toutes les mises à jour du logiciel disponibles.

  Par exemple, vous pouvez sélectionner des mises à jour spécifiques dans les cas suivants : pour vérifier leur installation dans un environnement d'essai, pour mettre à jour uniquement les applications critiques ou pour mettre à jour uniquement certaines applications.

- **&Installer automatiquement toutes les mises à jour précédentes des applications nécessaires à l'installation des mises à jour sélectionnées**

  Conservez cette option si vous acceptez l'installation de versions de l'application intermédiaires quand l'impose l'installation des mises à jour sélectionnées.

  Si vous désactivez cette option, seules les versions sélectionnées des applications sont installées. Désactivez cette option si vous souhaitez mettre à jour les applications d'une manière directe, sans tenter d'installer les versions successives. S'il est impossible d'installer les mises à jour sélectionnées sans installer les versions antérieures de l'application, la mise à jour de l'application échoue.

  Admettons que la version 3 d'une application est installée sur un appareil et vous souhaitez réaliser la mise à jour jusque la version 5, mais la version 5 de cette application peut être installée uniquement sur la version 4. Quand cette option est installée, le logiciel installe d'abord la version 4, puis la version 5. Si l'option est désactivée, le logiciel ne parvient pas à mettre l'application à jour.

  Cette option est activée par défaut.

5. Sur la page **Vulnérabilités**, sélectionnez les vulnérabilités que seront corrigées suite à l'installation des mises à jour sélectionnées :

- **Corriger toutes les vulnérabilités qui correspondent aux autres critères**

  Corrigez toutes les vulnérabilités qui satisfont les critères définis à la page **Critères généraux** de l'assistant. Sélectionné par défaut.

- **Corriger uniquement les vulnérabilités depuis la liste**

Corrigez uniquement les vulnérabilités que vous sélectionnez manuellement dans la liste. Cette liste contient toutes les vulnérabilités détectées.

Par exemple, vous pouvez sélectionner des vulnérabilités spécifiques dans les cas suivants : pour vérifier les corrections dans un environnement d'essai, pour corriger les vulnérabilités uniquement dans les applications critiques ou pour corriger les vulnérabilités uniquement dans certaines applications.

6. La page **Nom** permet de renseigner le nom de la règle ajoutée. Vous pouvez changer ce nom plus tard dans la section **Paramètres** de la fenêtre des propriétés de la tâche créée.

Une fois que l'assistant de création de règles a terminé, la nouvelle règle est ajoutée et s'affiche dans la liste des règles de l'assistant de création d'une tâche ou dans les propriétés de la tâche.

Pour ajouter une nouvelle règle pour les mises à jour de Windows Update, procédez comme suit :

1. Cliquez sur le bouton **Ajouter**.

   L'Assistant de création de règles se lance. Parcourez les étapes de l'assistant à l'aide du bouton **Suivant**.

2. Sur la page **Type de règle**, sélectionnez **Règle pour les mises à jour Windows Update**.

3. Dans la fenêtre **Conditions générales**, configurez les paramètres suivants :

- **Définir les mises à jour à installer**

  Sélectionnez les mises à jour qui doivent être installées sur les appareils clients :

  - **Installer uniquement les mises à jour confirmées**. Cette option installe uniquement les mises à jour confirmées.
  - **Installer toutes les mises à jour (sauf les mises à jour rejetées)**. Cette option installe les mises à jour avec l'état *Approuvé* ou *Non défini*.
  - **Installer toutes les mises à jour (y compris les mises à jour rejetées)**. Ceci installe toutes les mises à jour, quel que soit leur état d'approbation. Sélectionnez cette option avec prudence. Par exemple, utilisez cette option si vous souhaitez vérifier l'installation de certaines mises à jour rejetées dans une infrastructure d'essai.

- **Corriger les vulnérabilités de niveau de gravité égal ou supérieur à**

  Parfois, les mises à jour du logiciel peuvent nuire à l'expérience de l'utilisateur. Dans ce cas, il se peut que vous décidiez d'installer uniquement les mises à jour critiques au fonctionnement du logiciel et d'ignorer les autres.

  Quand cette option est activée, les mises à jour corrigent uniquement les vulnérabilités dont le niveau de gravité tel que défini par Kaspersky est égal ou supérieur à la valeur sélectionnée dans la liste (**Moyenne**, **Élevé** ou **Critique**). Les vulnérabilités dont le niveau de gravité est inférieur à la valeur sélectionnée ne sont pas corrigées.

  Si cette option est désactivée, les mises à jour corrigent toutes les vulnérabilités, quel que soit le niveau de gravité.

  Cette option est Inactif par défaut.

- **Corriger les vulnérabilités qui présentent un niveau de gravité selon MSRC égal ou supérieur à**

Parfois, les mises à jour du logiciel peuvent nuire à l'expérience de l'utilisateur. Dans ce cas, il se peut que vous décidiez d'installer uniquement les mises à jour critiques au fonctionnement du logiciel et d'ignorer les autres.

Quand cette option est activée, les mises à jour corrigent uniquement les vulnérabilités dont le niveau de gravité tel que défini par Microsoft Security Response Center (MSRC) est égal ou supérieur à la valeur sélectionnée dans la liste (**Bas**, **Moyenne**, **Élevé** ou **Critique**). Les vulnérabilités dont le niveau de gravité est inférieur à la valeur sélectionnée ne sont pas corrigées.

Si cette option est désactivée, les mises à jour corrigent toutes les vulnérabilités, quel que soit le niveau de gravité.

Cette option est Inactif par défaut.

4. Sur la page **Applications**, sélectionnez les applications et les versions des applications pour lesquelles vous voulez installer les mises à jour. Toutes les applications sont cochées par défaut.

5. Sur la page **Catégorie des mises à jour**, sélectionnez les catégories des mises à jour à installer. Ces catégories sont les mêmes que dans le catalogue Microsoft Update. Toutes les catégories sont cochées par défaut.

6. La page **Nom** permet de renseigner le nom de la règle ajoutée. Vous pouvez changer ce nom plus tard dans la section **Paramètres** de la fenêtre des propriétés de la tâche créée.

Une fois que l'assistant de création de règles a terminé, la nouvelle règle est ajoutée et s'affiche dans la liste des règles de l'assistant de création d'une tâche ou dans les propriétés de la tâche.

Pour ajouter une règle pour les mises à jour des produits tiers, procédez comme suit :

1. Cliquez sur le bouton **Ajouter**.

   L'Assistant de création de règles se lance. Parcourez les étapes de l'assistant à l'aide du bouton **Suivant**.

2. Sur la page **Type de règle**, sélectionnez **Règles pour les mises à jour tierces**.

3. Dans la fenêtre **Conditions générales**, configurez les paramètres suivants :

   - **Définir les mises à jour à installer**

     Sélectionnez les mises à jour qui doivent être installées sur les appareils clients :

     - **Installer uniquement les mises à jour confirmées**. Cette option installe uniquement les mises à jour confirmées.
     - **Installer toutes les mises à jour (sauf les mises à jour rejetées)**. Cette option installe les mises à jour avec l'état *Approuvé* ou *Non défini*.
     - **Installer toutes les mises à jour (y compris les mises à jour rejetées)**. Ceci installe toutes les mises à jour, quel que soit leur état d'approbation. Sélectionnez cette option avec prudence. Par exemple, utilisez cette option si vous souhaitez vérifier l'installation de certaines mises à jour rejetées dans une infrastructure d'essai.

   - **Corriger les vulnérabilités de niveau de gravité égal ou supérieur à**

Parfois, les mises à jour du logiciel peuvent nuire à l'expérience de l'utilisateur. Dans ce cas, il se peut que vous décidiez d'installer uniquement les mises à jour critiques au fonctionnement du logiciel et d'ignorer les autres.

Quand cette option est activée, les mises à jour corrigent uniquement les vulnérabilités dont le niveau de gravité tel que défini par Kaspersky est égal ou supérieur à la valeur sélectionnée dans la liste (**Moyenne**, **Élevé** ou **Critique**). Les vulnérabilités dont le niveau de gravité est inférieur à la valeur sélectionnée ne sont pas corrigées.

Si cette option est désactivée, les mises à jour corrigent toutes les vulnérabilités, quel que soit le niveau de gravité.

Cette option est Inactif par défaut.

4. Sur la page **Applications**, sélectionnez les applications et les versions des applications pour lesquelles vous voulez installer les mises à jour. Toutes les applications sont cochées par défaut.

5. La page **Nom** permet de renseigner le nom de la règle ajoutée. Vous pouvez changer ce nom plus tard dans la section Paramètres de la fenêtre des propriétés de la tâche créée.

Une fois que l'assistant de création de règles a terminé, la nouvelle règle est ajoutée et s'affiche dans la liste des règles de l'assistant de création d'une tâche ou dans les propriétés de la tâche.

Création de la tâche Installation des mises à jour Windows Update

La tâche Installation des mises à jour Windows Update vous permet d'installer les mises à jour du logiciel fournies par le service Windows Update sur les appareils client.

Les tâches d'installation de mise à jour du logiciel intègrent un certain nombre de limitations. Ces limitations dépendent de la licence sous laquelle vous utilisez Kaspersky Security Center Cloud Console et du mode de fonctionnement de Kaspersky Security Center Cloud Console.

Pour créer la tâche Installation des mises à jour Windows Update :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Tâches**.

2. Cliquez sur **Ajouter**.

   Ceci permet de lancer l'assistant de création d'une tâche. Parcourez les étapes de l'assistant à l'aide du bouton **Suivant**.

3. Pour l'application Kaspersky Security Center Cloud Console, sélectionnez le type de tâche **Installation des mises à jour Windows Update**.

4. Spécifiez le nom de la tâche créée.

   Le nom de la tâche ne peut pas contenir plus de 100 symboles et contenir de symboles spéciaux ("*<>?\:|).

5. Sélectionnez les appareils auxquels les tâches seront affectées.

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

   La liste des mises à jour s'ouvre.

7. Sélectionnez les mises à jour Windows Update que vous souhaitez installer, puis cliquez sur **OK**.

8. Définissez les paramètres de redémarrage du système d'exploitation :

- **Ne pas redémarrer l'appareil**

  Les appareils clients ne redémarrent pas automatiquement après l'opération. Pour arrêter le fonctionnement, il faut redémarrer l'appareil (par exemple, manuellement ou à l'aide d'une tâche d'administration des appareils). Les informations sur la nécessité du redémarrage sont enregistrées dans les résultats de la tâche et dans l'état de l'appareil. Cette option convient aux tâches d' sur les serveurs et autres appareils pour lesquels la continuité des opérations est critique.

- **Redémarrer l'appareil**

  Dans ce cas, le redémarrage des appareils clients est toujours exécuté automatiquement, si celui-ci est requis pour terminer l'opération. Cette option convient aux tâches d' sur des appareils pour lesquels des interruptions périodiques sont admises (débranchement, redémarrage).

- **Confirmer l'action auprès de l'utilisateur**

  Le message qui signale que l'appareil client doit être redémarré manuellement s'affiche sur l'écran de l'appareil. Pour cette option, il est possible de configurer des paramètres avancés : le texte du message pour l'utilisateur, la fréquence du message, ainsi que le délai à l'issue duquel le redémarrage sera forcé (sans confirmation de l'utilisateur). Cette option convient le mieux pour les postes de travail sur lesquels les utilisateurs doivent pouvoir sélectionner l'heure de redémarrage qui leur convient le mieux.

  Cette option est sélectionnée par défaut.

- **Répéter la demande toutes les (min.)**

  Quand cette option est activée, l'application invite l'utilisateur à redémarrer le système d'exploitation selon la fréquence indiquée.

  Cette option est activée par défaut. L'intervalle par défaut est de 5 minutes. La valeur peut être comprise entre 1 et 1 440 minutes.

  Si cette option est désactivée, l'invite est affichée une seule fois.

- **Redémarrer le système au bout de (min.)**

  Après avoir averti l'utilisateur, l'application force le redémarrage du système d'exploitation à l'issue de l'intervalle défini.

  Cette option est activée par défaut. Le délai par défaut est de 30 minutes. La valeur peut être comprise entre 1 et 1 440 minutes.

- **Forcer la fermeture des applications dans les sessions bloquées**

Les applications en cours d'exécution peuvent empêcher le redémarrage de l'appareil client. Par exemple, si un document est en train d'être modifié dans un logiciel de traitement de texte et qu'il n'est pas enregistré, l'application n'autorise pas le redémarrage de l'appareil.

Quand cette option est activée, l'arrêt forcé de ces applications sur un appareil verrouillé doit avoir lieu avant de pouvoir redémarrer l'appareil. Les utilisateurs pourraient perdre toute modification qui n'a pas été enregistrée à ce moment.

Si cette option est désactivée, un appareil verrouillé n'est pas redémarré. L'état de la tâche sur cet appareil indique qu'il faut redémarrer l'appareil. Les utilisateurs doivent quitter manuellement toutes les applications en cours d'exécution sur les appareils verrouillés, puis redémarrer ces appareils.

Cette option est Inactif par défaut.

9. Définissez les paramètres du compte :

   - **Compte par défaut**

     La tâche sera lancée sous le même compte utilisateur sous lequel l'application, exécutant cette tâche, a été installée et lancée.

     Cette option est sélectionnée par défaut.

   - **Indiquer un compte**

     Remplissez les champs **Compte utilisateur** et **Mot de passe** pour définir les détails d'un compte à partir duquel la tâche est exécutée. Le compte doit disposer de droits suffisants pour cette tâche.

   - **Compte**

     Le compte utilisateur au nom duquel la tâche sera lancée.

   - **Mot de passe**

     Mot de passe du compte utilisateur au nom duquel la tâche sera lancée.

10. Si vous souhaitez modifier les paramètres de la tâche par défaut, activez l'option **Ouvrir les détails de la tâche à la fin de la création** sur la page **Fin de la création de la tâche**. Si vous n'activez pas cette tâche, la tâche est créée selon les paramètres par défaut. Vous pourrez modifier ces paramètres par défaut plus tard, à tout moment.

11. Cliquez sur le bouton **Terminer**.

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

12. Cliquez sur le nom de la tâche créée pour ouvrir la fenêtre de propriétés de la tâche.

13. Dans la fenêtre des propriétés de la tâche, indiquez les paramètres généraux de la tâche en fonction de vos besoins.

14. Cliquez sur le bouton **Enregistrer**.

La tâche est créée et configurée.

Consultation des informations sur les mises à jour du logiciel tiers disponibles

Vous pouvez consulter la liste des mises à jour disponibles pour les logiciels tiers, y compris les logiciels Microsoft installés sur les appareils client.

Pour consulter la liste des mises à jour disponibles pour les applications tierces installées sur les appareils client,

Dans le menu principal, accédez à **Opérations** → **Gestion des correctifs** → **Mises à jour du logiciel**.

Une liste des mises à jour disponibles s'affiche.

Vous pouvez indiquer un filtre pour consulter la liste des mises à jour du logiciel. Cliquez sur l'icône **Filtre** ( ) dans le coin supérieur droit de la liste des mises à jour du logiciel pour gérer le filtre. Vous pouvez également sélectionner l'un des filtres prédéfinis dans la liste déroulante **Filtres prédéfinis** située au-dessus de la liste des vulnérabilités dans les applications.

Pour consulter les propriétés de la mise à jour, procédez comme suit :

1. Cliquez sur le nom de la mise à jour du logiciel concernée.
2. La fenêtre des propriétés de la mise à jour s'ouvre. Cette fenêtre affiche des informations regroupées sous les onglets suivants :

   - **Général**

     Cet onglet affiche les détails généraux de la mise à jour sélectionnée :

     - Mettre à jour l'état d'approbation (peut être modifié manuellement en sélectionnant un nouvel état dans la liste déroulante)
     - Catégorie Windows Server Update Services (WSUS) à laquelle appartient la mise à jour
     - Date et heure d'enregistrement de la mise à jour
     - Date et heure de création de la mise à jour
     - Niveau d'importance de la mise à jour
     - Exigences d'installation imposées par la mise à jour
     - Famille d'applications à laquelle appartient la mise à jour
     - Application à laquelle la mise à jour s'applique
     - Numéro de révision de la mise à jour

   - **Attributs**

Cet onglet affiche un ensemble d'attributs que vous pouvez utiliser pour en savoir plus à propos de la mise à jour sélectionnée. Cet ensemble diffère selon que la mise à jour est publiée par Microsoft ou par un fournisseur tiers.

L'onglet affiche les informations suivantes pour une mise à jour Microsoft :

- Niveau d'importance de la mise à jour, d'après Microsoft Security Response Center (MSRC)
- Lien vers l'article de Microsoft Knowledge Base décrivant la mise à jour
- Lien vers l'article de Microsoft Security Bulletin décrivant la mise à jour
- Identifiant de la mise à jour

L'onglet affiche les informations suivantes pour une mise à jour tierce :

- Que la mise à jour soit un correctif ou un paquet de distribution complet
- Langue de localisation de la mise à jour
- Si la mise à jour est installée automatiquement ou manuellement
- Si la mise à jour a été révoquée après avoir été appliquée
- Lien pour télécharger la mise à jour

- **Appareils**

  Cet onglet affiche une liste des appareils sur lesquels la mise à jour sélectionnée a été installée.

- **Vulnérabilités à corriger**

  Cet onglet affiche une liste de vulnérabilités que la mise à jour sélectionnée peut corriger.

- **Croisement 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. Cliquer sur un état ouvre une liste des appareils sur lesquels la mise à jour présente l'état sélectionné.

Vous pouvez consulter les informations sur les mises à jour du logiciel disponibles pour les logiciels tiers, y compris les logiciels Microsoft installés sur l'appareil administré sélectionné exécutant Windows.

Pour consulter la liste des mises à jour disponibles pour les logiciels tiers installés sur l'appareil administré sélectionné :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Appareils administrés**.

   La liste des appareils administrés s'affiche.

2. Dans la liste des appareils administrés, cliquez sur le lien portant le nom de l'appareil pour lequel vous souhaitez afficher les mises à jour du logiciel.

   La fenêtre des propriétés de l'appareil sélectionné s'affiche.

3. Dans la fenêtre des propriétés de l'appareil sélectionné, ouvrez l'onglet **Avancé**.

4. Dans le volet gauche, sélectionnez la section **Mises à jour 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, qui s'affiche actuellement vers les fichiers au format CSV ou TXT. Vous pouvez par exemple utiliser ces fichiers pour les envoyer à votre responsable de la sécurité de l'information ou les stocker à des fins statistiques.

Pour exporter vers un fichier texte la liste des mises à jour disponibles pour les logiciels tiers installés sur tous les appareils administrés, procédez comme suit :

1. Dans le menu principal, accédez à **Opérations** → **Gestion des correctifs** → **Mises à jour du logiciel**.

   La page affiche une liste des mises à jour disponibles pour les logiciels tiers installés sur tous les appareils administrés.

2. Cliquez sur le bouton **Exporter vers un fichier TXT** ou **Exporter vers un fichier CSV** en fonction du format que vous préférez exporter.

Le fichier contenant la liste des mises à jour disponibles pour les logiciels tiers, y compris les logiciels Microsoft, est téléchargé sur l'appareil que vous utilisez actuellement.

Pour exporter vers un fichier texte la liste des mises à jour disponibles pour les logiciels tiers installés sur les appareils administrés sélectionnés, procédez comme suit :

1. Ouvrez la liste des mises à jour du logiciel tiers disponibles sur l'appareil administré sélectionné.

2. Sélectionnez les mises à jour dans les applications que vous souhaitez exporter.

   Ignorez cette étape si vous souhaitez exporter une liste complète des mises à jour.

   Si vous souhaitez exporter la liste complète des mises à jour, seules les mises à jour affichées sur la page actuelle seront exportées.

Si vous souhaitez uniquement exporter les mises à jour installées, cochez la case **Afficher les mises à jour installées**.

3. Cliquez sur le bouton **Exporter vers un fichier TXT** ou **Exporter vers un fichier CSV** en fonction du format que vous préférez exporter.

Le fichier contenant la liste des mises à jour des logiciels tiers, y compris les logiciels Microsoft, installés sur l'appareil administré sélectionné est téléchargé sur l'appareil que vous utilisez en ce moment.

Approuver et refuser les mises à jour du logiciel tiers

Lorsque vous configurez la tâche *Installation des mises à jour requises et correction des vulnérabilités*, vous pouvez créer une règle qui exige un état particulier des mises à jour qui doivent être installées. Par exemple, une règle de mise à jour peut permettre l'installation des éléments suivants :

- Les mises à jour approuvées uniquement
- Les mises à jour approuvées et non définies uniquement
- Toutes les mises à jour peu importe l'état de la mise à jour

Vous pouvez approuver les mises à jour à installer et refuser les mises à jour qui ne doivent pas installer.

L'utilisation de l'état *Approuvé* pour gérer l'installation des mises à jour est efficace pour un petit nombre de mises à jour. Pour installer plusieurs mises à jour, utilisez les règles que vous pouvez configurer dans la tâche *Installation des mises à jour requises et correction des vulnérabilités*. Nous vous recommandons de définir l'état *Approuvé* uniquement pour les mises à jour particulières qui ne répondent pas aux critères spécifiés dans les règles. Lorsque vous approuvez manuellement une grande quantité de mises à jour, les performances du Serveur d'administration diminuent, ce qui peut entraîner une surcharge du Serveur d'administration.

Pour approuver ou refuser une ou plusieurs mises à jour :

1. Dans le menu principal, accédez à **Opérations → Gestion des correctifs → Mises à jour du logiciel**.

   Une liste des mises à jour disponibles s'affiche.

2. Sélectionnez les mises à jour que vous souhaitez approuver ou refuser.

3. Cliquez sur **Approuver** pour approuver les mises à jour sélectionnées ou sur **Refuser** pour les refuser.

   Par défaut, la valeur *Non défini* est cochée.

Les mises à jour sélectionnées ont les états que vous avez définis.

En option, vous pouvez modifier l'état d'approbation dans les propriétés d'une mise à jour en particulier.

Pour approuver ou refuser une mise à jour dans ses propriétés, procédez comme suit :

1. Dans le menu principal, accédez à **Opérations → Gestion des correctifs → Mises à jour du logiciel**.

   Une liste des mises à jour disponibles s'affiche.

2. Cliquez sur le nom de la mise à jour que vous souhaitez approuver ou refuser.

   La fenêtre de propriétés de la mise à jour s'affiche.

3. Dans la section **Général**, sélectionnez un état pour la mise à jour en modifiant l'option **État d'approbation de la mise à jour**. Vous pouvez sélectionner l'état *Approuvé*, *Rejeté* ou *Indéfini*.

4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications.

La mise à jour sélectionnée présente l'état que vous avez défini.

Si vous attribuez l'état **Rejetée** aux mises à jour du logiciel tiers, ces mises à jour ne sont pas installées sur les appareils où elles ont été planifiées mais pas encore installées. Les mises à jour seront conservées sur les appareils où elles ont déjà été installées. Si vous devez les supprimer, vous pouvez réaliser l'opération manuellement localement.

Mise à jour automatique des applications tierces

Certaines applications tierces peuvent être mises à jour automatiquement. Le fournisseur de l'application définit si l'application prend en charge ou non la fonctionnalité de mise à jour automatique. Si une application tierce installée sur un appareil administré prend en charge la mise à jour automatique, vous pouvez définir le paramètre de mise à jour automatique dans les propriétés de l'application. Une fois que vous avez modifié le paramètre de mise à jour automatique, les Agents d'administration appliquent le nouveau paramètre sur chaque appareil administré sur lequel l'application est installée.

Le paramètre de mise à jour automatique est indépendant des autres objets et paramètres de la fonctionnalité de la gestion des vulnérabilités et des correctifs. Par exemple, ce paramètre ne dépend pas d'un état d'approbation de mise à jour ou des tâches d'installation de mise à jour, comme *Installation des mises à jour requises et correction des vulnérabilités*, *Installation des mises à jour Windows Update* et *Corriger les vulnérabilités*.

Pour configurer le paramètre de mise à jour automatique pour une application tierce, procédez comme suit :

1. Dans le menu principal, accédez à **Opérations → Applications tierces → Registre des applications**.

2. Cliquez sur le nom de l'application pour laquelle vous souhaitez modifier le paramètre de mise à jour automatique.

   Pour simplifier la recherche, vous pouvez filtrer la liste par la colonne **État des mises à jour automatiques**.

   La fenêtre de propriétés de l'application s'affiche.

3. Dans la section **Général**, sélectionnez une valeur pour le paramètre suivant :

   État des mises à jour automatiques

Sélectionnez l'une des options ci-dessous :

- **Indéfini**

  La fonctionnalité de mise à jour automatique est désactivée. Kaspersky Security Center Cloud Console installe les mises à jour d'applications tierces à l'aide des tâches suivantes : *Installation des mises à jour requises et correction des vulnérabilités*, *Installation des mises à jour Windows Update* et *Corriger les vulnérabilités*.

- **Autorisé(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 Cloud Console installe les mises à jour d'applications tierces à l'aide des tâches suivantes : *Installation des mises à jour requises et correction des vulnérabilités*, *Installation des mises à jour Windows Update* et *Corriger les vulnérabilités*.

4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications.

Le paramètre de mise à jour automatique est appliqué à l'application sélectionnée.

Recherche et correction des vulnérabilités dans les applications

Kaspersky Security Center Cloud Console détecte et répare les vulnérabilités dans les applications sur les appareils administrés exécutant des familles de systèmes d'exploitation Microsoft Windows. Les vulnérabilités sont détectées dans le système d'exploitation et les logiciels tiers, y compris les logiciels Microsoft.

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

Recherche des vulnérabilités dans les applications

Pour rechercher les vulnérabilités dans les applications La Kaspersky Security Center Cloud Console utilise les caractéristiques de la base de données de vulnérabilités connues et de la base de données Windows Update. La base de données des vulnérabilités connues est créée et entretenue 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 Cloud Console utilise la tâche *Recherche de vulnérabilités et de mises à jour requises* pour rechercher les vulnérabilités dans les applications.

Correction des vulnérabilités dans les applications

Pour corriger les vulnérabilités dans les applications, Kaspersky Security Center Cloud Console utilise les mises à jour du logiciel publiées par les fournisseurs de logiciels. Vous pouvez consulter la liste des vulnérabilités dans les applications à n'importe quel moment. Les métadonnées des mises à jour du logiciel sont téléchargées dans le stockage du Serveur d'administration et dans les stockages des points de distribution à la suite de l'exécution de la tâche *Téléchargement des mises à jour sur les stockages des points de distribution*. Vous pouvez créer cette tâche à l'aide de l'assistant de démarrage rapide de l'application Kaspersky Security Center Cloud Console ou manuellement.

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 du logiciel qui corrigent des vulnérabilités dans les applications sont appelées *correctifs*. Dans Kaspersky Security Center Cloud Console, vous corrigez les vulnérabilités en utilisant les *correctifs recommandés*. Les correctifs recommandés sont des mises à jour du logiciel dont l'installation est recommandée par les experts de Kaspersky.

En fonction du mode de Kaspersky Security Center Cloud Console et de votre licence actuelle, vous pouvez utiliser la tâche *Installation des mises à jour requises et correction des vulnérabilités* ou la tâche *Corriger les vulnérabilités* pour corriger les vulnérabilités dans les applications.

La tâche *Installation des mises à jour requises et correction des vulnérabilités* corrige automatiquement de nombreuses vulnérabilités en installant les correctifs recommandés. Pour cette tâche, vous pouvez configurer manuellement certaines règles pour corriger plusieurs vulnérabilités.

Grâce à la tâche *Corriger les vulnérabilités*, vous pouvez corriger les vulnérabilités en installant les correctifs recommandés pour les logiciels Microsoft.

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.

Les tâches d'installation de mise à jour du logiciel intègrent un certain nombre de limitations. Ces limitations dépendent de la licence sous laquelle vous utilisez Kaspersky Security Center Cloud Console et du mode de fonctionnement de Kaspersky Security Center Cloud Console.

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 dans l'application ne pourra pas être corrigée.

Les informations sur chaque vulnérabilité corrigée sont stockées sur le Serveur d'administration pendant 90 jours. Passé ce délai, elles sont automatiquement supprimées.

Correction des vulnérabilités dans les applications

Une fois que vous avez obtenu la liste des vulnérabilités dans les applications, vous pouvez les corriger sur les appareils administrés qui fonctionnent sous Windows. Vous pouvez corriger les vulnérabilités dans les applications du système d'exploitation et des logiciels tiers, y compris les logiciels Microsoft, en créant et en exécutant la tâche *Corriger les vulnérabilités* ou la tâche *Installation des mises à jour requises et correction des vulnérabilités*.

Les tâches d'installation de mise à jour du logiciel intègrent un certain nombre de limitations. Ces limitations dépendent de la licence sous laquelle vous utilisez Kaspersky Security Center Cloud Console et du mode de fonctionnement de Kaspersky Security Center Cloud Console.

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.

  La disponibilité de cette fonctionnalité dépend du mode de Kaspersky Security Center Cloud Console et de votre licence actuelle.

  L'Assistant simplifie la création et la configuration d'une tâche de correction de la vulnérabilité et vous permet d'éliminer la création de tâches redondantes contenant les mêmes mises à jour à installer.

Correction des vulnérabilités dans les applications en utilisant la liste des vulnérabilités

Pour corriger les vulnérabilités dans les applications :

1. Ouvrez l'une des listes de vulnérabilités :

   - Pour ouvrir la liste générale des vulnérabilités, dans le menu principal, accédez à **Opérations → Gestion des correctifs → Vulnérabilités dans les applications**.

   - Pour ouvrir la liste des vulnérabilités d'un appareil administré, dans le menu principal, accédez à **Ressources (Appareils) → Appareils administrés → <nom de l'appareil> → Avancé → Vulnérabilités dans les applications**.

   - Pour ouvrir la liste des vulnérabilités d'une application en particulier, dans le menu principal, accédez à **Opérations → Applications tierces → Registre des applications → <nom de l'application> → Vulnérabilités**.

   Une page contenant une liste des vulnérabilités dans les applications tierces s'affiche.

2. Sélectionnez une ou plusieurs vulnérabilités dans la liste, puis cliquez sur le bouton **Corriger la vulnérabilité**.

Si une mise à jour du logiciel 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. En fonction du mode de Kaspersky Security Center Cloud Console et de votre licence actuelle, la tâche *Installation des mises à jour requises et correction des vulnérabilités* ou 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. En fonction du mode de Kaspersky Security Center Cloud Console et de votre licence actuelle, sélectionnez une tâche *Installation des mises à jour requises et correction des vulnérabilités* ou une tâche *Corriger les vulnérabilités*. Si vous 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 sélectionnez une tâche *Corriger les vulnérabilités*, les vulnérabilités sélectionnées seront ajoutées aux propriétés de la tâche.

     La fenêtre de propriétés de la tâche s'affiche. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications.

Si vous avez choisi de créer une tâche, la tâche est créée et affichée dans la liste des tâches à l'endroit suivant : **Ressources (Appareils)** → **Tâches**. Si vous avez choisi d'ajouter les vulnérabilités à une tâche existante, les vulnérabilités sont enregistrées dans les propriétés de la tâche.

Pour corriger les vulnérabilités dans les applications tierces, démarrez la tâche *Installation des mises à jour requises et correction des vulnérabilités* ou la tâche *Corriger les vulnérabilités*. Si vous avez créé la tâche *Corriger les vulnérabilités*, vous devez spécifier manuellement les mises à jour du logiciel pour corriger les vulnérabilités dans les applications énumérées dans les paramètres de la tâche.

Correction de la vulnérabilité dans les applications à l'aide de l'assistant de correction des vulnérabilités

La disponibilité de l'assistant de correction des vulnérabilités dépend de la licence que vous utilisez et du mode dans lequel Kaspersky Security Center Cloud Console fonctionne.

Pour corriger les vulnérabilités dans les applications à l'aide de l'assistant de correction des vulnérabilités, procédez comme suit :

1. Dans le menu principal, accédez à **Opérations** → **Gestion des correctifs** → **Vulnérabilités dans les applications**.

   Une page contenant une liste des vulnérabilités dans les applications tierces installés sur les appareils administrés s'affiche.

2. Cochez la case en regard de la vulnérabilité que vous souhaitez corriger.

3. Cliquez sur le bouton **Lancer l'Assistant de correction des vulnérabilités**.

L'Assistant de correction des vulnérabilités s'ouvre. La page **Sélectionnez la tâche de correction de la vulnérabilité** affiche la liste de toutes les tâches existantes des types suivants :

- *Installation des mises à jour requises et correction des vulnérabilités*
- *Installation des mises à jour Windows Update*
- *Corriger les vulnérabilités*

Vous ne pouvez pas modifier les deux derniers types de tâches pour installer de nouvelles mises à jour. Pour installer de nouvelles mises à jour, vous ne pouvez utiliser que la tâche *Installation des mises à jour requises et correction des vulnérabilités*.

4. Si vous souhaitez que l'assistant affiche uniquement les tâches qui corrigent la vulnérabilité que vous avez sélectionnée, activez l'option **Afficher uniquement les tâches corrigeant la vulnérabilité sélectionnée**.

5. Choisissez la manière dont vous voulez procéder :

   - Pour démarrer une tâche, cochez la case en regard du nom de la tâche, puis cliquez sur le bouton **Démarrer**.
   - Pour ajouter une nouvelle règle à une tâche existante :

     a. Cochez la case en regard du nom de la tâche, puis cliquez sur le bouton **Ajouter une règle**.

     b. Sur la page qui s'ouvre, configurez la nouvelle règle :

     - Règle de correction des vulnérabilités d'un niveau de gravité défini

       Parfois, les mises à jour du logiciel peuvent nuire à l'expérience de l'utilisateur. Dans ce cas, il se peut que vous décidiez d'installer uniquement les mises à jour critiques au fonctionnement du logiciel et d'ignorer les autres.

       Quand cette option est activée, les mises à jour corrigent uniquement les vulnérabilités dont le niveau de gravité, tel que défini par Kaspersky, est égal ou supérieur au niveau de la mise à jour sélectionnée (**Moyenne**, **Élevé** ou **Critique**). Les vulnérabilités dont le niveau de gravité est inférieur à la valeur sélectionnée ne sont pas corrigées.

       Si cette option est désactivée, les mises à jour corrigent toutes les vulnérabilités, quel que soit le niveau de gravité.

       Cette option est Inactif par défaut.

     - **Règle de correction des vulnérabilités au moyen de mises à jour du même type que la mise à jour définie comme recommandée pour la vulnérabilité sélectionnée** (disponible uniquement pour les vulnérabilités dans les applications Microsoft)
     - **Règle de correction des vulnérabilités dans les applications du fournisseur sélectionné** (disponible uniquement pour les vulnérabilités dans les applications tierces)
     - **Règle de correction d'une vulnérabilité dans toutes les versions de l'application sélectionnée** (disponible uniquement pour les vulnérabilités dans les applications tierces)
     - **Règle de correction de la vulnérabilité sélectionnée**
     - Approuver les mises à jour qui corrigent la vulnérabilité sélectionnée

La mise à jour sélectionnée est approuvée pour l'installation. Activez cette option si certaines règles appliquées de l'installation de la mise à jour autorisent l'installation des mises à jour confirmées uniquement.

Cette option est Inactif par défaut.

c. Cliquez sur le bouton **Ajouter**.

- Pour créer une tâche, procédez comme suit :

a. Cliquez sur le bouton **Nouvelle tâche**.

b. Sur la page qui s'ouvre, configurez la nouvelle règle :

- Règle de correction des vulnérabilités d'un niveau de gravité défini

Parfois, les mises à jour du logiciel peuvent nuire à l'expérience de l'utilisateur. Dans ce cas, il se peut que vous décidiez d'installer uniquement les mises à jour critiques au fonctionnement du logiciel et d'ignorer les autres.

Quand cette option est activée, les mises à jour corrigent uniquement les vulnérabilités dont le niveau de gravité, tel que défini par Kaspersky, est égal ou supérieur au niveau de la mise à jour sélectionnée (**Moyenne**, **Élevé** ou **Critique**). Les vulnérabilités dont le niveau de gravité est inférieur à la valeur sélectionnée ne sont pas corrigées.

Si cette option est désactivée, les mises à jour corrigent toutes les vulnérabilités, quel que soit le niveau de gravité.

Cette option est Inactif par défaut.

- **Règle de correction des vulnérabilités via des mises à jour de type** (disponible uniquement pour les vulnérabilités dans les applications Microsoft)
- **Règle de correction des vulnérabilités dans les applications du fournisseur sélectionné** (disponible uniquement pour les vulnérabilités dans les applications tierces)
- **Règle de correction d'une vulnérabilité dans toutes les versions de l'application sélectionnée** (disponible uniquement pour les vulnérabilités dans les applications tierces)
- **Règle de correction de la vulnérabilité sélectionnée**
- Approuver les mises à jour qui corrigent la vulnérabilité sélectionnée

La mise à jour sélectionnée est approuvée pour l'installation. Activez cette option si certaines règles appliquées de l'installation de la mise à jour autorisent l'installation des mises à jour confirmées uniquement.

Cette option est Inactif par défaut.

c. Cliquez sur le bouton **Ajouter**.

Si vous avez choisi de démarrer une tâche, vous pouvez fermer l'assistant. La tâche se poursuivra en mode arrière-plan. Il n'y a rien d'autre à faire.

Si vous avez choisi d'ajouter une règle à une tâche existante, la fenêtre des propriétés de la tâche s'ouvre. La nouvelle règle est déjà ajoutée aux propriétés de la tâche. Vous pouvez afficher ou modifier la règle ou d'autres paramètres de tâche. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications.

Si vous avez choisi de créer une tâche, vous continuez à créer la tâche dans l'assistant de création d'une tâche. La nouvelle règle que vous avez ajoutée dans l'assistant de correction des vulnérabilités s'affiche dans l'assistant de création d'une tâche. Lorsque vous terminez l'assistant de création d'une tâche, 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 Microsoft sur les appareils administrés qui fonctionnent sous Windows.

La disponibilité de cette fonctionnalité dépend du mode de Kaspersky Security Center Cloud Console et de votre licence actuelle. 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.

Les tâches d'installation de mise à jour du logiciel intègrent un certain nombre de limitations. Ces limitations dépendent de la licence sous laquelle vous utilisez Kaspersky Security Center Cloud Console et du mode de fonctionnement de Kaspersky Security Center Cloud Console.

Une interaction utilisateur peut être requise lorsque vous mettez à jour une application tierce ou corrigez une vulnérabilité dans une application tierce sur un appareil administré. Par exemple, l'utilisateur peut être invité à fermer l'application tierce si elle est actuellement ouverte.

Pour créer la tâche Corriger les vulnérabilités, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Tâches**.
2. Cliquez sur **Ajouter**.

   Ceci permet de lancer l'assistant de création d'une tâche. Parcourez les étapes de l'assistant à l'aide du bouton **Suivant**.
3. Pour l'application Kaspersky Security Center Cloud Console, sélectionnez le type de tâche **Corriger les vulnérabilités**.
4. Spécifiez le nom de la tâche créée.

   Le nom de la tâche ne peut pas contenir plus de 100 symboles et contenir de symboles spéciaux ("*<>?\:|).
5. Sélectionnez les appareils auxquels les tâches seront affectées.
6. Cliquez sur le bouton **Ajouter**.

   La liste des vulnérabilités s'ouvre.
7. Sélectionnez les vulnérabilités que vous souhaitez corriger, puis cliquez sur **OK**.
8. Définissez les paramètres de redémarrage du système d'exploitation :

- **Ne pas redémarrer l'appareil**

  Les appareils clients ne redémarrent pas automatiquement après l'opération. Pour arrêter le fonctionnement, il faut redémarrer l'appareil (par exemple, manuellement ou à l'aide d'une tâche d'administration des appareils). Les informations sur la nécessité du redémarrage sont enregistrées dans les résultats de la tâche et dans l'état de l'appareil. Cette option convient aux tâches d' sur les serveurs et autres appareils pour lesquels la continuité des opérations est critique.

- **Redémarrer l'appareil**

  Dans ce cas, le redémarrage des appareils clients est toujours exécuté automatiquement, si celui-ci est requis pour terminer l'opération. Cette option convient aux tâches d' sur des appareils pour lesquels des interruptions périodiques sont admises (débranchement, redémarrage).

- **Confirmer l'action auprès de l'utilisateur**

  Le message qui signale que l'appareil client doit être redémarré manuellement s'affiche sur l'écran de l'appareil. Pour cette option, il est possible de configurer des paramètres avancés : le texte du message pour l'utilisateur, la fréquence du message, ainsi que le délai à l'issue duquel le redémarrage sera forcé (sans confirmation de l'utilisateur). Cette option convient le mieux pour les postes de travail sur lesquels les utilisateurs doivent pouvoir sélectionner l'heure de redémarrage qui leur convient le mieux.

  Cette option est sélectionnée par défaut.

- **Répéter la demande toutes les (min.)**

  Quand cette option est activée, l'application invite l'utilisateur à redémarrer le système d'exploitation selon la fréquence indiquée.

  Cette option est activée par défaut. L'intervalle par défaut est de 5 minutes. La valeur peut être comprise entre 1 et 1 440 minutes.

  Si cette option est désactivée, l'invite est affichée une seule fois.

- **Redémarrer le système au bout de (min.)**

  Après avoir averti l'utilisateur, l'application force le redémarrage du système d'exploitation à l'issue de l'intervalle défini.

  Cette option est activée par défaut. Le délai par défaut est de 30 minutes. La valeur peut être comprise entre 1 et 1 440 minutes.

- **Forcer la fermeture des applications dans les sessions bloquées**

Les applications en cours d'exécution peuvent empêcher le redémarrage de l'appareil client. Par exemple, si un document est en train d'être modifié dans un logiciel de traitement de texte et qu'il n'est pas enregistré, l'application n'autorise pas le redémarrage de l'appareil.

Quand cette option est activée, l'arrêt forcé de ces applications sur un appareil verrouillé doit avoir lieu avant de pouvoir redémarrer l'appareil. Les utilisateurs pourraient perdre toute modification qui n'a pas été enregistrée à ce moment.

Si cette option est désactivée, un appareil verrouillé n'est pas redémarré. L'état de la tâche sur cet appareil indique qu'il faut redémarrer l'appareil. Les utilisateurs doivent quitter manuellement toutes les applications en cours d'exécution sur les appareils verrouillés, puis redémarrer ces appareils.

Cette option est Inactif par défaut.

9. Définissez les paramètres du compte :

   - **Compte par défaut**

     La tâche sera lancée sous le même compte utilisateur sous lequel l'application, exécutant cette tâche, a été installée et lancée.

     Cette option est sélectionnée par défaut.

   - **Indiquer un compte**

     Remplissez les champs **Compte utilisateur** et **Mot de passe** pour définir les détails d'un compte à partir duquel la tâche est exécutée. Le compte doit disposer de droits suffisants pour cette tâche.

   - **Compte**

     Le compte utilisateur au nom duquel la tâche sera lancée.

   - **Mot de passe**

     Mot de passe du compte utilisateur au nom duquel la tâche sera lancée.

10. Si sur la page **Fin de la création de la tâche** vous activez l'option **Ouvrir les détails de la tâche à la fin de la création**, vous pouvez modifier les paramètres de la tâche par défaut. Si vous n'activez pas cette tâche, la tâche est créée selon les paramètres par défaut. Vous pourrez modifier ces paramètres par défaut plus tard, à tout moment.

11. Cliquez sur le bouton **Terminer**.

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

12. Cliquez sur le nom de la tâche créée pour ouvrir la fenêtre de propriétés de la tâche.

13. Dans la fenêtre des propriétés de la tâche, indiquez les paramètres généraux de la tâche en fonction de vos besoins.

14. Cliquez sur le bouton **Enregistrer**.

La tâche est créée et configurée.

Création de la tâche Installer les mises à jour requises et corriger les vulnérabilités

La disponibilité de la tâche *Installation des mises à jour requises et correction des vulnérabilités* dépend du mode de Kaspersky Security Center Cloud Console et de votre licence actuelle.

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.

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.

Les tâches d'installation de mise à jour du logiciel intègrent un certain nombre de limitations. Ces limitations dépendent de la licence sous laquelle vous utilisez Kaspersky Security Center Cloud Console et du mode de fonctionnement de Kaspersky Security Center Cloud Console.

Pour créer une tâche Installation des mises à jour requises et correction des vulnérabilités :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Tâches**.
2. Cliquez sur **Ajouter**.

   Ceci permet de lancer l'assistant de création d'une tâche. Suivez les étapes de l'assistant.
3. Pour l'application Kaspersky Security Center Cloud Console, sélectionnez le type de tâche **Installation des mises à jour requises et correction des vulnérabilités**.
4. Spécifiez le nom de la tâche créée. Le nom de la tâche ne peut pas contenir plus de 100 symboles et contenir de symboles spéciaux ("*<>?\:|).
5. Sélectionnez les appareils auxquels les tâches seront affectées.
6. Indiquez les règles d'installation des mises à jour, puis définissez les paramètres suivants :

   - **Commencer l'installation au moment du redémarrage ou de l'arrêt de l'appareil**

     Si cette option est activée, les mises à jour sont installées lors du redémarrage ou de l'arrêt de l'appareil. Dans le cas contraire, les mises à jour sont installées selon la programmation.

     Utilisez cette option si l'installation des mises à jour peut avoir un impact sur les performances de l'appareil.

     Cette option est Inactif par défaut.

- **Installer les modules système général requis**

  Si cette option est activée, l'application, avant d'installer une mise à jour, installe automatiquement tous les composants généraux système (prérequis) requis pour l'installation de la mise à jour. Par exemple, il peut s'agir des mises à jour du système d'exploitation.

  Si cette option est désactivée, vous devrez peut-être installer les prérequis manuellement.

  Cette option est Inactif par défaut.

- **Autoriser l'installation de nouvelles versions de l'application lors des mises à jour**

  Si cette option est activée, les mises à jour sont autorisées lorsqu'elles entraînent l'installation d'une nouvelle version d'un logiciel.

  Si cette option est désactivée, le logiciel n'est pas mis à jour. Vous pouvez alors installer les nouvelles versions du logiciel manuellement ou via un autre tâche. Par exemple, vous pouvez utiliser cette option si l'infrastructure de votre entreprise n'est pas prise en charge par une nouvelle version du logiciel ou si vous souhaitez vérifier une mise à jour dans une infrastructure d'essai.

  Cette option est activée par défaut.

  La mise à jour d'une application peut provoquer un dysfonctionnement des applications dépendantes installées sur les appareils clients.

- **Télécharger les mises à jour sur l'appareil sans les installer**

  Quand cette option est activée, l'application télécharge les mises à jour sur l'appareil, mais ne les installe pas automatiquement. Vous pouvez installer les mises à jour manuellement par la suite.

  Les mises à jour Microsoft sont téléchargées dans le stockage Windows système. Les mises à jour des produits tiers (applications développées par des éditeurs d'application autres que Kaspersky et Microsoft) sont téléchargées dans le dossier indiqué dans le champ **Télécharger les mises à jour sur**.

  Si cette option est désactivée, les mises à jour sont installées automatiquement sur l'appareil.

  Cette option est Inactif par défaut.

- **Télécharger les mises à jour sur**

  Ce dossier est utilisé dans le cadre du téléchargement des mises à jour de produits tiers (applications développées par des éditeurs de logiciels autres que Kaspersky et Microsoft).

- **Activer le diagnostic avancé**

Quand cette fonction est activée, l'Agent d'administration enregistre les traces même si le traçage est désactivé pour l'agent d'administration dans l'utilitaire de diagnostic à distance Kaspersky Security Center Cloud Console. 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 Cloud Console. Aucune trace complémentaire n'est écrite.

Lors de la création d'une tâche, il n'est pas nécessaire d'activer le diagnostic avancé. Par contre, vous pouvez activer cette fonction plus tard si, par exemple, une tâche échoue sur certains appareils et que vous souhaitez obtenir des informations complémentaires lors d'une autre exécution de la tâche.

Cette option est Inactif par défaut.

- Taille maximale (Mo) des fichiers de diagnostic avancé

  La valeur par défaut est de 100 Mo, mais elle peut se situer entre 1 et 2 048 Mo. Il peut arriver qu'un expert du Support Technique de Kaspersky vous demande de modifier la valeur par défaut lorsque les informations reprises dans les fichiers de diagnostic avancés que vous avez envoyés ne suffisent pas pour résoudre le problème.

7. Définissez les paramètres de redémarrage du système d'exploitation :

- Ne pas redémarrer l'appareil

  Les appareils clients ne redémarrent pas automatiquement après l'opération. Pour arrêter le fonctionnement, il faut redémarrer l'appareil (par exemple, manuellement ou à l'aide d'une tâche d'administration des appareils). Les informations sur la nécessité du redémarrage sont enregistrées dans les résultats de la tâche et dans l'état de l'appareil. Cette option convient aux tâches d' sur les serveurs et autres appareils pour lesquels la continuité des opérations est critique.

- Redémarrer l'appareil

  Dans ce cas, le redémarrage des appareils clients est toujours exécuté automatiquement, si celui-ci est requis pour terminer l'opération. Cette option convient aux tâches d' sur des appareils pour lesquels des interruptions périodiques sont admises (débranchement, redémarrage).

- Confirmer l'action auprès de l'utilisateur

  Le message qui signale que l'appareil client doit être redémarré manuellement s'affiche sur l'écran de l'appareil. Pour cette option, il est possible de configurer des paramètres avancés : le texte du message pour l'utilisateur, la fréquence du message, ainsi que le délai à l'issue duquel le redémarrage sera forcé (sans confirmation de l'utilisateur). Cette option convient le mieux pour les postes de travail sur lesquels les utilisateurs doivent pouvoir sélectionner l'heure de redémarrage qui leur convient le mieux.

  Cette option est sélectionnée par défaut.

- Répéter la demande toutes les (min.)

Quand cette option est activée, l'application invite l'utilisateur à redémarrer le système d'exploitation selon la fréquence indiquée.

Cette option est activée par défaut. L'intervalle par défaut est de 5 minutes. La valeur peut être comprise entre 1 et 1 440 minutes.

Si cette option est désactivée, l'invite est affichée une seule fois.

- **Redémarrer le système au bout de (min.)**

  Après avoir averti l'utilisateur, l'application force le redémarrage du système d'exploitation à l'issue de l'intervalle défini.

  Cette option est activée par défaut. Le délai par défaut est de 30 minutes. La valeur peut être comprise entre 1 et 1 440 minutes.

- **Délai d'attente avant la fermeture forcée des ap&plications dans les sessions bloquées (min)**

  Arrêt forcé des applications lorsque l'appareil de l'utilisateur est verrouillé (arrêt manuel ou automatique après une période d'inactivité).

  Si cette option est activée, les applications en cours sur l'appareil verrouillé seront fermées de force à la fin du délai indiqué dans le champ situé à côté de la case.

  Si cette option est activée, les applications en cours sur l'appareil verrouillé ne seront pas fermées.

  Cette option est Inactif par défaut.

8. Si sur la page **Fin de la création de la tâche** vous activez l'option **Ouvrir les détails de la tâche à la fin de la création**, vous pouvez modifier les paramètres de la tâche par défaut. Si vous n'activez pas cette tâche, la tâche est créée selon les paramètres par défaut. Vous pourrez modifier ces paramètres par défaut plus tard, à tout moment.

9. Cliquez sur le bouton **Terminer**.

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

10. Cliquez sur le nom de la tâche créée pour ouvrir la fenêtre de propriétés de la tâche.

11. Dans la fenêtre des propriétés de la tâche, indiquez les paramètres généraux de la tâche en fonction de vos besoins.

12. Cliquez sur le bouton **Enregistrer**.

    La tâche est créée et configurée.

Si les résultats de la tâche contiennent un avertissement concernant l'erreur 0x80240033 " Erreur de l'agent de mise à jour Windows 80240033 (" Les conditions de licence n'ont pas pu être téléchargées ") ", vous pouvez résoudre ce problème via le registre Windows.

Ajout de règles pour l'installation de la mise à jour

La disponibilité de cette fonctionnalité dépend du mode de Kaspersky Security Center Cloud Console et de votre licence actuelle.

Lors de l'installation de mises à jour du logiciel ou de la correction de la vulnérabilité dans les applications à l'aide de la tâche *Installation des mises à jour requises et correction des vulnérabilités*, vous devez définir les règles pour l'installation de la mise à jour. Ces règles déterminent les mises à jour à installer et les vulnérabilités à corriger.

Les paramètres exacts dépendent de l'objet pour lequel vous ajoutez une règle : pour toutes les mises à jour, pour les mises à jour Windows Update ou pour les mises à jour d'applications tierces (applications développées par des éditeurs autres que Kaspersky et Microsoft). Lors de l'ajout d'une règle pour des mises à jour Windows Update ou des mises à jour d'applications tierces, vous pouvez sélectionner des applications spécifiques et les versions de l'application pour lesquelles vous souhaitez installer les mises à jour. Lors de l'ajout d'une règle pour toutes les mises à jour, vous pouvez sélectionner les mises à jour spécifiques que vous souhaitez installer et les vulnérabilités que vous souhaitez éliminer via l'installation des mises à jour.

Vous pouvez ajouter une règle pour l'installation de la mise à jour comme suit :

- En ajoutant une règle lors de la création d'une nouvelle tâche Installation des mises à jour requises et correction des vulnérabilités.
- En ajoutant une règle sous l'onglet **Paramètres de l'application** dans la fenêtre des propriétés d'une tâche *Installation des mises à jour requises et correction des vulnérabilités* existante.
- Via l'assistant d'installation des mises à jour ou l'assistant de correction des vulnérabilités.

Pour ajouter une nouvelle règle pour toutes les mises à jour, procédez comme suit :

1. Cliquez sur le bouton **Ajouter**.

   L'Assistant de création de règles se lance. Parcourez les étapes de l'assistant à l'aide du bouton **Suivant**.

2. Sur la page **Type de règle**, sélectionnez **Règle pour toutes les mises à jour**.

3. Sur la page **Critères généraux**, utilisez les listes déroulantes pour définir les paramètres suivants :

   - **Définir les mises à jour à installer**

     Sélectionnez les mises à jour qui doivent être installées sur les appareils clients :

     - **Installer uniquement les mises à jour confirmées**. Cette option installe uniquement les mises à jour confirmées.
     - **Installer toutes les mises à jour (sauf les mises à jour rejetées)**. Cette option installe les mises à jour avec l'état *Approuvé* ou *Non défini*.
     - **Installer toutes les mises à jour (y compris les mises à jour rejetées)**. Ceci installe toutes les mises à jour, quel que soit leur état d'approbation. Sélectionnez cette option avec prudence. Par exemple, utilisez cette option si vous souhaitez vérifier l'installation de certaines mises à jour rejetées dans une infrastructure d'essai.

   - **Corriger les vulnérabilités de niveau de gravité égal ou supérieur à**

Parfois, les mises à jour du logiciel peuvent nuire à l'expérience de l'utilisateur. Dans ce cas, il se peut que vous décidiez d'installer uniquement les mises à jour critiques au fonctionnement du logiciel et d'ignorer les autres.

Quand cette option est activée, les mises à jour corrigent uniquement les vulnérabilités dont le niveau de gravité tel que défini par Kaspersky est égal ou supérieur à la valeur sélectionnée dans la liste (**Moyenne**, **Élevé** ou **Critique**). Les vulnérabilités dont le niveau de gravité est inférieur à la valeur sélectionnée ne sont pas corrigées.

Si cette option est désactivée, les mises à jour corrigent toutes les vulnérabilités, quel que soit le niveau de gravité.

Cette option est Inactif par défaut.

4. Sur la page **Mises à jour**, sélectionnez les mises à jour à installer :

- **Installer toutes les mises à jour convenables**

  Installez toutes les mises à jour du logiciel qui répondent aux critères définis à la page **Critères généraux** de l'assistant. Sélectionné par défaut.

- **Installer uniquement les mises à jour depuis la liste**

  Installer uniquement les mises à jour du logiciel que vous sélectionnez manuellement dans la liste. Cette liste contient toutes les mises à jour du logiciel disponibles.

  Par exemple, vous pouvez sélectionner des mises à jour spécifiques dans les cas suivants : pour vérifier leur installation dans un environnement d'essai, pour mettre à jour uniquement les applications critiques ou pour mettre à jour uniquement certaines applications.

- **&Installer automatiquement toutes les mises à jour précédentes des applications nécessaires à l'installation des mises à jour sélectionnées**

  Conservez cette option si vous acceptez l'installation de versions de l'application intermédiaires quand l'impose l'installation des mises à jour sélectionnées.

  Si vous désactivez cette option, seules les versions sélectionnées des applications sont installées. Désactivez cette option si vous souhaitez mettre à jour les applications d'une manière directe, sans tenter d'installer les versions successives. S'il est impossible d'installer les mises à jour sélectionnées sans installer les versions antérieures de l'application, la mise à jour de l'application échoue.

  Admettons que la version 3 d'une application est installée sur un appareil et vous souhaitez réaliser la mise à jour jusque la version 5, mais la version 5 de cette application peut être installée uniquement sur la version 4. Quand cette option est installée, le logiciel installe d'abord la version 4, puis la version 5. Si l'option est désactivée, le logiciel ne parvient pas à mettre l'application à jour.

  Cette option est activée par défaut.

5. Sur la page **Vulnérabilités**, sélectionnez les vulnérabilités que seront corrigées suite à l'installation des mises à jour sélectionnées :

- **Corriger toutes les vulnérabilités qui correspondent aux autres critères**

  Corrigez toutes les vulnérabilités qui satisfont les critères définis à la page **Critères généraux** de l'assistant. Sélectionné par défaut.

- **Corriger uniquement les vulnérabilités depuis la liste**

Corrigez uniquement les vulnérabilités que vous sélectionnez manuellement dans la liste. Cette liste contient toutes les vulnérabilités détectées.

Par exemple, vous pouvez sélectionner des vulnérabilités spécifiques dans les cas suivants : pour vérifier les corrections dans un environnement d'essai, pour corriger les vulnérabilités uniquement dans les applications critiques ou pour corriger les vulnérabilités uniquement dans certaines applications.

6. La page **Nom** permet de renseigner le nom de la règle ajoutée. Vous pouvez changer ce nom plus tard dans la section **Paramètres** de la fenêtre des propriétés de la tâche créée.

Une fois que l'assistant de création de règles a terminé, la nouvelle règle est ajoutée et s'affiche dans la liste des règles de l'assistant de création d'une tâche ou dans les propriétés de la tâche.

Pour ajouter une nouvelle règle pour les mises à jour de Windows Update, procédez comme suit :

1. Cliquez sur le bouton **Ajouter**.

   L'Assistant de création de règles se lance. Parcourez les étapes de l'assistant à l'aide du bouton **Suivant**.

2. Sur la page **Type de règle**, sélectionnez **Règle pour les mises à jour Windows Update**.

3. Dans la fenêtre **Conditions générales**, configurez les paramètres suivants :

- **Définir les mises à jour à installer**

  Sélectionnez les mises à jour qui doivent être installées sur les appareils clients :

  - **Installer uniquement les mises à jour confirmées**. Cette option installe uniquement les mises à jour confirmées.
  - **Installer toutes les mises à jour (sauf les mises à jour rejetées)**. Cette option installe les mises à jour avec l'état *Approuvé* ou *Non défini*.
  - **Installer toutes les mises à jour (y compris les mises à jour rejetées)**. Ceci installe toutes les mises à jour, quel que soit leur état d'approbation. Sélectionnez cette option avec prudence. Par exemple, utilisez cette option si vous souhaitez vérifier l'installation de certaines mises à jour rejetées dans une infrastructure d'essai.

- **Corriger les vulnérabilités de niveau de gravité égal ou supérieur à**

  Parfois, les mises à jour du logiciel peuvent nuire à l'expérience de l'utilisateur. Dans ce cas, il se peut que vous décidiez d'installer uniquement les mises à jour critiques au fonctionnement du logiciel et d'ignorer les autres.

  Quand cette option est activée, les mises à jour corrigent uniquement les vulnérabilités dont le niveau de gravité tel que défini par Kaspersky est égal ou supérieur à la valeur sélectionnée dans la liste (**Moyenne**, **Élevé** ou **Critique**). Les vulnérabilités dont le niveau de gravité est inférieur à la valeur sélectionnée ne sont pas corrigées.

  Si cette option est désactivée, les mises à jour corrigent toutes les vulnérabilités, quel que soit le niveau de gravité.

  Cette option est Inactif par défaut.

- **Corriger les vulnérabilités qui présentent un niveau de gravité selon MSRC égal ou supérieur à**

Parfois, les mises à jour du logiciel peuvent nuire à l'expérience de l'utilisateur. Dans ce cas, il se peut que vous décidiez d'installer uniquement les mises à jour critiques au fonctionnement du logiciel et d'ignorer les autres.

Quand cette option est activée, les mises à jour corrigent uniquement les vulnérabilités dont le niveau de gravité tel que défini par Microsoft Security Response Center (MSRC) est égal ou supérieur à la valeur sélectionnée dans la liste (**Bas**, **Moyenne**, **Élevé** ou **Critique**). Les vulnérabilités dont le niveau de gravité est inférieur à la valeur sélectionnée ne sont pas corrigées.

Si cette option est désactivée, les mises à jour corrigent toutes les vulnérabilités, quel que soit le niveau de gravité.

Cette option est Inactif par défaut.

4. Sur la page **Applications**, sélectionnez les applications et les versions des applications pour lesquelles vous voulez installer les mises à jour. Toutes les applications sont cochées par défaut.

5. Sur la page **Catégorie des mises à jour**, sélectionnez les catégories des mises à jour à installer. Ces catégories sont les mêmes que dans le catalogue Microsoft Update. Toutes les catégories sont cochées par défaut.

6. La page **Nom** permet de renseigner le nom de la règle ajoutée. Vous pouvez changer ce nom plus tard dans la section **Paramètres** de la fenêtre des propriétés de la tâche créée.

Une fois que l'assistant de création de règles a terminé, la nouvelle règle est ajoutée et s'affiche dans la liste des règles de l'assistant de création d'une tâche ou dans les propriétés de la tâche.

Pour ajouter une règle pour les mises à jour des produits tiers, procédez comme suit :

1. Cliquez sur le bouton **Ajouter**.

   L'Assistant de création de règles se lance. Parcourez les étapes de l'assistant à l'aide du bouton **Suivant**.

2. Sur la page **Type de règle**, sélectionnez **Règles pour les mises à jour tierces**.

3. Dans la fenêtre **Conditions générales**, configurez les paramètres suivants :

   - **Définir les mises à jour à installer**

     Sélectionnez les mises à jour qui doivent être installées sur les appareils clients :

     - **Installer uniquement les mises à jour confirmées**. Cette option installe uniquement les mises à jour confirmées.
     - **Installer toutes les mises à jour (sauf les mises à jour rejetées)**. Cette option installe les mises à jour avec l'état *Approuvé* ou *Non défini*.
     - **Installer toutes les mises à jour (y compris les mises à jour rejetées)**. Ceci installe toutes les mises à jour, quel que soit leur état d'approbation. Sélectionnez cette option avec prudence. Par exemple, utilisez cette option si vous souhaitez vérifier l'installation de certaines mises à jour rejetées dans une infrastructure d'essai.

   - **Corriger les vulnérabilités de niveau de gravité égal ou supérieur à**

Parfois, les mises à jour du logiciel peuvent nuire à l'expérience de l'utilisateur. Dans ce cas, il se peut que vous décidiez d'installer uniquement les mises à jour critiques au fonctionnement du logiciel et d'ignorer les autres.

Quand cette option est activée, les mises à jour corrigent uniquement les vulnérabilités dont le niveau de gravité tel que défini par Kaspersky est égal ou supérieur à la valeur sélectionnée dans la liste (**Moyenne**, **Élevé** ou **Critique**). Les vulnérabilités dont le niveau de gravité est inférieur à la valeur sélectionnée ne sont pas corrigées.

Si cette option est désactivée, les mises à jour corrigent toutes les vulnérabilités, quel que soit le niveau de gravité.

Cette option est Inactif par défaut.

4. Sur la page **Applications**, sélectionnez les applications et les versions des applications pour lesquelles vous voulez installer les mises à jour. Toutes les applications sont cochées par défaut.

5. La page **Nom** permet de renseigner le nom de la règle ajoutée. Vous pouvez changer ce nom plus tard dans la section Paramètres de la fenêtre des propriétés de la tâche créée.

Une fois que l'assistant de création de règles a terminé, la nouvelle règle est ajoutée et s'affiche dans la liste des règles de l'assistant de création d'une tâche ou dans les propriétés de la tâche.

Consultation des informations relatives aux vulnérabilités dans les applications sur tous les appareils administrés

Une fois que vous avez analysé les applications des appareils administrés à la recherche de vulnérabilités, vous pouvez consulter la liste des vulnérabilités dans les applications détectées sur tous les appareils administrés. Si vous exécutez la tâche pour la hiérarchie des Serveurs d'administration, vous pouvez consulter la liste des appareils administrés pour lesquels des vulnérabilités ont été détectées uniquement pour le Serveur d'administration sélectionné.

Pour consulter la liste des vulnérabilités dans les applications détectées sur tous les appareils administrés,

Dans le menu principal, accédez à **Opérations** → **Gestion des correctifs** → **Vulnérabilités dans les applications**.

La page affiche la liste des vulnérabilités logicielles détectées sur les appareils client.

Vous pouvez également générer et consulter le rapport sur les vulnérabilités.

Vous pouvez indiquer un filtre pour consulter la liste des vulnérabilités dans les applications. Cliquez sur l'icône **Filtre** ( ) dans le coin supérieur droit de la liste des vulnérabilités dans les applications pour gérer le filtre. Vous pouvez également sélectionner l'un des filtres prédéfinis dans la liste déroulante **Filtres prédéfinis** située au-dessus de la liste des vulnérabilités dans les applications.

Vous pouvez obtenir des informations détaillées sur n'importe quelle vulnérabilité de la liste.

Pour obtenir des informations sur une vulnérabilité dans une application :

Cliquez sur le lien avec le nom de la vulnérabilité dans la liste des vulnérabilités dans les applications.

La fenêtre des propriétés de la vulnérabilité dans l'application s'ouvre.

Consultation des informations relatives aux vulnérabilités dans les applications sur l'appareil administré sélectionné

Vous pouvez consulter les informations relatives aux vulnérabilités dans les applications sur l'appareil administré sélectionné sous Windows.

Pour afficher la liste des vulnérabilités logicielles détectées sur l'appareil administré sélectionné :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Appareils administrés**.

   La liste des appareils administrés s'affiche.

2. Dans la liste des appareils administrés, cliquez sur le lien portant le nom de l'appareil pour lequel vous souhaitez afficher les vulnérabilités dans les applications détectées.

   La fenêtre des propriétés de l'appareil sélectionné s'affiche.

3. Dans la fenêtre des propriétés de l'appareil sélectionné, ouvrez l'onglet **Avancé**.

4. Dans le volet gauche, sélectionnez la section **Vulnérabilités dans les applications**.

La liste des vulnérabilités dans les applications détectées sur l'appareil administré sélectionné s'affiche.

Pour consulter les propriétés de la vulnérabilité dans l'application sélectionnée,

cliquez sur le lien avec le nom de la vulnérabilité dans l'application dans la liste des vulnérabilités dans les applications.

La fenêtre des propriétés de la vulnérabilité dans l'application sélectionnée s'affiche.

Consultation des statistiques relatives aux vulnérabilités sur les appareils administrés

Vous pouvez consulter les statistiques pour chaque vulnérabilité dans les applications des appareils administrés. Les statistiques sont représentées sous forme de diagramme. Le diagramme affiche le nombre d'appareils ayant les états suivants :

- *Ignorée sur : <nombre d'appareils>*. Cet état est attribué si vous avez réglé manuellement l'option d'ignorer la vulnérabilité dans les propriétés de cette dernière.
- *Corrigée sur : <nombre d'appareils>*. Cet état est attribué si la tâche visant à corriger la vulnérabilité est terminée avec succès.
- *Correctif prévu sur : <nombre d'appareils>*. Cet état est attribué si vous avez créé la tâche visant à corriger la vulnérabilité, mais qu'elle n'a pas encore été effectuée.
- *Correctif appliqué sur : <nombre d'appareils>*. Cet état est attribué si vous avez sélectionné manuellement la mise à jour du logiciel pour corriger la vulnérabilité, mais que cette mise à jour n'a pas corrigé la vulnérabilité.

- *Correctif nécessaire sur : <nombre d'appareils>*. Cet état est attribué si la vulnérabilité a été corrigée uniquement sur certains appareils administrés et si la correction de la vulnérabilité est nécessaire sur d'autres appareils.

Pour consulter les statistiques d'une vulnérabilité sur les appareils administrés :

1. Dans le menu principal, accédez à **Opérations → Gestion des correctifs → Vulnérabilités dans les applications**.

   La page affiche une liste des vulnérabilités dans les applications détectées sur les appareils administrés.

2. Cochez la case à côté de la vulnérabilité requise.

3. Cliquez sur le bouton **Statistiques de vulnérabilité sur les appareils**.

Un diagramme des états de la vulnérabilité s'affiche. Cliquer sur un état ouvre une liste des appareils sur lesquels la vulnérabilité possède l'état sélectionné.

Exportation de la liste des vulnérabilités dans les applications vers un fichier

Vous pouvez exporter la liste des vulnérabilités affichées au format CSV ou TXT. Vous pouvez par exemple utiliser ces fichiers pour les envoyer à votre responsable de la sécurité de l'information ou les stocker à des fins statistiques.

Pour exporter la liste des vulnérabilités dans les applications détectées sur tous les appareils administrés dans un fichier texte :

1. Dans le menu principal, accédez à **Opérations → Gestion des correctifs → Vulnérabilités dans les applications**.

   La page affiche une liste des vulnérabilités dans les applications détectées sur les appareils administrés.

2. Cliquez sur le bouton **Exporter vers un fichier TXT** ou **Exporter vers un fichier CSV** en fonction du format que vous préférez exporter.

Le fichier contenant la liste des vulnérabilités dans les applications est téléchargé sur l'appareil que vous utilisez actuellement.

Pour exporter la liste des vulnérabilités dans les applications détectées sur l'appareil administré sélectionné dans un fichier texte :

1. ouvrez la liste des vulnérabilités dans les applications détectées sur l'appareil administré sélectionné.

2. Sélectionnez les vulnérabilités dans les applications que vous souhaitez exporter.

   Ignorez cette étape si vous souhaitez exporter une liste complète des vulnérabilités dans les applications détectées sur l'appareil administré.

   Si vous souhaitez exporter la liste complète des vulnérabilités dans les applications détectées sur l'appareil administré, seules les vulnérabilités affichées sur la page actuelle seront exportées.

3. Cliquez sur le bouton **Exporter vers un fichier TXT** ou **Exporter vers un fichier CSV** en fonction du format que vous préférez exporter.

Le fichier contenant la liste des vulnérabilités dans les applications détectées sur l'appareil administré sélectionné est téléchargé sur l'appareil que vous utilisez actuellement.

Ignorer les vulnérabilités dans les applications

Vous pouvez ignorer les vulnérabilités dans les applications à corriger. Par exemple, les raisons d'ignorer les vulnérabilités dans les applications peuvent être les suivantes :

- Vous ne considérez pas la vulnérabilité dans l'application comme critique pour votre entreprise.
- Vous savez que la correction de la vulnérabilité dans l'application peut endommager les données relatives au logiciel pour lequel la correction de la vulnérabilité était nécessaire.
- Vous êtes sûr que la vulnérabilité dans l'application n'est pas dangereuse pour le réseau de votre entreprise car vous utilisez d'autres mesures pour protéger vos appareils administrés.

Vous pouvez ignorer une vulnérabilité dans une application sur tous appareils administrés ou seulement sur les appareils administrés sélectionnés.

Pour ignorer une vulnérabilité dans une application sur tous les appareils administrés :

1. Dans le menu principal, accédez à **Opérations → Gestion des correctifs → Vulnérabilités dans les applications**.

   La page affiche la liste des vulnérabilités dans les applications détectées sur les appareils administrés.

2. Cliquez sur le lien portant le nom de la vulnérabilité dans une application que vous souhaitez ignorer dans la liste des vulnérabilités dans les applications.

   La fenêtre des propriétés des vulnérabilités dans les applications s'ouvre.

3. Sous l'onglet **Général**, activez l'option **Ignorer la vulnérabilité**.

4. Cliquez sur le bouton **Enregistrer**.

   La fenêtre des propriétés de la vulnérabilité dans l'application se ferme.

La vulnérabilité dans l'application est ignorée sur les appareils administrés.

Pour ignorer une vulnérabilité dans l'application sur l'appareil administré sélectionné :

1. Dans le menu principal, accédez à **Ressources (Appareils) → Appareils administrés**.

   La liste des appareils administrés s'affiche.

2. Dans la liste des appareils administrés, cliquez sur le lien portant le nom de l'appareil pour lequel vous souhaitez ignorer une vulnérabilité dans une application.

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

3. Dans la fenêtre des propriétés de la Appareil, sélectionnez l'onglet **Avancé**.

4. Dans le volet gauche, sélectionnez la section **Vulnérabilités dans les applications**.

   La liste des vulnérabilités dans les applications détectées sur l'appareil s'affiche.

5. Sélectionnez la vulnérabilité que vous souhaitez ignorer sur l'appareil sélectionné dans la liste des vulnérabilités dans les applications.

   La fenêtre des propriétés des vulnérabilités dans les applications s'ouvre.

6. Dans la fenêtre des propriétés de la vulnérabilité dans l'application de l'onglet **Général**, activez l'option **Ignorer la vulnérabilité**.

7. Cliquez sur le bouton **Enregistrer**.

   La fenêtre des propriétés de la vulnérabilité dans l'application se ferme.

8. Fermez la fenêtre des propriétés de l'appareil.

La vulnérabilité dans l'application est ignorée sur l'appareil sélectionné.

La vulnérabilité dans l'application ignorée ne sera pas corrigée après la fin de la tâche *Corriger les vulnérabilités* ou de la tâche *Installation des mises à jour requises et correction des vulnérabilités*. Vous pouvez exclure les vulnérabilités logicielles ignorées de la liste des vulnérabilités à l'aide d'un filtre.

Scénario : rechercher et corriger les vulnérabilités dans les applications

Cette section fournit un scénario de recherche et de réparation des vulnérabilités sur les appareils administrés sous Windows. Vous pouvez rechercher et corriger les vulnérabilités dans les applications du système d'exploitation et dans les logiciels tiers, y compris les logiciels Microsoft.

Prérequis

- Kaspersky Security Center Cloud Console est déployé dans votre entreprise.
- Il existe des appareils administrés sous Windows dans votre organisation.

Étapes

La recherche et la correction des vulnérabilités dans les applications s'effectuent par étapes :

1. **Recherche de vulnérabilités dans les logiciels installés sur les appareils client**

   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 Cloud Console 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 démarrage rapide de l'application Kaspersky Security Center Cloud Console. Si vous n'aviez pas exécuté l'assistant, démarrez-le maintenant ou créez la tâche manuellement.

   Instructions pour : Créer la tâche Recherche de vulnérabilités et de mises à jour requises

2. **Analyser 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.

   Instructions pour :

   - Consultation des informations relatives aux vulnérabilités dans les applications

- Consultation des statistiques relatives aux vulnérabilités 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. La disponibilité de cette tâche dépend du mode de Kaspersky Security Center Cloud Console et de votre licence actuelle. 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* utilise les correctifs recommandés pour les logiciels Microsoft.

Vous pouvez démarrer l'assistant de correction des vulnérabilités qui crée automatiquement l'une de ces tâches ou vous pouvez créer l'une de ces tâches manuellement.

Instructions pratiques : correction des vulnérabilités dans les applications tierces, création de la tâche Installation des mises à jour requises et correction des vulnérabilités

4 Planification des tâches

Pour vous assurer que la liste des vulnérabilités est toujours d'actualité, planifiez la tâche *Recherche de vulnérabilités et de mises à jour requises* pour l'exécuter automatiquement de temps à autre. La fréquence moyenne recommandée est d'une fois par semaine.

Si vous avez créé la tâche *Installation des mises à jour requises et correction des vulnérabilités*, vous pouvez la planifier pour qu'elle soit exécutée à la même fréquence que la tâche *Recherche de vulnérabilités et de mises à jour requises* ou à une fréquence moindre. Lors de la planification de la tâche *Corriger les vulnérabilités*, notez que vous devez sélectionner des correctifs pour les logiciels Microsoft chaque fois avant de démarrer la tâche.

Lors de la planification des tâches, assurez-vous qu'une tâche pour corriger la vulnérabilité démarre une fois que la tâche *Recherche de vulnérabilités et de mises à jour requises* est terminée.

5 Ignorer les vulnérabilités dans les applications (facultatif)

Vous pouvez si vous les souhaitez ignorer les vulnérabilités dans les applications à corriger sur tous les appareils administrés ou seulement sur les appareils administrés sélectionnés.

Instructions : ignorer les vulnérabilités dans les applications

6 Exécution d'une tâche de correction de la vulnérabilité

Démarrez la tâche *Installation des mises à jour requises et correction des vulnérabilités* ou la tâche *Corriger les vulnérabilités*. Une fois la tâche terminée, assurez-vous qu'elle possède le statut *Terminée* dans la liste des tâches.

7 Créer le rapport sur les résultats de la correction des vulnérabilités dans les applications (facultatif)

Pour consulter les statistiques détaillées concernant la correction des vulnérabilités, générez le rapport sur les vulnérabilités. Le rapport affiche des informations sur les vulnérabilités dans les applications non corrigées. Ainsi, vous pouvez vous faire une idée de la recherche et la correction des vulnérabilités dans les logiciels tiers, y compris les logiciels Microsoft, dans votre organisation.

Instructions : génération et affichage d'un rapport

8 Vérification de la configuration de la recherche et de la correction des vulnérabilités dans les logiciels tiers

Assurez-vous des points suivants :

- La liste des vulnérabilités dans les applications sur les appareils administrés n'est pas vide.

- Une tâche de correction de la vulnérabilité est dans la liste des tâches.
- Les tâches de recherche et de correction des vulnérabilités sont planifiées pour qu'elles démarrent en séquence. Affichez les propriétés de ces tâches et comparez leur planification.
- La tâche de correction des vulnérabilités dans les applications s'est terminée avec succès. Affichez les informations sous l'onglet **Résultats** de la fenêtre de propriétés de la tâche.

Résultats

Si vous avez créé et configuré la tâche *Installation des mises à jour requises et correction des vulnérabilités*, les vulnérabilités sont corrigées automatiquement sur les appareils administrés. Lorsque la tâche est exécutée, elle met en corrélation la liste des mises à jour du logiciel disponibles avec les règles spécifiées dans les paramètres de la tâche. Toutes les mises à jour du logiciel qui répondent aux critères des règles seront téléchargées dans les stockages des points de distribution et seront installées pour corriger les vulnérabilités dans les applications, à l'exception des mises à jour Windows. Pour installer les mises à jour Windows, vous devez garantir l'accès aux serveurs publics de mises à jour de Microsoft sur vos appareils administrés.

Si vous avez créé la tâche *Corriger les vulnérabilités*, seules les vulnérabilités dans les applications des logiciels Microsoft sont corrigées.

Définition de la durée maximale de stockage des informations sur les vulnérabilités corrigées

Pour définir la période de stockage maximale dans la base de données pour les informations sur les vulnérabilités qui ont déjà été corrigées sur les appareils administrés, procédez comme suit :

1. Dans le menu principal, cliquez sur l'icône des paramètres ( ) en regard du nom du Serveur d'administration requis.

   La fenêtre des propriétés du Serveur d'administration s'ouvre.

2. Sur la page qui s'ouvre, accédez à l'onglet **Stockage d'événements**.

3. Indiquez la période de stockage maximale des informations sur les vulnérabilités corrigées dans la base de données.

   Par défaut, la durée de stockage est de 7 jours en mode d'essai et de 60 jours en mode commercial. La limite maximale est de 14 jours en mode d'essai et de 365 jours en mode commercial.

4. Cliquez sur **Enregistrer**.

La période de stockage maximale des informations sur les vulnérabilités corrigées est limitée au nombre de jours indiqué.

Gestion des applications exécutées sur les appareils client

Cette section décrit les fonctions de Kaspersky Security Center Cloud Console associées à la gestion des applications tierces installées sur les appareils client.

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 Cloud Console est déployé dans votre entreprise.
- La stratégie de Kaspersky Endpoint Security for Windows ou de Kaspersky Endpoint Security for Linux est créée et active.

Étapes

Le scénario d'utilisation Contrôle des applications se déroule par étapes :

1. **Formation et consultation de la liste des fichiers exécutables sur les appareils client**

   Cette étape vous permet de découvrir les fichiers exécutables qui figurent sur les appareils administrés. Consultez la liste des fichiers exécutables et comparez-la avec les listes des fichiers exécutables autorisés et interdits. Les restrictions d'utilisation des fichiers exécutables peuvent être liées aux stratégies de sécurité de l'information dans votre entreprise.

   Instructions pour : Obtention et consultation d'une liste des fichiers exécutables installés sur les appareils client

2. **Création de catégories pour les fichiers exécutables utilisés dans votre organisation**

   Analysez les listes des fichiers exécutables stockés sur les appareils administrés. En fonction de l'analyse, créez des catégories pour les fichiers exécutables. Il est recommandé de créer une catégorie "Applications de travail" qui englobe l'ensemble standard des fichiers exécutables utilisés dans votre organisation. Si différents groupes de sécurité utilisent leurs propres ensembles de fichiers exécutables dans leur travail, une catégorie distincte peut être créée pour chaque groupe de sécurité.

   Instructions pour : création d'une catégorie d'applications enrichie manuellement, création d'une catégorie d'applications incluant des fichiers exécutables provenant des appareils sélectionnés

3. **Configuration du Contrôle des applications dans la stratégie Kaspersky Endpoint Security for Windows**

   Configurez le composant Contrôle des applications dans la stratégie Kaspersky Endpoint Security for Windows 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 pour : Configuration du composant Contrôle des applications dans la stratégie Kaspersky Endpoint Security for Windows. Suivez ces instructions et activez le mode test dans le processus de configuration.

5. **Modification des paramètres des catégories du composant Contrôle des applications**

   Si nécessaire, modifiez les paramètres du Contrôle des applications. Selon les résultats des tests, vous pouvez ajouter des fichiers exécutables associés aux événements du composant Contrôle des applications à une catégorie d'applications enrichie manuellement.

   Instructions pour : Ajout de fichiers exécutables liés par un événement à la catégorie d'applications

6. **Appliquer les règles de 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 pour : Configuration du composant Contrôle des applications dans la stratégie Kaspersky Endpoint Security for Windows. Suivez ces instructions et désactivez le mode test dans le processus de configuration.

7. **Vérification de la configuration du Contrôle des applications**

   Assurez-vous des points suivants :

   - La liste des catégories des fichiers exécutables n'est pas vide. Affichez la liste des catégories et assurez-vous qu'elle contient les catégories que vous avez configurées.
   - La configuration du Contrôle des applications se fait à l'aide de catégories créées pour les fichiers exécutables. Affichez les paramètres de la stratégie de Kaspersky Endpoint Security for Windows et assurez-vous d'avoir configuré le Contrôle des applications dans **Paramètres des applications** → **Contrôles de sécurité** → **Contrôle des applications**.
   - Les règles de Contrôle des applications sont appliquées en mode de fonctionnement. Vérifiez le mode dans la stratégie de Kaspersky Endpoint Security for Windows et assurez-vous d'avoir désactivé le **Mode de test** dans **Paramètres des applications** → **Contrôles de sécurité** → **Contrôle des applications**.

Résultats

Une fois le scénario terminé, le démarrage des fichiers exécutables est contrôlé sur les appareils administrés. Les utilisateurs peuvent uniquement exécuter les fichiers exécutables autorisés dans votre organisation et ne peuvent pas exécuter les fichiers exécutables qui y sont interdits.

Pour obtenir des informations détaillées sur le Contrôle des applications, consultez les rubriques d'aide suivantes :

- Aide en ligne de Kaspersky Endpoint Security for Windows
- Aide en ligne de Kaspersky Endpoint Security for Linux

Modes et catégories du Contrôle des applications

Le module Contrôle des applications surveille les tentatives des utilisateurs de lancer des fichiers exécutables. Vous pouvez utiliser les règles du Contrôle des applications pour contrôler le lancement des fichiers exécutables.

Le module Contrôle des applications est disponible pour Kaspersky Endpoint Security for Windows et pour Kaspersky Endpoint Security for Linux (version 11.2 et suivante). Toutes les instructions de cette section décrivent la configuration du Contrôle des applications pour Kaspersky Endpoint Security.

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. Le mode *Liste de refus* est sélectionné par défaut.
- *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 deux types de catégories dans Kaspersky Security Center Cloud Console :

- Catégorie complétée à la main. vous définissez des conditions, par exemple les métadonnées du fichier, le hashcode du fichier, le certificat du fichier, la catégorie KL, le chemin d'accès au fichier, afin d'inclure des fichiers exécutables dans la catégorie.
- Catégorie incluant des fichiers exécutables depuis les appareils sélectionnés. Vous spécifiez un appareil dont les fichiers exécutables sont automatiquement inclus dans la catégorie.

Pour obtenir des informations détaillées sur le Contrôle des applications, consultez les rubriques d'aide suivantes :

- Aide en ligne de Kaspersky Endpoint Security for Windows
- Aide en ligne de Kaspersky Endpoint Security for Linux

Obtention et consultation d'une liste des applications installées sur les appareils client

Kaspersky Security Center Cloud Console 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, la liste des mises à jour du logiciel disponibles et la liste des vulnérabilités dans les applications détectées.

2. Vous pouvez regrouper et filtrer les données du tableau avec les applications installées comme suit :

- Cliquez sur l'icône des paramètres ( ) dans le coin supérieur droit du tableau.

  Dans le menu **Paramètres des colonnes** affiché, sélectionnez les colonnes à afficher dans le tableau. Pour consulter le type de système d'exploitation des appareils clients sur lesquels l'application est installée, sélectionnez la colonne **Type de S.E**.

- Cliquez sur l'icône du filtre ( ) dans le coin supérieur droit du tableau, puis indiquez et appliquez le critère de filtre dans le menu appelé.

  Le tableau filtré des applications installées s'affiche.

Pour afficher la liste des applications installées sur un appareil administré spécifique,

Dans le menu principal, accédez à **Appareils** → **Appareils administrés** → **<nom de l'appareil>** → **Avancé** → **Registre des applications**. Dans ce menu, vous pouvez exporter la liste des applications vers un fichier CSV ou un fichier TXT.

Pour obtenir des informations détaillées sur le Contrôle des applications, consultez les rubriques d'aide suivantes :

- Aide en ligne de Kaspersky Endpoint Security for Windows
- Aide en ligne de Kaspersky Endpoint Security for Linux

Obtention et consultation d'une liste des fichiers exécutables installés sur les appareils client

Vous pouvez obtenir la liste des fichiers exécutables stockés sur les appareils clients de l'une des manières suivantes :

- Activation des notifications sur le démarrage des applications dans la stratégie de Kaspersky Endpoint Security.
- Création d'une tâche d'inventaire.

Activation des notifications sur le démarrage des applications dans la stratégie de Kaspersky Endpoint Security

Pour activer les notifications relatives au démarrage des applications, procédez comme suit :

1. Ouvrez les paramètres de la stratégie de Kaspersky Endpoint Security, puis accédez à **Paramètres généraux** → **Rapports et stockage**.
2. Dans le groupe de paramètres **Transfert de données au Serveur d'administration**, cochez la case **À propos des applications lancées** et enregistrez les modifications.

Lorsqu'un utilisateur tente de lancer des fichiers exécutables, les informations relatives à ces fichiers sont ajoutées à la liste des fichiers exécutables sur un appareil client. Kaspersky Endpoint Security envoie ces informations à l'Agent d'administration, qui les transmet ensuite au Serveur d'administration.

Création d'une tâche d'inventaire

La fonction d'inventaire des fichiers exécutables est disponible pour les applications suivantes :

- Kaspersky Endpoint Security for Windows

- Kaspersky Endpoint Security for Linux (version 11.2 et suivante)

Vous pouvez réduire la charge sur la base de données tout en obtenant des informations sur les applications installées. Pour ce faire, il est recommandé d'exécuter une tâche d'inventaire sur les appareils de référence sur lesquels un ensemble standard de logiciels est installé. Il est préférable que le nombre d'appareils soit compris entre 1 et 3.

Nous vous déconseillons fortement d'exécuter la tâche d'inventaire lors de l'utilisation des bases de données suivantes : MySQL, PostgreSQL, SQL Server Express Edition et MariaDB (toutes les éditions).

Pour créer une tâche d'inventaire des fichiers exécutables sur les appareils clients, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Tâches**.

   La liste des tâches s'affiche.

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

   Ceci permet de lancer l'assistant de création d'une tâche. Suivez les étapes de l'assistant.

3. Sur la page **Paramètres de nouvelle tâche**, dans la liste déroulante **Application**, sélectionnez Kaspersky Endpoint Security for Windows ou Kaspersky Endpoint Security for Linux, selon le type de système d'exploitation des appareils clients.

4. À partir de la liste déroulante **Type de tâche**, sélectionnez **Inventaire**.

5. Sur la page **Fin de la création de la tâche**, cliquez sur le bouton **Terminer**.

   Une fois que l'assistant de création d'une tâche a terminé l'opération, la tâche **Inventaire** est créée et configurée. Si vous le souhaitez, vous pouvez modifier les paramètres de la tâche créée. La tâche qui vient d'être créée s'affiche dans la liste des tâches.

Pour obtenir une description détaillée de la tâche d'inventaire, consultez les aides suivantes :

- Aide de Kaspersky Endpoint Security for Windows
- Aide de Kaspersky Endpoint Security for Linux

Une fois la tâche **Inventaire** effectuée, la liste des fichiers exécutables installée sur les appareils administrés est créée et vous pouvez la consulter.

Lors de l'inventaire, les formats de fichiers exécutables 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 installés sur les appareils client.

Si nécessaire, vous pouvez envoyer le fichier exécutables de l'appareil administré à l'appareil sur lequel Kaspersky Security Center Cloud 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**. Le total des appareils pour lesquels l'option **Maintenir la connexion au Serveur &d'administration** a été sélectionnée ne peut être supérieur à 300.

4. Cliquez sur le bouton **Envoyer**.

Le fichier exécutable sélectionné est téléchargé pour être envoyé ultérieurement vers l'appareil sur lequel Kaspersky Security Center Cloud Console est ouvert.

Création d'une catégorie d'applications enrichie manuellement

Vous pouvez spécifier un ensemble de critères comme modèle pour les fichiers exécutables dont vous souhaitez autoriser ou bloquer le démarrage dans votre entreprise. En vous basant sur les fichiers exécutables correspondant aux critères, vous pouvez créer une catégorie d'applications et l'utiliser dans la configuration du composant Contrôle des applications.

Pour créer une catégorie d'applications enrichie manuellement, procédez comme suit :

1. Dans le menu principal, accédez à **Opérations** → **Applications tierces** → **Catégories d'applications**.

   La page comportant une liste des catégories d'applications s'affiche.

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

   L'Assistant de nouvelle catégorie démarre. Parcourez les étapes de l'Assistant à l'aide du bouton **Suivant**.

3. À l'étape **Sélectionner la méthode de création de catégorie**, sélectionnez l'option **Catégorie dont le contenu a été ajouté manuellement. Les données des fichiers exécutables sont ajoutées manuellement à la catégorie**.

4. À l'étape **Conditions**, cliquez sur le bouton **Ajouter** pour ajouter un critère de condition d'inclusion de fichiers à la catégorie créée.

5. À l'étape **Critère de condition**, sélectionnez un type de règle pour la création de la catégorie dans la liste :

   - 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.

- Définir le chemin d'accès à l'application (masques pris en charge)

  Si cette option a été sélectionnée, vous pouvez indiquer le chemin d'accès au fichier ou au dossier sur l'appareil client dont les fichiers exécutables seront ajoutés dans une catégorie d'applications définie par l'utilisateur. Vous pouvez utiliser des expressions régulières, comme *C:\path_to_exe** : *C:\Program Files\Internet Explorer**.

- Disque amovible

  Si cette option a été sélectionnée, vous pouvez indiquer le type de support (n'importe lequel ou disque amovible) sur lequel l'application est exécutée. Les applications, lancées sur le moyen de type sélectionné, seront ajoutées dans une catégorie d'applications définie par l'utilisateur.

- **Hash, métadonnées ou certificat** :

  - Sélectionner dans la liste des fichiers exécutables

    Si vous avez choisi cette option, vous pouvez sélectionner les applications à ajouter à une catégorie dans la liste des fichiers exécutables de l'appareil client.

  - Sélectionner dans le registre des applications

Si cette option est sélectionnée, le registre des applications s'affiche. Après avoir sélectionné une application dans le registre, la fenêtre s'ouvre avec les paramètres remplis par les métadonnées de l'application sélectionnée :

- Nom du fichier.
- Version du fichier. Vous pouvez spécifier une valeur précise pour la version ou décrire une condition, par exemple " supérieure à 5.0 ".
- Nom de l'application.
- Version de l'application. Vous pouvez spécifier une valeur précise pour la version ou décrire une condition, par exemple " supérieure à 5.0 ".
- Fournisseur.

Veuillez noter que seul le lancement des fichiers exécutables répondant aux paramètres spécifiés est bloqué, et non le lancement de l'application que vous sélectionnez. Si les métadonnées de l'application sélectionnée correspondent à celles du fichier exécutable qui est lancé lors du lancement de l'application, vous pouvez passer à l'étape suivante. Sinon, vous devez modifier les valeurs manuellement pour qu'elles correspondent aux métadonnées du fichier exécutable.

- **Définir manuellement**

Si cette option est sélectionnée, vous devez indiquer le hash du fichier, ou les métadonnées ou le certificat en guise de condition d'ajout des applications à la catégorie utilisateur.

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 Cloud Console pour les fichiers de la catégorie. Les informations relatives aux valeurs de hachage calculées par les fonctions de hachage sont stockées dans la base de données du Serveur d'administration.

SHA256 est une fonction de hachage cryptographique dont l'algorithme du calcul ne contient pas de vulnérabilités et il est considéré actuellement comme la fonction de chiffrement la plus sûre. Kaspersky Endpoint Security 10 Service Pack 2 for Windows et suivants prennent en charge le calcul de la fonction hash SHA256. Le calcul de la fonction de hachage MD5 est pris en charge pour les versions inférieures à Kaspersky Endpoint Security 10 Service Pack 2 for Windows.

Choisissez une des options du calcul de la fonction hash par l'application Kaspersky Security Center Cloud Console pour les fichiers de la catégorie :

- Si toutes les instances des applications de sécurité installées sur votre réseau sont Kaspersky Endpoint Security 10 Service Pack 2 for Windows ou des versions ultérieures, cochez la case **SHA256**. Il est déconseillé d'ajouter une catégorie créée selon le critère du hachage SHA256 du fichier exécutable pour les versions de l'application antérieures à Kaspersky Endpoint Security 10 Service Pack 2 for Windows. Cela pourrait entraîner un échec de l'application de sécurité. Dans ce cas vous pouvez utiliser la fonction de hachage cryptographique MD5 pour les fichiers de la catégorie.

- Si des versions antérieures à Kaspersky Endpoint Security 10 Service Pack 2 for Windows sont installées sur votre réseau, sélectionnez **Hash MD5**. Il est interdit d'ajouter une catégorie créée selon le critère de la somme de contrôle MD5 du fichier exécutable pour les versions Kaspersky Endpoint Security 10 Service Pack 2 for Windows et suivantes. Dans ce cas vous pouvez utiliser la fonction de hachage cryptographique SHA256 pour les fichiers de la catégorie.

- Si différents appareils de votre réseau utilisent à la fois des versions antérieures et ultérieures de Kaspersky Endpoint Security 10, cochez à la fois la case **SHA256** et la case **Hash MD5**.

Données méta

Si cette option est sélectionnée, vous pouvez spécifier les métadonnées du fichier, telles que le nom du fichier, la version du fichier, le fournisseur. La condition de catégorie ne concerne que les fichiers exécutables ayant les mêmes métadonnées.

Certificat

Si cette option a été sélectionnée, vous pouvez indiquer les certificats du stockage. La condition de catégorie correspond uniquement aux fichiers exécutables signés par le certificat spécifié.

- Depuis un fichier ou un paquet MSI / un fichier archivé

Si cette option a été sélectionnée, vous pouvez indiquer le fichier de l'installateur MSI en tant que la condition d'ajout des applications dans une catégorie d'utilisateur. Les données méta de l'installateur de l'application seront transmises sur le Serveur d'administration. Les applications, dont les données méta de l'installateur coïncident avec l'installateur MSI indiqué, seront ajoutées dans une catégorie d'applications définie par l'utilisateur.

Le critère sélectionné est ajouté à la liste des conditions.

Vous pouvez ajouter autant de critères que nécessaire à la création de la catégorie d'applications.

6. À l'étape **Exclusions**, cliquez sur le bouton **Ajouter** pour ajouter un critère de condition d'exclusion de fichiers de la catégorie en cours de création.

7. À l'étape **Critère de condition**, sélectionnez un type de règle dans la liste, comme vous avez sélectionné une règle pour la création de la catégorie.

   Lorsque l'Assistant a terminé l'opération, la catégorie d'applications est créée. Elle s'affiche dans la liste des catégories d'applications. Vous pouvez utiliser la catégorie d'application créée lorsque vous configurez le Contrôle des applications.

Pour obtenir des informations détaillées sur le Contrôle des applications, consultez les rubriques d'aide suivantes :

- Aide en ligne de Kaspersky Endpoint Security for Windows
- Aide en ligne de Kaspersky Endpoint Security for Linux

Création d'une catégorie d'applications incluant des fichiers exécutables provenant des appareils sélectionnés

Vous pouvez utiliser des fichiers exécutables des appareils sélectionnés comme modèle des fichiers exécutables que vous souhaitez autoriser ou bloquer. En vous basant sur les fichiers exécutables des appareils sélectionnés, vous pouvez créer une catégorie et l'utiliser dans la configuration du composant Contrôle des applications.

Pour créer une catégorie incluant des fichiers exécutables provenant des appareils sélectionnés :

1. Dans le menu principal, accédez à **Opérations** → **Applications tierces** → **Catégories d'applications**.

   La page comportant une liste des catégories de fichiers exécutables s'affiche.

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

   L'Assistant de nouvelle catégorie démarre. Parcourez les étapes de l'assistant à l'aide du bouton **Suivant**.

3. À l'étape **Sélectionner la méthode de création de catégorie**, spécifiez le nom de la catégorie et sélectionnez l'option **Catégorie qui reprend les fichiers exécutables issus d'appareils sélectionnés. Ces fichiers exécutables sont traités automatiquement et leurs métriques sont ajoutées à la catégorie**.

4. Cliquez sur le bouton **Ajouter**.

5. Dans la fenêtre qui s'ouvre, sélectionnez l'appareil (les appareils) dont les fichiers exécutables seront utilisés pour créer la catégorie.

6. Définissez les paramètres suivants :

   - Algorithme de calcul de la fonction hash

En fonction de la version de l'application de sécurité installée sur les appareils de votre réseau, il faut choisir un algorithme de calcul de la fonction hash par l'application Kaspersky Security Center Cloud Console pour les fichiers de la catégorie. Les informations relatives aux valeurs de hachage calculées par les fonctions de hachage sont stockées dans la base de données du Serveur d'administration.

SHA256 est une fonction de hachage cryptographique dont l'algorithme du calcul ne contient pas de vulnérabilités et il est considéré actuellement comme la fonction de chiffrement la plus sûre. Kaspersky Endpoint Security 10 Service Pack 2 for Windows et suivants prennent en charge le calcul de la fonction hash SHA256. Le calcul de la fonction de hachage MD5 est pris en charge pour les versions inférieures à Kaspersky Endpoint Security 10 Service Pack 2 for Windows.

Choisissez une des options du calcul de la fonction hash par l'application Kaspersky Security Center Cloud Console pour les fichiers de la catégorie :

- Si toutes les instances des applications de sécurité installées sur votre réseau sont Kaspersky Endpoint Security 10 Service Pack 2 for Windows ou des versions ultérieures, cochez la case **SHA256**. Il est déconseillé d'ajouter une catégorie créée selon le critère du hachage SHA256 du fichier exécutable pour les versions de l'application antérieures à Kaspersky Endpoint Security 10 Service Pack 2 for Windows. Cela pourrait entraîner un échec de l'application de sécurité. Dans ce cas vous pouvez utiliser la fonction de hachage cryptographique MD5 pour les fichiers de la catégorie.

- Si des versions antérieures à Kaspersky Endpoint Security 10 Service Pack 2 for Windows sont installées sur votre réseau, sélectionnez **Hash MD5**. Il est interdit d'ajouter une catégorie créée selon le critère de la somme de contrôle MD5 du fichier exécutable pour les versions Kaspersky Endpoint Security 10 Service Pack 2 for Windows et suivantes. Dans ce cas vous pouvez utiliser la fonction de hachage cryptographique SHA256 pour les fichiers de la catégorie.

Si différents appareils de votre réseau utilisent à la fois des versions antérieures et ultérieures de Kaspersky Endpoint Security 10, cochez à la fois la case **SHA256** et la case **Hash MD5**.

La case **Calculer SHA256 pour les fichiers en la catégorie (pris en charge pour Kaspersky Endpoint Security 10 Service Pack 2 for Windows et versions supérieures)** est cochée par défaut.

La case **Calculer MD5 pour les fichiers en la catégorie (pris en charge pour les versions inférieures à Kaspersky Endpoint Security 10 Service Pack 2 for Windows)** est décochée.

- Synchroniser les données avec le stockage du Serveur d'administration

Sélectionnez cette option si vous souhaitez que le Serveur d'administration vérifie régulièrement les modifications dans le ou les dossiers spécifiés.

Cette option est Inactif par défaut.

Si vous activez cette option, indiquez la période (en heures) pour vérifier les modifications dans le ou les dossiers spécifiés. L'intervalle de l'analyse est de 24 heures par défaut.

- Type de fichier

Dans cette section, vous pouvez spécifier le type de fichier utilisé pour créer la catégorie d'applications.

tous les fichiers ;. Tous les fichiers sont pris en compte lors de la création de la catégorie. Cette option est sélectionnée par défaut.

Uniquement les fichiers hors des catégories d'applications. Seuls les fichiers hors catégories d'applications sont pris en compte lors de la création de la catégorie.

- Dossiers

Dans cette section, vous pouvez spécifier les dossiers de l'appareil (des appareils) sélectionné(s) contenant les fichiers utilisés pour créer la catégorie d'applications.

Tous les dossiers. Tous les dossiers sont pris en compte pour la catégorie en cours de création. Cette option est sélectionnée par défaut.

Dossier indiqué. Seul le dossier spécifié est pris en compte pour la catégorie en cours de création. Si vous sélectionnez cette option, vous devez indiquer le chemin d'accès au dossier.

À la fin de l'Assistant, la catégorie des fichiers exécutables est créée. Elle s'affiche dans la liste des catégories. Vous pouvez utiliser la catégorie créée lorsque vous configurez le Contrôle des applications.

Affichage de la liste des catégories d'applications

Vous pouvez consulter la liste des catégories d'applications configurées et les paramètres de chaque catégorie d'applications.

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 d'applications s'affiche.

Pour consulter les propriétés d'une catégorie d'applications,

Cliquez sur le nom de la catégorie d'applications.

La fenêtre des propriétés de la catégorie d'applications s'affiche. Les propriétés sont regroupées sur plusieurs onglets.

Configuration du Contrôle des applications dans la stratégie Kaspersky Endpoint Security for Windows

Après avoir créé les catégories du Contrôle des applications, vous pouvez les utiliser pour la configuration du Contrôle des applications dans les stratégies Kaspersky Endpoint Security for Windows.

Pour configurer le Contrôle des applications dans la stratégie Kaspersky Endpoint Security for Windows :

1. Dans le menu principal, accédez à **Ressources (Appareils) → Stratégies et profils**.
   Une page comportant une liste des stratégies s'affiche.
2. Cliquez sur la stratégie **Kaspersky Endpoint Security for Windows**.
   La fenêtre des paramètres de la stratégie s'ouvre.
3. Accédez à **Paramètres 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 de Contrôle des applications et autorisez Kaspersky Endpoint Security for Windows à bloquer le lancement des applications.

   Si vous souhaitez tester les règles de Contrôle des applications, activez le mode test dans la section **Paramètres du Contrôle des applications**. En mode test, Kaspersky Endpoint Security for Windows ne bloque pas le lancement des applications, mais consigne dans le rapport les informations relatives aux règles déclenchées. Cliquez sur le lien **Consulter le rapport** pour afficher ces informations.

6. Activez l'option **Contrôler le chargement des modules DLL** si vous souhaitez que Kaspersky Endpoint Security for Windows surveille le chargement des modules DLL lorsque des applications sont démarrées par les utilisateurs.

   Les informations concernant le module et l'application ayant chargé le module seront enregistrées dans un rapport.

   Kaspersky Endpoint Security for Windows surveille uniquement les modules DLL et les pilotes chargés après que l'option **Contrôler le chargement des modules DLL** a été sélectionnée. Redémarrez l'ordinateur après avoir sélectionné l'option **Contrôler le chargement des modules DLL** si vous souhaitez que Kaspersky Endpoint Security for Windows surveille tous les modules DLL et les pilotes, y compris ceux qui ont été chargés avant le démarrage de Kaspersky Endpoint Security for Windows.

7. (Facultatif) Dans le bloc **Modèles de message**, vous pouvez modifier le modèle du message qui s'affiche lorsque le démarrage d'une application est bloqué et lorsque le modèle d'email vous est envoyé.

8. Dans les paramètres du groupe **Mode de contrôle des applications**, sélectionnez le mode **Liste de refus** ou **Liste d'autorisation**.

   Le mode **Liste de refus** est sélectionné par défaut.

9. Cliquez sur le lien **Paramètres des listes de règles**.

   La fenêtre **Listes de refus et d'autorisation** s'ouvre pour vous permettre d'ajouter une catégorie d'applications. Par défaut, l'onglet **Liste de refus** est sélectionné si le mode **Liste de refus** est sélectionné ou l'onglet **Liste d'autorisation** est sélectionné si le mode **Liste d'autorisation** est sélectionné.

10. Dans la fenêtre **Listes de refus et listes d'autorisation**, cliquez sur le bouton **Ajouter**.

    La fenêtre **Règle de contrôle des applications** s'ouvre.

11. Cliquez sur le lien **Veuillez choisir une catégorie**.

    La fenêtre **Catégorie d'applications** s'ouvre.

12. Ajoutez la ou les catégories d'applications que vous avez créées précédemment.

    Vous pouvez modifier les paramètres d'une catégorie créée en cliquant sur le bouton **Modifier**.

    Vous pouvez créer une nouvelle catégorie en cliquant sur le bouton **Ajouter**.

    Vous pouvez supprimer une catégorie dans la liste en cliquant sur le bouton **Supprimer**.

13. Une fois que la liste des catégories d'applications est complète, cliquez sur le bouton **OK**.

    La fenêtre **Catégorie d'applications** se ferme.

14. Dans la fenêtre de la règle de **Contrôle des applications**, créez la liste des utilisateurs et des groupes d'utilisateurs auxquels s'applique la règle de Contrôle des applications dans la section **Sujets et leurs droits**.

15. Cliquez sur le bouton **OK** pour enregistrer les paramètres et fermer la fenêtre **Règle du contrôle des applications**.

16. Cliquez sur le bouton **OK** pour enregistrer les paramètres et fermer la fenêtre **Listes de refus et listes d'autorisation**.

17. Cliquez sur le bouton **OK** pour enregistrer les paramètres et fermer la fenêtre **Contrôle des applications**.

18. Fermez la fenêtre avec les paramètres de la stratégie de Kaspersky Endpoint Security for Windows.

    Le Contrôle des applications est configuré. Une fois la stratégie propagée aux appareils client, le démarrage des fichiers exécutables est administré.

Pour obtenir des informations détaillées sur le Contrôle des applications, consultez les rubriques d'aide suivantes :

- Aide en ligne de Kaspersky Endpoint Security for Windows
- Aide en ligne de Kaspersky Endpoint Security for Linux

Ajout de fichiers exécutables liés par un événement à la catégorie d'applications

Une fois que le Contrôle des applications est configuré dans les stratégies Kaspersky Endpoint Security for Windows, les événements suivants s'affichent dans la liste des événements :

- **Lancement de l'application interdit** (événement *Critique*). Cet événement s'affiche si vous avez configuré le Contrôle des applications pour appliquer des règles.
- **Lancement de l'application interdit en mode de test** (événement d'*Information*). Cet événement s'affiche si vous avez configuré le Contrôle des applications pour tester des règles.
- **Message à l'administrateur concernant l'interdiction de lancement de l'application** (l'événement *Avertissement*). Cet événement s'affiche si vous avez configuré le Contrôle des applications pour appliquer des règles et si un utilisateur a demandé à accéder à l'application dont le démarrage est bloqué.

Il est recommandé de créer des sélections d'événements pour consulter les événements associés au fonctionnement du Contrôle des applications.

Vous pouvez ajouter des fichiers exécutables associés aux événements du Contrôle des applications à une catégorie d'applications existante ou à une nouvelle catégorie d'applications. Vous pouvez ajouter des fichiers exécutables uniquement à une catégorie d'applications enrichie manuellement.

Pour ajouter des fichiers exécutables liés aux événements du Contrôle des applications à une catégorie d'applications :

1. Dans le menu principal, accédez à **Surveillance et rapports → Sélections d'événements**.

   La liste des sélections d'événements s'affiche.

2. Sélectionnez la sélection d'événements pour consulter les événements associés au Contrôle des applications et démarrer cette sélection d'événements.

   Si vous n'avez pas créé de sélection d'événements associée au Contrôle des applications, vous pouvez sélectionner et démarrer une sélection prédéfinie, par exemple, les **Événements récents**.

   La liste des événements s'affiche.

3. Sélectionnez les événements dont vous souhaitez ajouter les fichiers exécutables associés à la catégorie d'applications, puis cliquez sur le bouton **Affecter à une catégorie**.

   L'Assistant de nouvelle catégorie démarre. Parcourez les étapes de l'assistant à l'aide du bouton **Suivant**.

4. Indiquez les paramètres appropriés sur la page de l'assistant :

   - Dans la section **Action sur le fichier exécutable lié à l'événement**, sélectionnez une des options suivantes :

     - Ajoute une nouvelle catégorie d'applications

       Sélectionnez cette option si vous souhaitez créer une nouvelle catégorie d'applications basée sur des fichiers exécutables liés par un événement.

       Cette option est sélectionnée par défaut.

       Si vous avez sélectionné cette option, indiquez un nouveau nom de catégorie.

     - Ajouter à une catégorie d'application existante

       Sélectionnez cette option s'il est nécessaire d'ajouter des fichiers exécutables liés par un événement à une catégorie d'applications existante.

       Par défaut, cette option n'est pas sélectionnée.

       Si vous avez sélectionné cette option, sélectionnez la catégorie d'applications enrichie manuellement à laquelle vous souhaitez ajouter les fichiers exécutables.

   - Dans la section **Type de règle**, sélectionnez une des options suivantes :

     - **Règles pour l'ajout aux inclusions**
     - **Règles pour l'ajout aux exclusions**

   - Dans la section **Paramètre utilisé comme condition**, sélectionnez une des options suivantes :

     - Détails du certificat (ou hash SHA256 pour les fichiers sans certificat)

       Les fichiers peuvent être signés par un certificat. De plus un certificat peut signer plusieurs fichiers. Par exemple, différentes versions d'une application peuvent être signées par un certificat ou plusieurs applications différentes d'un même éditeur peuvent être signées par un même certificat. En cas de sélection du certificat, la catégorie peut reprendre plusieurs versions de l'application ou plusieurs applications d'un même éditeur.

       Chaque fichier possède sa propre fonction de hachage SHA256 unique. En cas de sélection de la fonction hash SHA256, la catégorie reprend uniquement un seul fichier correspondant, par exemple, la version définie de l'application.

       Sélectionnez cette option si vous souhaitez ajouter les données du certificat du fichier exécutable (ou la fonction hash SHA256 pour les fichiers sans certificat) aux règles de la catégorie.

       Cette option est sélectionnée par défaut.

     - Détails du certificat (les fichiers sans certificat sont ignorés)

Les fichiers peuvent être signés par un certificat. De plus un certificat peut signer plusieurs fichiers. Par exemple, différentes versions d'une application peuvent être signées par un certificat ou plusieurs applications différentes d'un même éditeur peuvent être signées par un même certificat. En cas de sélection du certificat, la catégorie peut reprendre plusieurs versions de l'application ou plusieurs applications d'un même éditeur.

Sélectionnez cette option si vous souhaitez ajouter les données du certificat du fichier exécutable aux règles de la catégorie. Si le fichier exécutable n'a pas de certificat, ce fichier sera ignoré. Les informations le concernant ne seront pas ajoutées dans la catégorie.

- **SHA256 uniquement (les fichiers sans hash sont ignorés)**

  Chaque fichier possède sa propre fonction de hachage SHA256 unique. En cas de sélection de la fonction hash SHA256, la catégorie reprend uniquement un seul fichier correspondant, par exemple, la version définie de l'application.

  Sélectionnez cette option si vous souhaitez ajouter uniquement les données de la fonction hash SHA256 du fichier exécutable.

- **MD5 uniquement (mode supprimé, uniquement pour Kaspersky Endpoint Security 10 Service Pack 1)**

  Chaque fichier possède sa propre fonction de hachage MD5 unique. En cas de sélection de la fonction hash MD5, la catégorie reprend uniquement un seul fichier correspondant, par exemple, la version définie de l'application.

  Sélectionnez cette option si vous souhaitez ajouter uniquement les données de la fonction hash MD5 du fichier exécutable. Le calcul de la fonction de hachage MD5 est pris en charge pour les versions inférieures à Kaspersky Endpoint Security 10 Service Pack 1 for Windows.

5. Cliquez sur le bouton **OK**.

Lorsque l'assistant a terminé, les fichiers exécutables associés aux événements du Contrôle des applications sont ajoutés à une catégorie d'applications existante ou à une nouvelle catégorie d'applications. Vous pouvez consulter les paramètres de la catégorie d'applications que vous avez modifiée ou créée.

Pour obtenir des informations détaillées sur le Contrôle des applications, consultez les rubriques d'aide suivantes :

- Aide en ligne de Kaspersky Endpoint Security for Windows
- Aide en ligne de Kaspersky Endpoint Security for Linux

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.

La création des paquets d'installation des applications tierces à partir de la base de données Kaspersky est uniquement disponible sous la licence pour le fonctionnement 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**.
3. Sur la page Assistant de création du paquet d'installation qui s'ouvre, sélectionnez l'option **Sélectionner l'application de la base de Kaspersky pour créer un paquet d'installation**, puis cliquez sur **Suivant**.
4. Dans la liste des applications qui s'ouvre, sélectionnez l'application appropriée, puis cliquez sur **Suivant**.
5. Sélectionnez la version linguistique appropriée dans la liste déroulante, puis cliquez sur **Suivant**.

   Cette étape ne s'affiche que si l'application propose un choix de plusieurs options de langue.

6. Si vous êtes invité à accepter un Contrat de licence dans le cadre de l'installation, sur la page **Contrat de licence utilisateur final** qui s'ouvre, cliquez sur le lien pour lire le Contrat de licence sur le site Web du fournisseur, puis cochez la case **Je confirme que j'ai entièrement lu, que je comprends et que j'accepte les termes et les conditions de ce Contrat de licence utilisateur final**.
7. Sur la page **Nom du nouveau paquet d'installation** qui s'ouvre, dans le champ **Nom de l'archive**, entrez le nom du paquet d'installation, puis cliquez sur **Suivant**.

Attendez que le paquet d'installation nouvellement créé soit chargé sur le Serveur d'administration. Lorsque l'Assistant de création du paquet d'installation affiche le message vous informant que le processus de création de paquet a réussi, cliquez sur **Terminer**.

Le paquet d'installation nouvellement créé s'affiche dans la liste des paquets d'installation. Vous pouvez sélectionner ce paquet lors de la création ou de la reconfiguration de la tâche *Installation à distance d'une application*.

Affichage et modification des paramètres d'un paquet d'installation d'une application tierce à partir de la base de données de Kaspersky

Si vous avez précédemment créé des paquets d'installation d'applications tierces mentionnées dans la base de données de Kaspersky, vous pouvez afficher et modifier les paramètres de ces paquets.

La modification des paramètres d'un paquet d'installation d'une application tierce à partir de la base de données de Kaspersky n'est proposée que sous la licence de Gestion des vulnérabilités et des correctifs.

Pour afficher et modifier les paramètres d'un paquet d'installation d'une application tierce à partir de la base de données de Kaspersky :

1. Dans le menu principal, accédez à **Découverte et déploiement → Déploiement et attribution → Paquets d'installation**.
2. Dans la liste des paquets d'installation qui s'ouvre, cliquez sur le nom du paquet concerné.
3. Sur la page de propriétés qui s'ouvre, modifiez les paramètres, si nécessaire.

4. Cliquez sur le bouton **Enregistrer**.

Les paramètres que vous avez modifiés sont enregistrés.

Paramètres d'un paquet d'installation d'une application tierce à partir de la base de données de Kaspersky

Les paramètres d'un paquet d'installation d'une application tierce sont regroupés dans les onglets suivants :

Seule une partie des paramètres listés ci-dessous est affichée par défaut, vous pouvez donc ajouter les colonnes correspondantes en cliquant sur le bouton **Filtre** et en sélectionnant les noms de colonnes appropriées dans la liste.

- Onglet **Général** :
  - Champ de saisie contenant le nom du paquet d'installation qui peut être modifié manuellement
  - Application

    Le nom de l'application tierce pour laquelle le paquet d'installation est créé.
  - Version

    Le numéro de version de l'application tierce pour laquelle le paquet d'installation est créé.
  - Taille

    La taille du paquet d'installation tiers (en kilo-octets).
  - 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.

- **Révoquée**

  Affiche la date et l'heure de révocation de la mise à jour.

- **État d'approbation de la mise à jour**

  Indique si la mise à jour est approuvée pour l'installation.

- **Révision**

  Affiche le numéro de révision actuel de la mise à jour.

- **Identifiant de mise à jour**

  Affiche l'identifiant de la mise à jour.

- **Version de l'application**

  Affiche le numéro de version vers lequel l'application 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.

- L'ongle **Paramètres** affichant les paramètres des paquets d'installation (avec leurs noms, leurs descriptions et leurs valeurs) utilisés comme paramètres de ligne de commande lors de l'installation. Si le paquet ne fournit pas de tels paramètres, le message correspondant s'affiche. Vous pouvez modifier les valeurs de ces paramètres.

- L'onglet **Historique des révisions** qui affiche les révisions du paquet d'installation et qui contient les colonnes suivantes :

  - **Révision** – le numéro de la révision des paquets d'installation.

  - **Heure** – la date et l'heure de modification des paramètres du paquet d'installation.

  - **Utilisateur** – le nom de l'utilisateur ayant modifié les paramètres du paquet d'installation.

  - **Action** – les actions effectuées sur le paquet d'installation dans la révision.

  - **Description** – la description de la révision de modification des paramètres du paquet d'installation.

    Par défaut, la description de la révision n'est pas remplie. Pour ajouter une description de la révision, choisissez la révision requise, puis cliquez sur le bouton **Modifier la description**. Dans la fenêtre qui s'ouvre, saisissez un texte correspondant à la description de la révision.

Tags de l'application

Kaspersky Security Center Cloud Console vous permet de tagger les applications à partir du registre des applications. Un tag est l'identificateur d'une application qui peut être utilisé pour regrouper ou rechercher des applications. Un tag attribué à des applications peut servir de condition dans les sélections d'appareils.

Par exemple, vous pouvez créer le tag `[Browsers]` et l'affecter à tous les navigateurs (Microsoft Internet Explorer, Google Chrome, Mozilla Firefox, etc.).

Création d'un tag de l'application

Pour créer un tag de l'application, procédez comme suit :

1. Dans le menu principal, accédez à **Opérations → Applications tierces → Tags de l'application**.
2. Cliquez sur **Ajouter**.

   Une fenêtre de nouveau tag s'ouvre.
3. Saisissez le nom du tag.
4. Cliquez sur le bouton **OK** afin d'enregistrer les modifications.

Le nouveau tag apparaît dans la liste des tags de l'application.

Renommage d'un tag de l'application

Pour renommer un tag de l'application, procédez comme suit :

1. Dans le menu principal, accédez à **Opérations → Applications tierces → Tags de l'application**.
2. Cochez la case en regard du tag que vous voulez renommer, puis cliquez sur **Modifier**.

   Une fenêtre de propriété du tag s'ouvre.
3. Modifiez le nom du tag.
4. Cliquez sur le bouton **OK** afin d'enregistrer les modifications.

Le tag mis à jour apparaît dans la liste des tags de l'application.

Attribution de tags à une application

Pour attribuer un ou plusieurs tags à une application, procédez comme suit :

1. Dans le menu principal, accédez à **Opérations → Applications tierces → Registre des applications**.
2. Cliquez sur le nom de l'application à laquelle vous souhaitez attribuer les tags.
3. Sélectionnez l'onglet **Tags**.

   L'onglet affiche tous les tags de l'application qui existent sur le Serveur d'administration. Pour les tags attribués à l'application sélectionnée, la case dans la colonne **Tag défini** est cochée.
4. Pour les tags que vous souhaitez attribuer, cochez les cases dans la colonne **Tag défini**.
5. Cliquez sur le bouton **Enregistrer** afin d'enregistrer les modifications.

Les tags sont attribués à l'application.

Suppression de tags attribués à un appareil

Pour supprimer un ou plusieurs tags d'une application, procédez comme suit :

1. Dans le menu principal, accédez à **Opérations → Applications tierces → Registre des applications**.
2. Cliquez sur le nom de l'application de laquelle vous souhaitez supprimer les tags.
3. Sélectionnez l'onglet **Tags**.

   L'onglet affiche tous les tags de l'application qui existent sur le Serveur d'administration. Pour les tags attribués à l'application sélectionnée, la case dans la colonne **Tag défini** est cochée.
4. Pour les tags que vous souhaitez supprimer, cochez les cases dans la colonne **Tag défini**.
5. Cliquez sur le bouton **Enregistrer** afin d'enregistrer les modifications.

Les tags sont supprimés de l'application.

Les tags de l'application supprimés ne sont pas supprimés. Si vous le voulez, vous pouvez les supprimer manuellement.

Suppression d'un tag de l'application

Pour supprimer un tag de l'application, procédez comme suit :

1. Dans le menu principal, accédez à **Opérations** → **Applications tierces** → **Tags de l'application**.
2. Dans la liste, sélectionnez le tag de l'application que vous souhaitez supprimer.
3. Cliquez sur le bouton **Supprimer**.
4. Dans la fenêtre qui s'ouvre, cliquez sur **OK**.

Le tag de l'application est supprimé. Le tag supprimé est automatiquement retiré de toutes les applications auxquelles il était attribué.

Configuration du Serveur d'administration

Cette section décrit la configuration et les propriétés du Serveur d'administration de Kaspersky Security Center.

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

Vous pouvez désigner un Serveur d'administration, fonctionnant sur site, en tant que Serveur d'administration secondaire et définir en même temps une relation hiérarchique " serveur primaire – serveur secondaire " sur votre réseau. Pour le Serveur d'administration de l'infrastructure Kaspersky, les Serveurs d'administration primaires et secondaires de votre réseau sont des Serveurs secondaires. Vous pouvez ajouter un serveur d'administration Windows ainsi qu'un serveur d'administration Linux.

Pour ajouter un Serveur d'administration secondaire disponible pour la connexion, procédez comme suit :

1. Assurez-vous que Kaspersky Security Center Web Console est installé sur le futur Serveur d'administration secondaire.

2. Sur le futur Serveur d'administration secondaire, téléchargez le certificat du Serveur d'administration et enregistrez-le pour pouvoir l'ajouter au Serveur d'administration principal lors d'une des étapes de l'assistant d'ajout de Serveur d'administration secondaire.

3. Exécutez les actions suivantes via Kaspersky Security Center Web Console sur le futur Serveur d'administration secondaire (vous pouvez également demander à l'administrateur du futur Serveur d'administration secondaire d'exécuter ces actions) :

   a. Dans le menu principal, cliquez sur l'icône des paramètres ( ) en regard du nom du futur Serveur d'administration secondaire.

   b. Sur la page des propriétés qui s'ouvre, accédez à la section **Hiérarchie des Serveurs d'administration** de l'onglet **Général**.

   c. Sélectionnez l'option **Ce Serveur d'administration est secondaire dans la hiérarchie**.

   d. Sélectionnez **Cloud Console** en tant que type du Serveur d'administration principal.

      Les champs des paramètres permettant d'établir une connexion entre les Serveurs d'administration primaires et secondaires sont disponibles.

   e. Dans les champs **Adresse du serveur HDS (à partir du Serveur d'administration principal sur Cloud Console)** et **Ports du serveur HDS**, saisissez l'adresse et le port du Serveur d'administration principal de Kaspersky Security Center Cloud Console.

      Vous pouvez trouver l'adresse du serveur HDS et le port du serveur HDS dans le Serveur d'administration de Kaspersky Security Center Cloud Console, dans la section **Hiérarchie des Serveurs d'administration** de l'onglet **Général** de la fenêtre des propriétés. Vous pouvez copier et coller ces données dans les champs de la fenêtre du Serveur d'administration secondaire.

   f. Cliquez sur le bouton **Indiquer le certificat du Serveur d'administration principal**, puis sélectionnez le certificat.

      Vous pouvez télécharger ce certificat depuis le Serveur d'administration de Kaspersky Security Center Cloud Console, dans la section **Hiérarchie des Serveurs d'administration** de l'onglet **Général** de la fenêtre des propriétés, en cliquant sur le bouton **Afficher le certificat du Serveur d'administration**.

g. Cliquez sur le bouton **Indiquer les certificats du service de découverte hébergé**, puis sélectionnez le certificat.

Vous pouvez télécharger ce certificat depuis le Serveur d'administration de Kaspersky Security Center Cloud Console, dans la section **Hiérarchie des Serveurs d'administration** de l'onglet **Général** de la fenêtre des propriétés, en cliquant sur le bouton **Certificat de l'AC racine HDS**.

h. Si vous utilisez un serveur proxy pour vous connecter au Serveur d'administration de Kaspersky Security Center Cloud Console (c'est-à-dire le Serveur primaire dans la hiérarchie que vous avez créée), spécifiez-le et saisissez les informations d'identification du serveur proxy.

i. Sélectionnez l'option **Connecter le Serveur d'administration principal au Serveur d'administration secondaire dans DMZ** si le Serveur d'administration secondaire se trouve dans une zone démilitarisée.

j. Cliquez sur **Enregistrer** pour enregistrer les modifications et quittez la fenêtre.

4. Dans le menu principal, cliquez sur l'icône des paramètres ( ) en regard du nom du futur Serveur d'administration principal.

5. Sur la page des propriétés qui s'ouvre, cliquez sur l'onglet **Serveurs d'administration**.

6. Cochez la case en regard du nom du groupe d'administration auquel vous souhaitez ajouter le Serveur d'administration secondaire.

7. Sur la ligne de menu, cliquez sur **Connecter un Serveur d'administration secondaire**.

L'Assistant d'ajout de Serveur d'administration secondaire démarre. Parcourez les étapes de l'assistant à l'aide du bouton **Suivant**.

8. Remplissez les champs suivants :

- Nom d'affichage du Serveur d'administration secondaire

  Le nom sous lequel le Serveur d'administration secondaire sera affiché dans la hiérarchie. Si vous le souhaitez, vous pouvez saisir l'adresse IP en tant que nom ou vous pouvez utiliser un nom comme, par exemple, " Serveur secondaire pour le groupe 1 ".

- Adresse du Serveur d'administration secondaire (facultative)

  Spécifiez l'adresse IP ou le nom de domaine du Serveur d'administration secondaire.

  Ce paramètre est obligatoire si l'option **Connecter le Serveur d'administration principal au Serveur d'administration secondaire dans la DMZ** est activée.

9. Si vous utilisez un serveur proxy pour vous connecter au Serveur d'administration de Kaspersky Security Center Cloud Console (c'est-à-dire le futur Serveur primaire), spécifiez-le et saisissez les informations d'identification du serveur proxy.

10. Suivez les autres instructions de l'assistant.

Une fois l'exécution de l'assistant terminée, la hiérarchie " primaire/secondaire " est établie. Le Serveur d'administration principal commence à accepter la connexion du Serveur d'administration secondaire via le port 13000. Les tâches et les stratégies du Serveur d'administration principal sont reçues et appliquées. Le Serveur d'administration secondaire s'affiche sur le Serveur d'administration principal, dans le groupe d'administration auquel il a été ajouté.

Configuration de la durée de stockage des événements concernant les appareils supprimés

Dans Kaspersky Security Center Cloud Console, les événements sont stockés dans un stockage d'événements. Vous ne pouvez pas configurer le nombre d'événements à stocker dans le stockage d'événements.

Dans la section **Stockage d'événements** de la fenêtre de propriétés du Serveur d'administration, vous pouvez configurer la durée maximale de stockage des événements concernant les appareils supprimés. La durée de stockage maximale est de 1000 jours.

Pour configurer le nombre de jours de stockage des événements relatifs aux appareils supprimés :

1. Dans le menu principal, cliquez sur l'icône des paramètres ( ) à côté du Serveur d'administration de Kaspersky Security Center Cloud Console.

   La fenêtre des propriétés du Serveur d'administration s'ouvre.

2. Sous l'onglet **Général**, sélectionnez la section **Stockage d'événements**.

3. Activez l'option **Conserver les événements après la suppression des appareils**.

4. Dans la zone d'édition **Durée maximale de stockage (jours)**, spécifiez le nombre de jours de stockage des événements relatifs aux appareils supprimés.

Le nombre de jours de stockage des événements concernant les appareils supprimés est limité par la valeur spécifiée.

De plus, vous pouvez modifier les paramètres de n'importe quelle tâche pour enregistrer les événements liés à la progression de la tâche ou enregistrer uniquement les résultats de l'exécution de la tâche. Ainsi, vous diminuez le nombre d'événements dans la base de données, vous augmentez la vitesse de fonctionnement des scénarios liés à l'analyse du tableau des événements dans la base de données, et vous réduisez le risque que les événements critiques soient ignorés.

Agrégation de courriels sur les événements

Pendant l'opération, Kaspersky Security Center Cloud Console et les applications administrées de Kaspersky génèrent des événements. Chaque événement est lié à un type défini et à un niveau de gravité (*Critique*, *Erreur de fonctionnement*, *Avertissement*, *Information*). Selon les conditions dans lesquelles un événement s'est produit, Kaspersky Security Center Cloud Console peut affecter différents niveaux de gravité à des événements de même type.

Kaspersky Security Center Cloud Console envoie automatiquement, par email, des notifications sur les événements. Kaspersky Security Center Cloud Console envoie des notifications sur les événements répertoriés dans la fenêtre **Propriétés du Serveur d'administration**, dans l'onglet **Configuration des événements**. Les paramètres de notification courants sont utilisés pour tous les types d'événements.

Pour limiter le nombre d'emails à envoyer, Kaspersky Security Center Cloud Console, agrège les événements ayant le même niveau de gravité pendant des périodes définies. Les valeurs des périodes sont administrées par les spécialistes de Kaspersky. Par conséquent, les destinataires reçoivent des messages électroniques agrégés selon le modèle suivant : " <Number><Severity_level> (et de niveau inférieur) se sont produits ".

Limitations de l'administration des Serveurs d'administration secondaires fonctionnant sur site via Kaspersky Security Center Cloud Console

Après avoir basculé vers un Serveur d'administration secondaire fonctionnant sur site à l'aide de l'option correspondante dans Kaspersky Security Center Cloud Console, l'application impose des limitations spécifiques à l'administration de ce Serveur d'administration secondaire. Les paramètres suivants liés au fonctionnement de Kaspersky Security Center Cloud Console ne sont plus disponibles pour l'utilisateur :

- Dans les paramètres des stratégies de l'Agent d'administration et des stratégies du Serveur d'administration, les onglets **Configuration des événements** et **Paramètres de l'application** ne sont pas disponibles ; aucune nouvelle stratégie ne peut être créée.
- Dans les paramètres des tâches de l'Agent d'administration et des tâches du Serveur d'administration, les onglets **Configuration des événements** et **Paramètres de l'application** ne sont pas disponibles ; aucune nouvelle tâche ne peut être créée.
- L'administration de l'Agent d'administration et du Serveur d'administration n'est pas disponible, ainsi que la fenêtre des propriétés du Serveur d'administration secondaire.
- L'Assistant de démarrage rapide de l'application n'est pas disponible.
- Les paramètres de stockage et de notification des événements de l'Agent d'administration et du Serveur d'administration ne peuvent pas être modifiés.
- La section **Versions actuelles des applications** n'est pas disponible.
- La section **Paquets d'installation** n'est pas disponible.

Affichage de la liste des Serveurs d'administration secondaires

Pour afficher la liste des Serveurs d'administration secondaires (virtuels inclus) :

Dans le menu principal, cliquez sur le nom du Serveur d'administration, qui est à côté de l'icône des paramètres ( ).

La liste déroulante des Serveurs d'administration secondaires (virtuels inclus) s'affiche.

Vous pouvez aller à l'un de ces serveur d'administration en cliquant sur son nom.

Suppression d'une hiérarchie des Serveurs d'administration

Si vous ne souhaitez plus disposer d'une hiérarchie de Serveurs d'administration, vous pouvez les déconnecter de cette hiérarchie.

Pour supprimer une hiérarchie de Serveurs d'administration :

1. Dans le menu principal, cliquez sur l'icône des paramètres ( ) en regard du nom du Serveur d'administration principal.
2. Sur la page qui s'ouvre, accédez à l'onglet **Serveurs d'administration**.
3. Dans le groupe d'administration où vous voulez supprimer le Serveur d'administration secondaire, sélectionnez le Serveur d'administration secondaire.
4. Dans la ligne du menu, cliquez sur **Supprimer ;**.
5. Dans la fenêtre qui s'ouvre, cliquez sur **OK** pour confirmer que vous voulez supprimer le Serveur d'administration secondaire.

L'ancien Serveur d'administration principal et l'ancien Serveur d'administration secondaire sont désormais indépendants l'un de l'autre. La hiérarchie n'existe plus.

Configuration de l'interface

Vous pouvez configurer l'interface de Kaspersky Security Center Cloud 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 Cloud Console conformément à l'ensemble de fonctionnalités actuellement utilisé, procédez comme suit :

1. Dans le menu principal, allez dans les paramètres de votre compte et puis sélectionnez **Options d'interface**.
2. Dans la fenêtre **Options d'interface** qui s'ouvre, activez ou désactivez les options :
   - Afficher le chiffrement et la protection des données

     Vous pouvez utiliser cette option pour masquer ou afficher la section **Opérations → Chiffrement et protection des données** dans l'interface. Kaspersky Security Center Cloud Console enregistre la valeur de cette option uniquement pour votre propre compte utilisateur, tandis que l'autre utilisateur peut définir une valeur différente.

   - Afficher les fonctionnalités MDR

     Vous pouvez utiliser cette option pour masquer ou afficher la section **Surveillance et rapports → Incidents** dans l'interface. Kaspersky Security Center Cloud Console enregistre la valeur de cette option uniquement pour votre propre compte utilisateur, tandis que l'autre utilisateur peut définir une valeur différente.
3. Définissez le nombre d'appareils que Kaspersky Security Center Cloud Console affiche dans les résultats de la distribution des stratégies.
4. Cliquez sur **Enregistrer**.

Les paramètres de l'interface de la console sont configurés en fonction de vos préférences.

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.

Pour créer et ajouter un Serveur d'administration virtuel, procédez comme suit :

1. Dans le menu principal, cliquez sur l'icône des paramètres ( ) en regard du nom du Serveur d'administration requis.
2. Sur la page qui s'ouvre, accédez à l'onglet **Serveurs d'administration**.
3. Choisissez le groupe d'administration auquel vous souhaitez ajouter un Serveur d'administration virtuel.
4. Dans la ligne du menu, cliquez sur **Nouveau Serveur d'administration virtuel**.
5. Sur la page qui s'ouvre, définissez **Nom du Serveur d'administration virtuel**.
6. Cliquez sur **Enregistrer**.

Le nouveau Serveur d'administration virtuel est créé, ajouté au groupe d'administration et s'affiche sous l'onglet **Serveurs d'administration**.

Activation et désactivation d'un Serveur d'administration virtuel

Lorsque vous créez un nouveau Serveur d'administration virtuel, il est activé par défaut. Vous pouvez le désactiver ou le réactiver à tout moment. Désactiver ou activer un Serveur d'administration virtuel revient à éteindre ou allumer un Serveur d'administration physique.

Pour activer ou désactiver un Serveur d'administration virtuel :

1. Dans le menu principal, cliquez sur l'icône des paramètres ( ) en regard du nom du Serveur d'administration requis.
2. Sur la page qui s'ouvre, accédez à l'onglet **Serveurs d'administration**.
3. Sélectionnez le Serveur d'administration virtuel que vous souhaitez activer ou désactiver.
4. Sur la ligne du menu, cliquez sur le bouton **Activer / désactiver le Serveur d'administration virtuel**.

L'état du Serveur d'administration virtuel passe à activé ou désactivé en fonction de son état précédent. L'état mis à jour est affiché à côté du nom du Serveur d'administration.

Désignation d'un administrateur pour un Serveur d'administration virtuel

Lorsque vous utilisez des Serveurs d'administration virtuels dans votre organisation, vous souhaiterez peut-être désigner un administrateur dédié pour chaque Serveur d'administration virtuel. Par exemple, cela peut être utile lorsque vous créez des Serveurs d'administration virtuels pour administrer des bureaux ou des services distincts de votre organisation, ou si vous êtes un fournisseur MSP et que vous administrez vos locataires 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 affecter un administrateur à un Serveur d'administration virtuel uniquement, assurez-vous que l'administrateur ne figure pas dans la liste **Privilèges d'accès** dans les propriétés du Serveur d'administration principal.

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

Lorsque vous désignez un administrateur, assurez-vous que vous accordez l'accès à un seul Serveur d'administration virtuel. Un administrateur ayant accès à plusieurs Serveurs d'administration virtuels ne peut pas se connecter à Kaspersky Security Center Cloud Console.

L'administrateur d'un Serveur d'administration virtuel se connecte à Kaspersky Security Center Cloud Console de la même manière qu'il se connecte au Serveur d'administration principal. Kaspersky Security Center Cloud 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 principal, vous avez créé un compte utilisateur pour l'administrateur que vous souhaitez affecter au Serveur d'administration virtuel.
- Le compte créé par l'administrateur du Serveur virtuel ne figure pas dans les listes **Privilèges d'accès** des propriétés des Serveurs, qu'ils soient primaires ou secondaires.
- 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. Dans le menu principal, basculez vers le Serveur d'administration virtuel requis :

   a. Cliquez sur l'icône en forme de chevron (›) à droite du nom actuel du Serveur d'administration.

   b. Sélectionnez le Serveur d'administration requis.

2. Dans le menu principal, cliquez sur l'icône des paramètres ( ) à côté du nom du Serveur d'administration.

   La fenêtre des propriétés du Serveur d'administration s'ouvre.

3. Sous l'onglet **Privilèges d'accès**, cliquez sur le bouton **Ajouter**.

   Une liste unifiée des utilisateurs du Serveur d'administration principal et du Serveur d'administration virtuel actuel s'ouvre.

4. Dans la liste des utilisateurs, sélectionnez le compte utilisateur de l'administrateur que vous souhaitez affecter au Serveur d'administration virtuel, puis cliquez sur le bouton **OK**.

   L'application ajoute l'utilisateur sélectionné à la liste des utilisateurs sous l'onglet **Privilèges d'accès**.

5. Cochez la case en regard du nom du compte ajouté, puis cliquez sur le bouton **Privilèges d'accès**.

6. Configurez les privilèges de l'administrateur sur le Serveur d'administration virtuel.

   Pour que l'authentification réussisse, l'administrateur doit disposer au minimum des privilèges suivants :

   - Accorde les droits de **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. Dans le menu principal, basculez vers le Serveur d'administration virtuel requis :

   a. Cliquez sur l'icône en forme de chevron (›) à droite du nom actuel du Serveur d'administration.

   b. Sélectionnez le Serveur d'administration requis.

3. Attribuez le nouveau rôle ou plusieurs rôles au compte administrateur.

Lors de l'attribution de rôles à un utilisateur, dans le menu principal, accédez à **Utilisateurs et rôles** → **Utilisateurs et groupes**, puis sélectionnez l'onglet **Utilisateurs**. Si vous sélectionnez l'onglet **Groupes**, puis que vous attribuez des rôles au groupe dont l'utilisateur est membre, l'utilisateur ne pourra pas se connecter à Kaspersky Security Center Cloud Console.

L'application attribue le nouveau rôle 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.

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 Cloud Console, exécutez l'interrogation du réseau, puis déplacez les appareils trouvés du groupe Appareils non définis vers les groupes d'administration.

Pour supprimer un Serveur d'administration virtuel :

1. Dans le menu principal, cliquez sur l'icône des paramètres ( ) à côté du nom du Serveur d'administration.
2. Sur la page qui s'ouvre, accédez à l'onglet **Serveurs d'administration**.
3. Sélectionnez le Serveur d'administration virtuel que vous souhaitez supprimer.
4. Dans la ligne du menu, cliquez sur le bouton **Supprimer ;**.

Le Serveur d'administration virtuel est supprimé.

Surveillance et rapports

Cette section décrit les capacités de surveillance et de rapports de Kaspersky Security Center Cloud Console. Ces capacités offrent un aperçu de votre infrastructure, des états de la protection et des statistiques.

Une fois Kaspersky Security Center Cloud Console 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 Cloud Console.

Prérequis

Une fois que vous avez déployé Kaspersky Security Center Cloud Console sur le réseau d'une entreprise, vous pouvez commencer à le surveiller et obtenir des rapports opérationnels.

Étapes

La configuration de la surveillance et des rapports sur le réseau d'une organisation se déroule 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 d'importance 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 pratiques : Configuration des notifications (par email) sur les événements survenus sur les appareils clients

3. **Modification de la réaction de votre réseau de sécurité à l'événement Propagation de virus**

   Vous pouvez configurer les seuils spécifiques dans les propriétés du Serveur d'administration. Vous pouvez également créer une stratégie plus stricte qui sera activée ou créer une tâche qui sera exécutée quand l'événement se produira.

4. **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 contrôler la sélection d'événements **Critique**

7. **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 sur un réseau d'organisation sont conservées dans la base de données du Serveur d'administration. Sur la base des événements, Kaspersky Security Center Cloud 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

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 Cloud Console pour configuration.

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 Cloud Console, dans la section **Surveillance et rapports**, en cliquant sur **Tableau de bord**.

Le tableau de bord fournit des widgets qui peuvent être personnalisés. Vous pouvez choisir parmi une grande quantité de widgets différents, sous la forme de diagrammes circulaires, tableaux, graphiques, diagrammes en barre et listes. Les informations affichées dans les widgets sont automatiquement mises à jour, la période de mise à jour est d'une à deux minutes. L'intervalle entre les mises à jour varie selon les différents widgets. Vous pouvez actualiser les données sur un widget manuellement à tout moment à l'aide du menu de paramètres.

Par défaut, les widgets incluent des informations sur tous les événements stockés dans la base de données du Serveur d'administration.

Kaspersky Security Center Cloud 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 visualiser le détail des informations en cliquant sur un lien.

Lors de la configuration du tableau de bord, vous pouvez ajouter les widgets dont vous avez besoin, masquer les widgets dont vous n'avez pas besoin, changer la taille ou l'apparence des widgets, déplacer des widgets, et modifier leurs paramètres.

Ajout de widgets au tableau de bord

Pour ajouter des widgets au tableau de bord :

1. Dans le menu principal, accédez à **Surveillance et rapports** → **Tableau de bord**.
2. Cliquez sur le bouton **Ajouter ou restaurer un widget web**.
3. Sélectionnez dans la liste des widgets disponibles ceux que vous souhaitez ajouter au tableau de bord.

   Les widgets sont organisés en catégories. Pour voir la liste des widgets inclus dans une catégorie, cliquez sur l'icône en chevron (›) en regard du nom de la catégorie.
4. Cliquez sur le bouton **Ajouter**.

Les widgets sélectionnés sont ajoutés à la fin du tableau de bord.

Vous pouvez alors modifier la représentation et les paramètres des widgets ajoutés.

Dissimulation d'un widget dans le tableau de bord

Pour masquer un widget affiché sur le tableau de bord :

1. Dans le menu principal, accédez à **Surveillance et rapports** → **Tableau de bord**.
2. Cliquez sur l'icône des paramètres (⚙) en regard du widget que vous souhaitez masquer.
3. Sélectionnez **Masquer le widget web**.
4. Dans la fenêtre **Avertissement** qui s'ouvre, cliquez sur **OK**.

Le widget sélectionné est masqué. Plus tard, vous pourrez à nouveau ajouter ce widget au tableau de bord.

Déplacement d'un widget sur le tableau de bord

Pour déplacer un widget sur le tableau de bord, procédez comme suit :

1. Dans le menu principal, accédez à **Surveillance et rapports** → **Tableau de bord**.
2. Cliquez sur l'icône des paramètres (⚙) en regard du widget que vous souhaitez déplacer.

3. Sélectionnez **Déplacer**.

4. Cliquez sur l'endroit vers lequel vous souhaitez déplacer le widget. Vous pouvez sélectionner uniquement un autre widget.

Les widgets sélectionnés permutent de position.

Modification de la taille et de l'apparence du widget

S'agissant des widgets qui affichent un diagramme, vous pouvez modifier la représentation : barres ou lignes. Certains widgets acceptent une modification de la taille : compact, moyen ou maximal.

Pour modifier la représentation d'un widget, procédez comme suit :

1. Dans le menu principal, accédez à **Surveillance et rapports → Tableau de bord**.

2. Cliquez sur l'icône des paramètres (⚙) en regard du widget que vous souhaitez modifier.

3. Exécutez une des actions suivantes :

   - Pour afficher le widget en tant que graphique à barres, sélectionnez **Type de graphique : barres**.
   - Pour afficher le widget en tant que graphique à lignes, sélectionnez **Type de graphique : courbes**.
   - Pour modifier la zone occupée par le widget, sélectionnez l'une des valeurs suivantes :
     - **Compact**
     - **Compact (barre seulement)**
     - **Moyen (graphique en anneau)**
     - **Moyen (graphique à barres)**
     - **Maximal**

La représentation du widget sélectionné change.

Modification des réglages d'un widget

Pour modifier les réglages d'un widget :

1. Dans le menu principal, accédez à **Surveillance et rapports → Tableau de bord**.

2. Cliquez sur l'icône des paramètres (⚙) en regard du widget que vous souhaitez modifier.

3. Sélectionnez **Afficher les paramètres**.

4. Dans la fenêtre des paramètres du widget qui s'ouvre, modifiez les paramètres du widget selon vos besoins.

5. Cliquez sur le bouton **Enregistrer** afin d'enregistrer les modifications.

Les paramètres du widget sélectionnés sont modifiés.

L'ensemble de paramètres dépend de chaque widget. Ci-dessous figurent quelques paramètres habituels :

- **Portée du widget web** (l'ensemble d'objets pour lesquels le widget affiche des informations) : par exemple, un groupe d'administration ou une sélection d'appareils.
- **Sélectionnez une tâche** (la tâche pour laquelle le widget affiche des informations).
- **Période** (la période pendant laquelle les informations sont affichées dans le widget) : entre deux dates définies ; depuis une date définie jusqu'au jour actuel ; jusqu'à un nombre de jours défini avant le jour actuel.
- **Définir l'état comme "Critique" si** et **Définir l'état comme "Avertissement" si** (les règles qui déterminent la couleur d'un indicateur de couleur).

Après avoir modifié les paramètres du widget, vous pouvez mettre à jour manuellement les données sur le widget.

Pour mettre à jour les données d'un widget, procédez comme suit :

1. Dans le menu principal, accédez à **Surveillance et rapports → Tableau de bord**.
2. Cliquez sur l'icône des paramètres (⚙) en regard du widget que vous souhaitez déplacer.
3. Sélectionnez **Actualiser**.

Les données du widget sont à jour.

À propos le mode Tableau de bord uniquement

Vous pouvez configurer le mode Tableau de bord uniquement pour les employés qui ne gèrent pas le réseau mais qui souhaitent consulter les statistiques de protection du réseau dans Kaspersky Security Center Cloud Console (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 uniquement, 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 primaire ou d'un serveur secondaire physique. Il n'est pas possible de régler le mode sur un serveur virtuel.

Pour configurer le mode Tableau de bord uniquement :

1. Dans le menu principal, accédez à **Utilisateurs et rôles → Utilisateurs et groupes**, puis sélectionnez l'onglet **Utilisateurs**.
2. Cliquez sur le nom du compte utilisateur dont vous souhaitez ajuster le tableau de bord avec des widgets.
3. Dans la fenêtre des paramètres du compte qui s'ouvre, cliquez sur l'onglet **Tableau de bord**.

   Sur l'onglet qui s'ouvre, le même tableau de bord s'affiche pour vous et pour l'utilisateur.
4. Si l'option **Afficher la console en mode Tableau de bord uniquement** est activée, basculez le bouton bascule pour la désactiver.

   Lorsque cette option est activée, vous ne pouvez pas non plus modifier le tableau de bord. Après avoir désactivé l'option, vous pouvez gérer les widgets.
5. Configurez l'apparence du tableau de bord. L'ensemble des widgets préparés sur l'onglet **Tableau de bord** est disponible pour l'utilisateur avec le compte personnalisable. Il ou elle ne peut pas modifier les paramètres ou la taille des widgets, ajouter ou supprimer des widgets du tableau de bord. Par conséquent, ajustez-les pour l'utilisateur afin qu'il puisse consulter les statistiques de protection du réseau. Pour cela, dans l'onglet **Tableau de bord**, vous pouvez réaliser les mêmes actions avec les widgets que dans la section **Surveillance et rapports → Tableau de bord** :
   - Ajoutez des nouveaux widgets au tableau de bord.
   - Cachez les widgets dont l'utilisateur n'a pas besoin.
   - Déplacez les widgets dans un ordre spécifique.
   - Modifiez la taille ou l'apparence des widgets.
   - Modifiez les paramètres du widget.
6. Basculez le bouton à bascule pour activer l'option **Afficher la console en mode Tableau de bord uniquement**.

   Après cela, seul le tableau de bord est disponible pour l'utilisateur. Il peut surveiller les statistiques mais ne peut pas modifier les paramètres de protection du réseau ni l'apparence du tableau de bord. Comme le même tableau de bord s'affiche pour vous et pour l'utilisateur, vous ne pouvez pas non plus modifier le tableau de bord.

Si vous laissez l'option désactivée, le menu principal s'affiche pour l'utilisateur afin qu'il puisse effectuer diverses actions dans Kaspersky Security Center Cloud Console, 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 Cloud Console sous le compte personnalisé et suivre les statistiques de protection du réseau en mode Tableau de bord uniquement.

Rapports

Cette section décrit comment utiliser les rapports, gérer les modèles de rapport personnalisés, utiliser les modèles de rapport pour générer de nouveaux rapports et créer des tâches de remise de rapports.

Utilisation des rapports

Les rapports permettent d'obtenir des informations numériques détaillées sur la sécurité du réseau de votre organisation, d'enregistrer ces informations dans un fichier, de les envoyer par email et les imprimer.

Les rapports sont disponibles dans Kaspersky Security Center Cloud Console, dans la section **Surveillance et rapports**, en cliquant sur **Rapports**.

Par défaut, les rapports incluent des informations sur les 30 derniers jours.

Kaspersky Security Center Cloud Console contient un ensemble de rapports par défaut pour 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.

Créer le nouveau rapport

Pour créer un modèle de rapport, procédez comme suit :

1. Dans le menu principal, accédez à **Surveillance et rapports** → **Rapports**.

2. Cliquez sur **Ajouter**.

   Finalement, l'assistant de création du modèle du rapport se lancera. Parcourez les étapes de l'assistant à l'aide du bouton **Suivant**.

3. Saisissez le nom du rapport, puis sélectionnez le type de rapport.

4. À l'étape **Zone 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.

5. À l'étape **Période du rapport** de l'assistant, définissez la période du rapport. Les valeurs disponibles sont les suivantes :

   - Entre deux dates définies
   - Depuis la date définie jusqu'à la date de création du rapport
   - Depuis la date de création du rapport moins le nombre de jours indiqué avant la date de création du rapport

   Cette page peut ne pas apparaître avec certains rapports.

6. Cliquez sur le bouton **OK** pour quitter l'Assistant.

7. Exécutez une des actions suivantes :

   - Cliquez sur le bouton **Enregistrer et exécuter** pour enregistrer le nouveau modèle de rapport et pour exécuter un rapport créé sur la base de ce modèle.

     Le modèle de rapport est enregistré. Le rapport est créé.

   - Cliquez sur le bouton **Enregistrer** pour enregistrer le nouveau modèle de rapport.

     Le modèle de rapport est enregistré.

Ce nouveau modèle peut être utilisé pour créer et afficher des rapports.

Consultation et modification des propriétés du modèle de rapport

Vous pouvez consulter et modifier les propriétés de base d'un modèle de rapport par exemple, le nom du modèle de rapport ou les champs affichés dans le rapport.

Pour consulter et modifier les propriétés d'un modèle de rapport :

1. Dans le menu principal, accédez à **Surveillance et rapports** → **Rapports**.

2. Cochez la case en regard du modèle de rapport dont vous souhaitez consulter et modifier les propriétés.

   Vous pouvez également d'abord créé le rapport, puis cliquer sur le bouton **Modifier**.

3. Cliquez sur le bouton **Ouvrir les propriétés du modèle de rapport**.

   La fenêtre **Édition du rapport <nom du rapport>** s'ouvre à l'onglet **Général**.

4. Modifiez les propriétés du modèle de rapport.

- Onglet **Général** :
  - Nom du modèle de rapport
  - **Nombre maximal d'entrées affichées**

    Quand cette option est activée, le nombre d'entrées affichées dans le tableau contenant les données détaillées du rapport ne peut être supérieur à la valeur indiquée. Notez que cette option n'affecte pas le nombre maximal d'événements que vous pouvez inclure dans le rapport lorsque vous exportez le rapport dans un fichier.

    Les entrées du rapport sont tout d'abord classées en fonction des règles définies dans la section **Champs → Champs d'informations** des propriétés des modèles de rapport, puis seule la première des entrées obtenues est conservée. L'en-tête du tableau contenant les données détaillées du rapport reprend le nombre d'entrées affichées et le nombre total d'entrées disponible qui correspondent aux autres paramètres du modèle de rapport.

    Quand cette option est désactivée, le tableau contenant les données détaillées du rapport affiche toutes les entrées disponibles. Nous déconseillons de désactiver cette option. La restriction du nombre d'entrées affichées dans le rapport réduit la charge sur le système de gestion de base de données (SGBD) et réduit le temps requis pour la création et l'exportation du rapport. Certains rapports contiennent trop d'entrées. Dans ce cas, il peut être difficile de les lire et de les analyser tous. Aussi, votre appareil pourrait épuiser sa mémoire lors de la création de ces rapports et vous empêcher de les visualiser.

    Cette option est activée par défaut. La valeur par défaut est de 1000.

    Notez que l'interface de Kaspersky Security Center Cloud Console peut afficher un maximum de 2 500 entrées. Si vous avez besoin d'afficher un nombre d'événements supérieur, utilisez la fonctionnalité rapport d'exportation.

  - **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. Les valeurs disponibles sont les suivantes :

    - Entre deux dates définies
    - Depuis la date définie jusqu'à la date de création du rapport
    - Depuis la date de création du rapport moins le nombre de jours indiqué avant la date de création du rapport

  - **Inclure les données 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 à intervalles réguliers des données au Serveur d'administration pour lequel le rapport est créé. Vous pouvez spécifier cette période en heures. Une valeur égale à 0 signifie que les données sont transférées uniquement lorsque le rapport est créé.

  La valeur par défaut est de 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 qui seront affichés dans le rapport, et utilisez les boutons **Haut** et **Bas** pour changer l'ordre des champs. Cliquez sur le bouton **Ajouter** ou **Modifier** pour indiquer si les informations du rapport doivent être triées et filtrées selon chaque filtre.

  Dans la section **Filtres des champs Détails**, vous pouvez également cliquer sur le bouton **Convertir les filtres** pour commencer à utiliser le format de filtrage étendu. Ce format vous permet de combiner les conditions de filtrage précisées dans divers champs à l'aide de l'opération logique OU. Après avoir cliqué sur le bouton, le panneau **Convertir les filtres** s'ouvre sur la droite. Cliquez sur le bouton **Convertir les filtres** pour confirmer la conversion. Vous pouvez maintenant définir un filtre converti avec les conditions de la section **Champs d'informations** appliquées à l'aide de l'opération logique OU.

  > La conversion d'un rapport au format prenant en charge des conditions de filtrage complexes le rendra incompatible avec les versions précédentes de Kaspersky Security Center (11 et antérieures). De plus, le rapport converti ne contiendra aucune donnée des Serveurs d'administration secondaires exécutant ces versions incompatibles.

5. Cliquez sur le bouton **Enregistrer** afin d'enregistrer les modifications.
6. Fermez la fenêtre **Modification du rapport <Nom du rapport>**.

Le modèle de rapport mis à jour apparaît dans la liste des modèles de rapport.

Exportation d'un rapport dans un fichier

Vous pouvez enregistrer un ou plusieurs rapports au format XML, HTML ou PDF. Kaspersky Security Center Cloud Console vous permet d'exporter simultanément jusqu'à 10 rapports vers des fichiers du format spécifié.

Pour exporter un rapport dans un fichier, procédez comme suit :

1. Dans le menu principal, accédez à **Surveillance et rapports** → **Rapports**.
2. Choisissez les rapports que vous souhaitez exporter.

   Si vous choisissez plus de 10 rapports, le bouton **Rapport d'exportation** sera désactivé.
3. Cliquez sur le bouton **Rapport d'exportation**.
4. Dans la fenêtre ouverte, indiquez les paramètres d'exportation 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.

   - **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.

5. Cliquez sur le bouton **Rapport d'exportation**.

Le rapport est enregistré dans un fichier au format indiqué.

Génération et affichage d'un rapport

Pour former et consulter le rapport, procédez comme suit :

1. Dans le menu principal, accédez à **Surveillance et rapports → Rapports**.
2. Cliquez sur le nom du modèle de rapport que vous souhaitez utiliser pour créer un rapport.

   Un rapport utilisant le modèle sélectionné s'affiche.

Les données du rapport s'affichent uniquement en anglais, les autres localisations ne sont pas disponibles.

Le rapport affiche les données suivantes :

- Sous l'onglet **Récapitulatif** :
  - Le type et le nom du rapport, une brève description et la période couverte, ainsi que les informations sur la création d'un rapport créée pour un groupe d'appareils.
  - Graphique présentant les données les plus représentatives du rapport.
  - Tableau récapitulatif avec les indices énumérés du rapport.
- Dans l'onglet **En savoir plus**, un tableau contenant les données de rapport détaillées.

Création d'une tâche d'envoi du rapport

Vous pouvez créer une tâche qui enverra les rapports sélectionnés.

Pour créer une tâche de diffusion des rapports, procédez comme suit :

1. Dans le menu principal, accédez à **Surveillance et rapports → Rapports**.
2. Cochez les cases en regard des modèles de rapport pour lequel vous souhaitez créer une tâche de diffusion des rapports.
3. Cliquez sur le bouton **Créer une tâche d'envoi**.

   Ceci permet de lancer l'assistant de création d'une tâche. Parcourez les étapes de l'assistant à l'aide du bouton **Suivant**.
4. À l'étape **Paramètres de nouvelle tâche** de l'Assistant, saisissez le nom de la tâche.

   Le nom par défaut est **Envoi de rapports**. Si une tâche portant ce nom existe déjà, un numéro d'ordre (<N>) est ajouté au nom de la tâche.

5. À l'étape de **Configuration du rapport** de l'Assistant, configurez les paramètres suivants :

   a. Modèles de rapports que la tâche doit diffuser.

   b. Le format du rapport est HTML, XLS ou PDF.

      L'outil wkhtmltopdf est requis pour convertir un rapport au format PDF. Lorsque vous sélectionnez l'option PDF, le Serveur d'administration vérifie si l'outil wkhtmltopdf est installé sur l'appareil. Si l'outil n'est pas installé, l'application affiche un message indiquant la nécessité d'installer l'outil sur l'appareil du Serveur d'administration. Installez l'outil manuellement, puis passez à l'étape suivante.

   c. Si les rapports doivent être envoyés par email avec les paramètres d'envoi par email.

      Vous pouvez définir jusqu'à 20 adresses email. Pour séparer les adresses email, appuyez sur la touche **Entrée**. Vous pouvez également coller une liste d'adresses email séparées par une virgule, puis appuyer sur la touche **Entrée**.

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 lundi à l'heure système actuelle.

   - Chaque mois

La tâche s'exécute régulièrement le jour du mois défini, à l'heure indiquée.

Si le jour en question ne figure pas dans le mois, la tâche s'exécute le dernier jour.

La tâche s'exécute par défaut le premier jour de chaque mois, à l'heure système actuelle.

- Aux jours indiqués

  La tâche s'exécute régulièrement les jours du mois définis, à l'heure indiquée.

  Par défaut, aucun jour du mois n'est sélectionné. L'heure de début par défaut est 18:00.

- Lors de la détection d'une 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. Ce paramètre ne fonctionne que si les deux tâches sont affectées aux mêmes appareils. Par exemple, vous pouvez exécuter la tâche *Administration des appareils* avec l'option **&Activer l'appareil** et, une fois celle-ci terminée, exécuter la tâche de *recherche de virus* comme tâche de déclenchement.

  Il faut sélectionner la tâche de déclenchement dans le tableau et l'état avec lequel cette tâche doit se terminer (**Terminée avec succès** ou **Échec**).

  Si nécessaire, vous pouvez rechercher, trier et filtrer les tâches dans le tableau comme suit :

  - Saisissez le nom de la tâche dans le champ de recherche pour rechercher une tâche par son nom.
  - Cliquez sur l'icône de tri pour trier les tâches par nom.

    Par défaut, les tâches sont triées par ordre alphabétique croissant.
  - Cliquez sur l'icône du filtre, et dans la fenêtre qui s'ouvre, filtrez les tâches par groupe, puis cliquez sur le bouton **Appliquer**.

7. À cette étape de l'Assistant, configurez d'autres paramètres de planification de tâches :

   - Dans la section **Calendrier de la tâche**, vérifiez ou reconfigurez la planification précédemment sélectionnée, puis définissez l'intervalle de temps, les jours du mois ou de la semaine, la condition de propagation de virus ou la fin d'une autre tâche comme déclencheur du lancement de celle-ci. Une heure de début peut également être définie dans cette section si la planification applicable est sélectionnée.

- Dans la section **Paramètres supplémentaires**, définissez les paramètres suivants :
  - Lancer les tâches non exécutées

    Cette option détermine le comportement d'une tâche si un appareil client n'est pas visible sur le réseau quand la tâche est sur le point de démarrer.

    Si la case est Activé, lors du lancement suivant de l'application de Kaspersky sur cet appareil client, une tentative de lancement de la tâche sera faite. Si la programmation de la tâche est **Manuel**, **Une fois** ou **Immédiatement**, la tâche est immédiatement lancée dès que l'appareil apparaît sur le réseau ou immédiatement après l'inclusion de l'appareil dans la zone d'action de la tâche.

    Si cette option est désactivée, seules les tâches planifiées s'exécutent sur les appareils clients. Pour les planifications **Manuel**, **Une fois** et **Immédiatement**, les tâches s'exécutent uniquement sur les appareils clients qui sont visibles sur le réseau. Par exemple, vous pouvez désactiver cette option pour une tâche qui consomme des ressources que vous voulez exécuter uniquement en dehors des heures de bureau.

    Cette option est Inactif par défaut.

  - Adopter un décalage aléatoire automatique pour les lancements de tâche

    Si cette option est activée, la tâche est lancée sur les appareils clients de manière aléatoire au cours d'un intervalle défini. C'est ce qu'on appelle un *lancement échelonné d'une tâche*. Un lancement échelonné de tâche permet d'éviter la communication simultanée d'un nombre important d'appareils clients avec le Serveur d'administration lors du lancement de la tâche programmée.

    Le temps du lancement aléatoire est automatiquement calculée lors de la création d'une tâche selon le nombre d'appareils clients sur lesquels la tâche est diffusée. Par la suite, la tâche démarre toujours à l'heure de lancement calculée. Toutefois, quand les paramètres de la tâche sont modifiés ou si la tâche est lancée manuellement, la valeur calculée de l'heure de lancement de la tâche est modifiée.

    Si la case n'est pas cochée, le lancement de la tâche sur les appareils clients s'opère selon la planification.

  - Décaler aléatoirement et automatiquement le lancement de la tâche dans un intervalle de

    Si cette option est activée, la tâche est lancée sur les appareils clients de manière aléatoire au cours de l'intervalle défini. Un lancement échelonné de tâche permet d'éviter la communication simultanée d'un nombre important d'appareils clients avec le Serveur d'administration lors du lancement de la tâche programmée.

    Si la case n'est pas cochée, le lancement de la tâche sur les appareils clients s'opère selon la planification.

    Cette option est Inactif par défaut. Par défaut, la valeur de cet intervalle est de une minute.

  - Arrêter la tâche si elle prend plus de

    A l'issue du délai défini, la tâche s'arrête automatiquement, qu'elle soit finie ou non.

    Activez cette option si vous souhaitez interrompre (ou arrêter) les tâches dont l'exécution dure trop longtemps.

    Cette option est Inactif par défaut. La durée d'exécution de la tâche par défaut est de 120 minutes.

8. À l'étape **Sélection du compte utilisateur pour exécuter la tâche** de l'Assistant, indiquez les identifiants du compte utilisateur qui sera utilisé pour exécuter la tâche.

9. Si vous souhaitez modifier un autre paramètre de la tâche une fois que la tâche est créée, à l'étape **Fin de la création de la tâche** de l'Assistant, activez l'option **Ouvrir les détails de la tâche à la fin de la création** (cette option est activée par défaut).

10. Cliquez sur le bouton **Terminer** pour créer la tâche et fermer l'Assistant.

    La tâche de remise de rapports est créée. Si l'option **Ouvrir les détails de la tâche à la fin de la création** est activée, la fenêtre des paramètres de la tâche s'ouvre.

Suppression des modèles de rapport

Pour supprimer un ou plusieurs modèles de rapport, procédez comme suit :

1. Dans le menu principal, accédez à **Surveillance et rapports → Rapports**.
2. Cochez les cases en regard des modèles de rapport que vous souhaitez supprimer.
3. Cliquez sur le bouton **Supprimer**.
4. Dans la fenêtre qui s'ouvre, cliquez **OK** pour confirmer votre choix.

Les modèles de rapport sélectionnés sont supprimés. Si ces modèles de rapport ont été inclus dans les tâches de diffusion des rapports, ils sont également retirés des tâches.

Événements et sélections d'événements

Cette section fournit des informations sur les événements et les sélections d'événements, sur les types d'événements qui se produisent dans les modules de Kaspersky Security Center Cloud Console et sur la gestion du blocage d'événements fréquents.

À propos des événements dans Kaspersky Security Center Cloud Console

Kaspersky Security Center Cloud Console vous permet d'obtenir des informations sur les événements survenus pendant le fonctionnement du Serveur d'administration et des applications Kaspersky installées sur les appareils administrés. Les informations relatives aux événements sont conservées dans la base de données du Serveur d'administration. Vous pouvez exporter ces informations dans des systèmes SIEM externes. L'exportation des informations relatives aux événements vers des systèmes SIEM externes permet à l'administrateur des systèmes SIEM de réagir efficacement aux événements du système de sécurité survenus sur les appareils administrés ou dans les groupes d'appareils.

Événements par type

Dans Kaspersky Security Center Cloud Console, 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 Cloud Console :
  - 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 Cloud Console. 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 Cloud Console

Chaque composant de Kaspersky Security Center Cloud Console possède son propre ensemble de types d'événements. Cette section reprend les types d'événements qui se produisent dans le Serveur d'administration de Kaspersky Security Center Cloud Console 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 Cloud Console 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 Cloud Console.
- **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.

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 montre les événements du Serveur d'administration de Kaspersky Security Center Cloud Console au niveau d'importance **Critique**.

Pour chaque événement pouvant être généré par une application, vous pouvez spécifier les paramètres de notification et les paramètres de stockage sous l'onglet **Configuration des événements** dans la stratégie de l'application. Pour le Serveur d'administration, vous pouvez également consulter et configurer la liste des événements dans les propriétés du Serveur d'administration. Si vous souhaitez configurer les paramètres de notification pour tous les événements à la fois, configurez les paramètres de notification généraux dans les propriétés du Serveur d'administration.

Événements critiques du Serveur d'administration

Nom affiché du type d'événement	ID de type d'événement	Type d'événement	Description	Durée de stockage par défaut
La	4099	KLSRV_EV_LICENSE_CHECK_MORE_110	Une fois par jour, Kaspersky Security Center Cloud	180 jours

restriction de la licence a été dépassée			Console vérifie si une limite de licence est dépassée. Ce type d'événements se produit si le serveur d'administration détecte que certaines limites de licence sont dépassées par les applications Kaspersky installées sur les appareils clients et si le nombre d'unités de licence actuellement utilisé sous licence unique est supérieur à 110 % du nombre total d'unités sous licence. Même lorsque cet événement se produit, les appareils clients sont protégés. Vous pouvez répondre à l'événement des manières suivantes : • Parcourez la liste des appareils administrés. Supprimez les appareils inutilisés. • Fournissez une licence pour plusieurs appareils (ajoutez un code d'activation valide ou un fichier clé au serveur d'administration). Kaspersky Security Center Cloud Console définit les règles de génération d'événements lorsqu'une limite de la licence est dépassée.	
Propagation de virus	26 (pour la Protection contre les fichiers malicieux)	GNRL_EV_VIRUS_OUTBREAK	Ce type d'événements se produit lorsque le nombre d'objets malveillants détectés sur plusieurs appareils administrés dépasse le seuil sur une courte durée. Vous pouvez répondre à l'événement des manières suivantes : • Vous pouvez configurer le seuil dans les propriétés du Serveur d'administration. • Vous pouvez aussi créer une stratégie plus stricte qui sera activée ou créer une tâche qui sera exécutée quand l'événement se produit.	180 jours
Propagation de virus	27 (pour la Protection contre les menaces par emails)	GNRL_EV_VIRUS_OUTBREAK	Ce type d'événements se produit lorsque le nombre d'objets malveillants détectés sur plusieurs appareils administrés dépasse le seuil sur une courte durée. Vous pouvez répondre à l'événement des manières suivantes : • Vous pouvez configurer le seuil dans les propriétés du Serveur d'administration. • Vous pouvez aussi créer une stratégie plus stricte qui sera activée ou créer une tâche qui sera exécutée quand l'événement se produit.	180 jours
Propagation de virus	28 (pour le pare-feu)	GNRL_EV_VIRUS_OUTBREAK	Ce type d'événements se produit lorsque le nombre d'objets malveillants détectés sur plusieurs appareils administrés dépasse le seuil sur une courte durée. Vous pouvez répondre à l'événement des manières suivantes : • Vous pouvez configurer le seuil dans les propriétés du Serveur d'administration. • Vous pouvez aussi créer une stratégie plus stricte qui sera activée ou créer une tâche qui sera exécutée quand l'événement se produit.	180 jours
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.	180 jours

			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.	
L'appareil est en état Critique	4113	KLSRV_HOST_STATUS_CRITICAL	Ce type d'événements se produit lorsqu'un appareil administré a reçu l'état *Critique*. Vous pouvez configurer les conditions dans lesquelles l'état de l'appareil devient *Critique*.	180 jours
Mode limité	4130	KLSRV_EV_LICENSE_SRV_LIMITED_MODE	Ce type d'événements se produit lorsque Kaspersky Security Center Cloud Console commence à fonctionner avec les fonctionnalités de base, sans les fonctionnalités de la 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 Cloud Console (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 licence expire bientôt	4129	KLSRV_EV_LICENSE_SRV_EXPIRE_SOON	Des événements de ce type se produisent lorsque la date de fin de la durée de validité de la licence commerciale approche. Une fois par jour, Kaspersky Security Center vérifie si la date de fin de la durée de validité de la licence approche. Les événements de ce type sont publiés 30 jours, 15 jours, 5 jours et 1 jour avant la date de fin de la durée de validité de la licence. 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 Cloud Console 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 durée de validité du certificat MDM a expiré	4132	KLSRV_CERTIFICATE_EXPIRED	Des événements de ce type se produisent lorsque le certificat du Serveur d'administration pour l'Administration des appareils mobiles expire. Vous devez mettre à jour le certificat expiré.	180 jours
Les mises à jour des modules des applications Kaspersky ont été rappelées	4142	KLSRV_SEAMLESS_UPDATE_REVOKED	Ce type d'événements se produit si des mises à jour continues ont été révoquées (l'état *Révoqué* est affiché pour ces mises à jour) par des spécialistes techniques de Kaspersky ; par exemple, ils doivent être mis à jour vers une version plus récente. L'événement concerne les correctifs de Kaspersky Security Center Cloud Console et non les modules d'applications administrés par	180 jours

			Kaspersky. L'événement indique que les mises à jour continues ne sont pas installées.	
Audit : l'exportation vers le SIEM a échoué	5130	KLAUD_EV_SIEM_EXPORT_ERROR	Les événements de ce type se produisent lorsque l'exportation d'événements vers le système SIEM a échoué en raison d'une erreur de connexion avec le système SIEM.	180 jours

Événements liés à des erreurs de fonctionnement du Serveur d'administration

Le tableau ci-dessous montre les événements du Serveur d'administration de Kaspersky Security Center Cloud Console au niveau d'importance **Erreur de fonctionnement**.

Pour chaque événement pouvant être généré par une application, vous pouvez spécifier les paramètres de notification et les paramètres de stockage sous l'onglet **Configuration des événements** dans la stratégie de l'application. Pour le Serveur d'administration, vous pouvez également consulter et configurer la liste des événements dans les propriétés du Serveur d'administration. Si vous souhaitez configurer les paramètres de notification pour tous les événements à la fois, configurez les paramètres de notification généraux dans les propriétés du Serveur d'administration.

Événements liés à des erreurs de fonctionnement du Serveur d'administration

Nom affiché du type d'événement	ID de type d'événement	Type d'événement	Description	Durée de stockage par défaut
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). Des événements de ce type se produisent si, dans Kaspersky Security Center Cloud Console, vous gérez les clés de licence d'applications tierces et si le nombre d'installations a dépassé la limite définie par la clé de licence de l'application tierce. Vous pouvez répondre à l'événement des manières suivantes : • Parcourez la liste des appareils administrés. Supprimez l'application tierce des appareils où l'application n'est pas utilisée. • Utiliser une licence tierce pour plusieurs appareils. Vous pouvez gérer les clés de licence d'applications tierces à l'aide des fonctionnalités des groupes des applications sous licence. Un groupe des applications sous licence inclut les applications tierces qui répondent aux critères que vous avez définis.	180 jours
Échec du sondage du segment dans le cloud	4143	KLSRV_KLCLOUD_SCAN_ERROR	Des événements de ce type se produisent lorsque le Serveur d'administration ne parvient pas à interroger un segment de réseau dans un environnement cloud. Lisez les détails dans la description de l'événement et répondez en conséquence.	Non stocké

Événements d'avertissement du Serveur d'administration

Le tableau ci-dessous montre les événements du Serveur d'administration de Kaspersky Security Center Cloud Console au niveau d'importance **Avertissement**.

Pour chaque événement pouvant être généré par une application, vous pouvez spécifier les paramètres de notification et les paramètres de stockage sous l'onglet **Configuration des événements** dans la stratégie de l'application. Pour le Serveur d'administration, vous pouvez également consulter et configurer la liste des événements dans les propriétés du Serveur d'administration. Si vous souhaitez configurer les paramètres de notification pour tous les événements à la fois, configurez les paramètres de notification généraux dans les propriétés du Serveur d'administration.

Événements d'avertissement du Serveur d'administration

Nom affiché du type d'événement	ID de type d'événement	Type d'événement	Description	Durée de stockage par défaut
La restriction de la licence a été dépassée	4098	KLSRV_EV_LICENSE_CHECK_100_110	Une fois par jour, Kaspersky Security Center Cloud Console vérifie si une limite de licence est dépassée. Ce type d'événements se produit si le serveur d'administration détecte que certaines limites de licence sont dépassées par les applications Kaspersky installées sur les appareils clients et si le nombre d'unités de licence actuellement utilisé sous licence unique représente 100 % à 110 % du nombre total d'unités sous licence. Même lorsque cet événement se produit, les appareils clients sont protégés. Vous pouvez répondre à l'événement des manières suivantes : • Parcourez la liste des appareils administrés. Supprimez les appareils inutilisés. • Fournissez une licence pour plusieurs appareils (ajoutez un code d'activation valide ou un fichier clé au serveur d'administration). Kaspersky Security Center Cloud Console définit les règles de génération d'événements lorsqu'une limite de la licence est dépassée.	90 jours
L'appareil est resté inactif sur le réseau depuis longtemps	4103	KLSRV_EVENT_HOSTS_NOT_VISIBLE	Des événements de ce type se produisent lorsqu'un appareil administré est inactif pendant un certain temps. Le plus souvent, cela se produit lorsqu'un appareil administré est mis hors service. Vous pouvez répondre à l'événement des manières suivantes : • Supprimez manuellement l'appareil de la liste des appareils administrés. Spécifiez l'intervalle de temps après lequel l'événement **L'appareil est resté inactif sur le réseau depuis longtemps** est créé à l'aide de Kaspersky Security Center Cloud Console. • Spécifiez l'intervalle de temps après lequel l'appareil est automatiquement supprimé du groupe à l'aide de Kaspersky Security Center Cloud Console.	90 jours
Noms d'appareil en conflit	4102	KLSRV_EVENT_HOSTS_CONFLICT	Des événements de ce type se produisent lorsque le Serveur d'administration considère deux ou plusieurs appareils administrés comme un seul appareil.	90 jours

			Bien que le clonage ne soit pas pris en charge dans Kaspersky Security Center Cloud Console, cet événement peut se produire si vous effectuez le clonage à l'aide d'un outil tiers. Pour éviter cet événement, lorsque vous copiez l'image d'un appareil sur lequel l'Agent d'administration est installé, vous devez respecter les recommandations suivantes : • Sur l'appareil étalon, arrêter le service de l'Agent d'administration et lancer l'utilitaire klmover avec la clé -dupfix. Par la suite, refuser le lancement du service de l'Agent d'administration jusqu'à l'exécution de l'opération de prise de l'image. • Garantir le lancement de l'utilitaire klmover avec la clé -dupfix avant (point important) le premier lancement du service de l'Agent d'administration sur les appareils au premier démarrage du système d'exploitation après le déploiement de l'image. L'utilitaire klmover fait partie du paquet d'installation de l'Agent d'administration. Si vous capturez l'image d'un appareil sur lequel l'Agent d'administration n'est pas installé, effectuez le déploiement de l'image sur les appareils cibles, puis déployez l'Agent d'administration. Vous devez autoriser l'accès au dossier réseau avec les paquets d'installation autonomes à partir des appareils.	
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
Pour un des groupes des applications sous licence, la limite du nombre d'installations sera bientôt dépassée	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.	90 jours
Le certificat a été demandé	4133	KLSRV_CERTIFICATE_REQUESTED	Des événements de ce type se produisent lorsqu'un certificat pour l'administration des appareils mobiles ne parvient pas à être réémis automatiquement. Les causes et les réponses appropriées à cet événement peuvent être les suivantes : • La réémission automatique a été lancée pour un certificat pour lequel l'option **Le certificat a été demandé** est désactivée. Cela peut être dû à une	90 jours

			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.	
Le certificat a été supprimé	4134	KLSRV_CERTIFICATE_REMOVED	Des événements de ce type se produisent lorsqu'un administrateur supprime tout type de certificat (général, email, VPN) pour l'Administration des appareils mobiles. Une fois qu'un certificat aura été supprimé, les appareils mobiles connectés via ce certificat ne parviendront pas à se connecter au Serveur d'administration. Cet événement pourrait être utile lors d'une enquête sur les dysfonctionnements liés à l'administration des appareils mobiles.	90 jours
La durée de validité du certificat APNs a expiré	4135	KLSRV_APN_CERTIFICATE_EXPIRED	Des événements de ce type se produisent lorsqu'un certificat APNs expire. Vous devez renouveler manuellement le certificat APNs et l'installer sur un serveur MDM iOS.	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.	90 jours
Échec de l'envoi d'un message FCM sur l'appareil mobile	4138	KLSRV_GCM_DEVICE_ERROR	Des événements de ce type se produisent lorsque l'Administration des appareils mobiles est configurée de façon à utiliser Google Firebase Cloud Messaging (FCM) pour se connecter aux appareils mobiles administrés avec un système d'exploitation Android et que le serveur FCM ne parvient pas à traiter certaines des requêtes reçues de la part du Serveur d'administration. Cela signifie que certains des appareils mobiles administrés ne recevront aucune notification push. Lisez le code HTTP dans les détails de la description de l'événement et répondez en conséquence. Pour en savoir plus sur les codes HTTP reçus de la part du serveur FCM et sur les erreurs qui y sont liées, veuillez consulter la documentation du service Google Firebase (voir le chapitre " Codes de réponse d'erreur aux messages en aval ").	90 jours
Erreur HTTP lors de l'envoi d'un message FCM sur le serveur FCM	4139	KLSRV_GCM_HTTP_ERROR	Des événements de ce type se produisent lorsque l'Administration des appareils mobiles est configurée de façon à utiliser Google Firebase Cloud Messaging (FCM) pour connecter les appareils mobiles administrés avec le système d'exploitation Android et que le serveur FCM revient à la requête du Serveur d'administration avec un code HTTP différent de 200 (OK). Les causes et les réponses appropriées à cet événement peuvent être les suivantes :	90 jours

			• Problèmes du côté du serveur FCM. Lisez le code HTTP dans les détails de la description de l'événement et répondez en conséquence. Pour en savoir plus sur les codes HTTP reçus de la part du serveur FCM et sur les erreurs qui y sont liées, veuillez consulter la documentation du service Google Firebase (voir le chapitre " Codes de réponse d'erreur aux messages en aval "). • Problèmes du côté du serveur proxy (si vous utilisez un serveur proxy). Lisez le code HTTP dans les détails de l'événement et répondez en conséquence.	
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
La connexion au Serveur d'administration secondaire a été perdue	4116	KLSRV_EV_SLAVE_SRV_DISCONNECTED	Des événements de ce type se produisent lorsqu'une connexion au Serveur d'administration secondaire est interrompue. Lisez le journal du système d'exploitation sur l'appareil sur lequel le serveur d'administration secondaire est installé et répondez en conséquence.	90 jours
La connexion au Serveur d'administration principal a été interrompue	4118	KLSRV_EV_MASTER_SRV_DISCONNECTED	Des événements de ce type se produisent lorsqu'une connexion au Serveur d'administration principal est interrompue. Lisez le journal du système d'exploitation sur l'appareil sur lequel le serveur d'administration primaire est installé et répondez en conséquence.	90 jours
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

Événements informatifs du Serveur d'administration

Le tableau ci-dessous montre les événements du Serveur d'administration de Kaspersky Security Center Cloud Console au niveau d'importance **Information**.

Pour chaque événement pouvant être généré par une application, vous pouvez spécifier les paramètres de notification et les paramètres de stockage sous l'onglet **Configuration des événements** dans la stratégie de l'application. Pour le Serveur d'administration, vous pouvez également consulter et configurer la liste des événements dans les propriétés du Serveur d'administration. Si vous souhaitez configurer les paramètres de notification pour tous les événements à la fois, configurez les paramètres de notification généraux dans les propriétés du Serveur d'administration.

Événements informatifs du Serveur d'administration

Nom affiché du type d'événement	ID de type d'événement	Type d'événement	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 limites de licence sont sur le point d'être dépassées par les applications Kaspersky installées sur les appareils clients et si le nombre d'unités de licence actuellement utilisé sous licence unique constitue plus de 90 % du nombre total d'unités sous licence. Même lorsqu'une limite de licence est dépassée, les appareils clients sont protégés. Vous pouvez répondre à l'événement des manières suivantes : • Parcourez la liste des appareils administrés. Supprimez les appareils inutilisés. • Fournissez une licence pour plusieurs appareils (ajoutez un code d'activation valide ou un fichier clé au serveur d'administration). Kaspersky Security Center Cloud Console définit les règles de génération d'événements lorsqu'une limite de la licence est dépassée.	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
L'appareil a été déplacé automatiquement selon la règle	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 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
Pour un des groupes des applications sous licence, le nombre d'installations autorisées est épuisé à plus de 95 %	4128	KLSRV_INVLICPROD_EXPIRED_SOON	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.	30 jours

			Vous pouvez gérer les clés de licence d'applications tierces à l'aide des fonctionnalités des groupes d'applications sous licence.	
Des fichiers à envoyer à Kaspersky pour analyse ont été détectés	4131	KLSRV_APS_FILE_APPEARED		30 jours
L'ID d'instance FCM de l'appareil mobile a modifié	4137	KLSRV_GCM_DEVICE_REGID_CHANGED	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
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
La connexion au Serveur d'administration secondaire a été établie	4115	KLSRV_EV_SLAVE_SRV_CONNECTED	Pour en savoir plus, consultez la rubrique suivante : Création d'une hiérarchie des Serveurs d'administration : ajout d'un Serveur d'administration secondaire.	30 jours
La connexion au Serveur d'administration principal a été établie	4117	KLSRV_EV_MASTER_SRV_CONNECTED		30 jours
Les bases de données ont été mises à jour (Dans Kaspersky Security Center Cloud Console, ce type d'événement est uniquement disponible pour un serveur d'administration secondaire.)	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
Le proxy KSN a démarré. La vérification de la disponibilité de KSN a réussi	7718	KSNPROXY_STARTED_CON_CHK_OK		30 jours
Le serveur proxy KSN a été arrêté	7720	KSNPROXY_STOPPED		30 jours
Audit : une connexion au Serveur d'administration a été établie	4147	KLAUD_EV_SERVERCONNECT		30 jours
Audit : un objet a été modifié	4148	KLAUD_EV_OBJECTMODIFY	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 : 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 : 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 : les clés de chiffrement ont été importées ou exportées à partir du Serveur d'administration	5100	KLAUD_EV_DPEKEYSEXPORT		30 jours
Audit : le test de connexion au serveur SIEM a réussi	5110	KLAUD_EV_SIEM_TEST_SUCCESS		30 jours

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, regroupés par niveau de gravité **Erreur de fonctionnement**.

Pour chaque événement pouvant être généré par une application, vous pouvez spécifier les paramètres de notification et les paramètres de stockage sous l'onglet **Configuration des événements** dans la stratégie de l'application. Si vous souhaitez configurer les paramètres de notification pour tous les événements à la fois, configurez les paramètres de notification généraux dans les propriétés du Serveur d'administration.

Événements liés aux erreurs de fonctionnement de l'Agent d'administration

Nom affiché du type d'événement	ID de type d'événement	Type d'événement	Description	Durée de stockage par défaut
Erreur d'installation de la mise à jour	7702	KLNAG_EV_PATCH_INSTALL_ERROR	Des événements de ce type se produisent si l'installation automatique des mises à jour et des correctifs pour les composants de Kaspersky Security Center Cloud Console ne réussit pas. L'événement ne concerne pas les mises à jour des applications Kaspersky administrées. Lisez la description de l'événement. Cet événement peut être dû à un problème Windows sur le serveur d'administration. Si la description mentionne un problème de configuration Windows, résolvez le problème.	30 jours
Échec de l'installation de la mise à jour du logiciel tiers	7697	KLNAG_EV_3P_PATCH_INSTALL_ERROR	Des événements de ce type se produisent si les fonctionnalités de la gestion des vulnérabilités et des correctifs et d'administration des appareils mobiles sont en cours d'utilisation, et si la mise à jour des logiciels tiers n'a pas réussi. Vérifiez si le lien vers le logiciel tiers est valide. Lisez la description de l'événement.	30 jours
Échec de l'installation des mises à jour Windows Update	7717	KLNAG_EV_WUA_INSTALL_ERROR	Ce type d'événements se produit si les mises à jour Windows échouent. Configurez les mises à jour Windows dans une stratégie d'Agent d'administration. Lisez la description de l'événement. Recherchez l'erreur dans la base de connaissance Microsoft. Contactez le Support Technique de Microsoft si vous ne parvenez pas à résoudre le problème vous-même.	30 jours

Événements d'avertissement de l'Agent d'administration

Le tableau suivant reprend les événements de l'Agent d'administration de Kaspersky Security Center, regroupés par niveau de gravité **Avertissement**.

Pour chaque événement pouvant être généré par une application, vous pouvez spécifier les paramètres de notification et les paramètres de stockage sous l'onglet **Configuration des événements** dans la stratégie de l'application. Si vous souhaitez configurer les paramètres de notification pour tous les événements à la fois, configurez les paramètres de notification généraux dans les propriétés du Serveur d'administration.

Événements d'avertissement de l'Agent d'administration

Nom affiché du type d'événement	ID de type d'événement	Type d'événement	Durée de stockage par défaut
Avertissement renvoyé lors de l'installation des mises à jour des modules de l'application	7701	KLNAG_EV_PATCH_INSTALL_WARNING	30 jours
L'installation de la mise à jour du logiciel tiers s'est terminée avec un avertissement	7696	KLNAG_EV_3P_PATCH_INSTALL_WARNING	30 jours
L'installation de la mise à jour du logiciel tiers a été reportée	7698	KLNAG_EV_3P_PATCH_INSTALL_SLIPPED	30 jours
Un problème de sécurité est survenu	549	GNRL_EV_APP_INCIDENT_OCCURED	30 jours
Le proxy KSN a démarré. Échec de la vérification de la disponibilité de KSN	7718	KSNPROXY_STARTED_CON_CHK_FAILED	30 jours

Événements informatifs de l'Agent d'administration

Le tableau suivant reprend les événements de l'Agent d'administration de Kaspersky Security Center, regroupés par niveau de gravité **Information**.

Pour chaque événement pouvant être généré par une application, vous pouvez spécifier les paramètres de notification et les paramètres de stockage sous l'onglet **Configuration des événements** dans la stratégie de l'application. Si vous souhaitez configurer les paramètres de notification pour tous les événements à la fois, configurez les paramètres de notification généraux dans les propriétés du Serveur d'administration.

Événements informatifs de l'Agent d'administration

Nom affiché du type d'événement	ID de type d'événement	Type d'événement	Durée de stockage par défaut
La mise à jour des modules de l'application a bien été appliquée	7699	KLNAG_EV_PATCH_INSTALLED_SUCCESSFULLY	30 jours
L'installation des mises à jour pour les modules de l'application a démarré	7700	KLNAG_EV_PATCH_INSTALL_STARTING	30 jours
L'application a été installée	7703	KLNAG_EV_INV_APP_INSTALLED	30 jours
L'application a été désinstallée	7704	KLNAG_EV_INV_APP_UNINSTALLED	30 jours
L'application contrôlée a été installée	7705	KLNAG_EV_INV_OBS_APP_INSTALLED	30 jours
L'application contrôlée a été désinstallée	7706	KLNAG_EV_INV_OBS_APP_UNINSTALLED	30 jours
L'application tierce a été installée	7707	KLNAG_EV_INV_CMPTR_APP_INSTALLED	30 jours
Un nouvel appareil a été ajouté	7708	KLNAG_EV_DEVICE_ARRIVAL	30 jours
L'appareil a été supprimé	7709	KLNAG_EV_DEVICE_REMOVE	30 jours
L'appareil a été détecté	7710	KLNAG_EV_NAC_DEVICE_DISCOVERED	30 jours

L'appareil a été autorisé	7711	KLNAG_EV_NAC_HOST_AUTHORIZED	30 jours
Partage du bureau Windows : le fichier est lu	7712	KLUSRLOG_EV_FILE_READ	30 jours
Partage du bureau Windows : le fichier a été modifié	7713	KLUSRLOG_EV_FILE_MODIFIED	30 jours
Partage du bureau Windows : l'application a démarré	7714	KLUSRLOG_EV_PROCESS_LAUNCHED	30 jours
Partage du bureau Windows : lancé	7715	KLUSRLOG_EV_WDS_BEGIN	30 jours
Partage du bureau Windows : arrêté	7716	KLUSRLOG_EV_WDS_END	30 jours
L'installation de la mise à jour d'un logiciel tiers a réussi	7694	KLNAG_EV_3P_PATCH_INSTALLED_SUCCESSFULLY	30 jours
L'installation de la mise à jour du logiciel tiers est lancée	7695	KLNAG_EV_3P_PATCH_INSTALL_STARTING	30 jours
Le proxy KSN a démarré. La vérification de la disponibilité de KSN a réussi	7719	KSNPROXY_STARTED_CON_CHK_OK	30 jours
Le serveur proxy KSN a été arrêté	7720	KSNPROXY_STOPPED	30 jours

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 Cloud Console pour configuration.

Les sélections d'événements sont disponibles dans Kaspersky Security Center Cloud Console, dans la section **Surveillance et rapports**, en cliquant sur **Sélections d'événements**.

Par défaut, les sélections d'événements incluent des informations sur les 7 derniers jours.

Kaspersky Security Center Cloud Console offre un groupe par défaut de sélections (prédéfinies) d'événements :

- Événements de différents niveaux d'importance :
  - **Événements critique**
  - **Erreur de fonctionnement**
  - **Avertissements**
  - **Messages d'information**
- **Requêtes des utilisateurs** (événements d'applications administrées)
- **Derniers événements** (de la dernière semaine)

- **Événements de l'audit**

  Les événements de l'audit liés aux opérations de service dans votre espace de travail s'affichent dans Kaspersky Security Center Cloud Console. Ces événements sont conditionnés par les actions des experts Kaspersky. Ces événements incluent par exemple les éléments suivants : modification des ports du Serveur d'administration, sauvegarde de la base de données du Serveur d'administration, création, modification et suppression de comptes utilisateurs.

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 Cloud Console pour afficher ces événements. Plus la base de données est volumineuse, plus le processus peut prendre de temps.

Vous pouvez réaliser les opérations suivantes :

- Modifier les propriétés des sélections d'événements
- Générer des sélections d'événements
- Afficher les détails des sélections d'événements
- Supprimer des sélections d'événements
- Supprimer des événements de la base de données du Serveur d'administration

Création d'une sélection d'événements

Pour créer une sélection d'événements, procédez comme suit :

1. Dans le menu principal, accédez à **Surveillance et rapports** → **Sélections d'événements**.
2. Cliquez sur **Ajouter**.
3. Dans la fenêtre **Nouvelle sélection d'événements** qui s'ouvre, définissez les paramètres de la nouvelle sélection d'événements. Réalisez ceci dans une ou plusieurs sections de la fenêtre.
4. Cliquez sur le bouton **Enregistrer** afin d'enregistrer les modifications.

   La fenêtre de confirmation s'ouvre.
5. Pour voir les résultats de la sélection d'événements, ne décochez pas la case **Accéder au résultat de la sélection**.
6. Cliquez sur **Enregistrer** pour confirmer la création de la sélection d'événements.

Si vous n'avez pas décoché la case **Accéder au résultat de la sélection**, les résultats de la sélection d'événements sont affichés. Dans le cas contraire, la nouvelle sélection d'événements apparaît dans a liste des sélection d'événements.

Édition d'une sélection d'événements

Pour modifier une sélection d'événements, procédez comme suit :

1. Dans le menu principal, accédez à **Surveillance et rapports → Sélections d'événements**.
2. Cochez la case en regard de la sélection d'événements que vous souhaitez modifier.
3. Cliquez sur le bouton **Propriétés**.

   Une fenêtre avec les paramètres de la sélection d'événements s'ouvre.
4. Modifiez les propriétés de la sélection d'événements.

   > Pour les sélections d'événements prédéfinies, vous pouvez modifier uniquement les propriétés sous les onglets suivants : **Général** (sauf pour le nom de la sélection), **Heure** et **Privilèges d'accès**.

   Pour les sélections définies par l'utilisateur, vous pouvez modifier toutes les propriétés.
5. Cliquez sur le bouton **Enregistrer** afin d'enregistrer les modifications.

La sélection d'événements modifiée apparaît dans la liste.

Affichage d'une liste d'une sélection d'événements

Pour afficher une sélection d'événements, procédez comme suit :

1. Dans le menu principal, accédez à **Surveillance et rapports → Sélections d'événements**.
2. Cochez la case en regard de la sélection d'événements que vous souhaitez lancer.
3. Exécutez une des actions suivantes :

   - Si vous souhaitez configurer le tri dans le résultat de la sélection d'événements, procédez comme suit :

     a. Cliquez sur le bouton **Reconfigurer le tri et démarrer**.

     b. Dans la fenêtre ouverte **Reconfigurer le tri pour la sélection d'événements**, définissez les paramètres de tri.

     c. Cliquez sur le nom de la sélection.

   - Sinon, si vous souhaitez afficher la liste des événements tels qu'ils sont triés sur le Serveur d'administration, cliquez sur le nom de la sélection.

Le résultat de la sélection d'événements s'affiche.

Exportation d'une sélection d'événements

Kaspersky Security Center Cloud Console 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 Cloud Console (sélections prédéfinies) ne peuvent pas être enregistrées dans un fichier.

Pour exporter une sélection d'événements, procédez comme suit :

1. Dans le menu principal, accédez à **Surveillance et rapports → Sélections d'événements**.
2. Cochez la case en regard de la sélection d'événements que vous souhaitez exporter.

   Vous ne pouvez pas exporter plusieurs sélections d'événements à la fois. Si vous sélectionnez plusieurs sélections, le bouton **Exporter** sera désactivé.
3. Cliquez sur le bouton **Exporter**.
4. Dans la fenêtre **Enregistrer sous** qui s'ouvre, indiquez le nom et le chemin du fichier de sélection d'événements, puis cliquez sur le bouton **Enregistrer**.

   La fenêtre **Enregistrer sous** s'affiche uniquement si vous utilisez Google Chrome, Microsoft Edge ou Opera. Si vous utilisez un autre navigateur, le fichier de sélection d'événements est automatiquement enregistré dans le dossier **Téléchargements**.

Importation d'une sélection d'événements

Kaspersky Security Center Cloud Console vous permet d'importer une sélection d'événements à partir d'un fichier KLO. Le fichier KLO contient la sélection d'événements exportée et ses paramètres.

Pour importer une sélection d'événements, procédez comme suit :

1. Dans le menu principal, accédez à **Surveillance et rapports → Sélections d'événements**.
2. Cliquez sur le bouton **Importer**, puis choisissez un fichier de sélection d'événements à importer.
3. Dans la fenêtre ouverte, spécifiez le chemin d'accès au fichier KLO, puis cliquez sur le bouton **Ouvrir**. Notez que vous ne pouvez sélectionner qu'un seul fichier de sélection d'événements.

   Le traitement de la sélection d'événements démarre.

La notification avec les résultats de l'importation s'affiche. Si l'importation de la sélection d'événements a réussi, vous pouvez cliquer sur le lien **Afficher les détails de l'importation** pour afficher les propriétés de la sélection d'événements.

Après une importation réussie, la sélection d'événements s'affiche dans la liste de sélection. Les paramètres de la sélection d'événements sont également importés.

Si la sélection d'événements nouvellement importée a un nom identique à celui d'une sélection d'événements existante, le nom de la sélection importée est suivi de l'index **(<numéro de séquence suivant>)**, par exemple : **(1)**, **(2)**.

Affichage des détails d'un événement

Pour afficher les détails d'un événement :

1. Démarrage d'une sélection d'événements.
2. Cliquez sur l'heure de l'événement requis.

   La fenêtre des **Propriétés de l'événement** s'affiche.
3. Dans la fenêtre qui s'affiche, vous pouvez effectuer l'une des opérations suivantes :
   - Affichez les informations sur l'événement sélectionné
   - Accédez à l'événement suivant et précédent dans la résultat de la sélection d'événements
   - Accédez à l'appareil où l'événement s'est produit
   - Accédez au groupe d'administration qui inclut l'appareil sur lequel l'événement s'est produit
   - Pour un événement lié à une tâche, accédez aux propriétés de la tâche

Exportation des événements dans un fichier

Kaspersky Security Center Cloud Console permet d'enregistrer les événements de la sélection d'événements dans un fichier TXT.

Pour exporter des événements vers un fichier :

1. Démarrage d'une sélection d'événements.
2. Cochez la case à côté de l'événement requis.

   Vous pouvez également sélectionner plusieurs événements ou toute la sélection d'événements.
3. Cliquez sur le bouton **Exporter dans un fichier**.

L'événement sélectionné est exporté dans un fichier TXT.

Voir un historique d'objet à partir d'un événement

Pour un événement de création ou de modification d'un objet qui prend en charge la gestion des révisions, vous pouvez passer à l'historique des révisions de l'objet.

Pour voir un historique d'objet à partir d'un événement :

1. Démarrage d'une sélection d'événements.
2. Cochez la case à côté de l'événement requis.
3. Cliquez sur le bouton **Historique des révisions**.

L'Historique des révisions de l'objet est ouvert.

Enregistrement des événements sur les tâches et les stratégies

Cette section propose des recommandations sur la manière de réduire le nombre d'événements pour les tâches et les stratégies stockées dans la base de données de Kaspersky Security Center Cloud Console. Par défaut, tous les 1 000 appareils ont 100 000 événements. Si cette limite est dépassée, les nouveaux événements écrasent les anciens. Par conséquent, les événements critiques peuvent disparaître. De plus, l'événement d'avertissement du Serveur d'administration nommé **La limite du nombre d'événements dans la base de données est dépassée, les événements ont été supprimés** peut se produire. Dans ces cas, nous vous recommandons de suivre les instructions de cette section.

Vous augmenterez ainsi la vitesse d'exécution des scénarios associés à l'analyse des événements. En outre, ces recommandations vous aident à réduire le risque que les événements critiques soient écrasés par un grand nombre d'événements.

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 une tâche est exécutée fréquemment (par exemple, plus d'une fois par semaine), le nombre d'événements peut s'avérer trop important et les événements peuvent inonder 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, Kaspersky Security Center Cloud Console stocke uniquement les informations sur le lancement, la progression et l'achèvement de la tâche (réussie, avec un avertissement ou avec une erreur) de chaque appareil sur lequel la tâche est exécutée.
- **Sauvegarder uniquement le résultat de la tâche**. Dans ce cas, Kaspersky Security Center Cloud Console stocke uniquement les informations sur l'achèvement de la tâche (réussie, avec un avertissement ou avec une erreur) de chaque appareil sur lequel la tâche est exécutée.

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 ce cas, il est recommandé de sélectionner uniquement les événements les plus critiques dans les paramètres de stratégie et d'activer leur enregistrement. Il est recommandé de désactiver l'enregistrement de tous les autres événements.

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 conseillé de modifier les paramètres de stockage des événements si les événements sur les modifications des états intermédiaires des tâches de groupe et les événements sur l'application des stratégies occupent une grande partie de tous les événements de la base de données de Kaspersky Security Center Cloud Console.

Supprimer des événements

Pour supprimer un ou plusieurs événements :

1. Démarrage d'une sélection d'événements.
2. Cochez la case à côté des événements requis.
3. Cliquez sur le bouton **Supprimer**.

Les événements sélectionnés sont supprimés et ne peuvent pas être restaurés.

Suppression de sélections d'événements

Vous ne pouvez supprimer que les sélection d'événements définies par les utilisateurs. Les sélections d'événement prédéfinies ne peuvent pas être supprimées.

Pour supprimer une ou plusieurs sélections d'événements, procédez comme suit :

1. Dans le menu principal, accédez à **Surveillance et rapports → Sélections d'événements**.
2. Cochez les cases en regard des sélections d'événements que vous souhaitez supprimer.
3. Cliquez sur **Supprimer**.
4. Dans la fenêtre qui s'ouvre, cliquez sur **OK**.

La sélection d'événements est supprimée.

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.

Présentation des notifications

Kaspersky Security Center Cloud Console vous permet de surveiller le réseau de votre organisation en envoyant des notifications sur tout événement que vous considérez comme important. Vous pouvez configurer les notifications par email pour n'importe quel événement.

Dès réception de notifications par email, vous pouvez décider de votre réponse à l'événement. Cette réaction doit être celle qui est la plus appropriée pour le réseau de votre organisation.

Configuration de la permutation des états des appareils

Vous pouvez modifier les conditions pour attribuer le statut *Critique* ou *Avertissement* à un appareil.

Pour activer le changement d'état de l'appareil sur Critique :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Hiérarchie des groupes**.
2. Dans la liste des groupes qui s'affiche, cliquez sur le lien portant le nom d'un groupe dont vous voulez changer les états de l'appareil.
3. Dans la fenêtre des propriétés qui s'ouvre, sélectionnez l'onglet **État de l'appareil**.
4. Dans le volet de gauche, sélectionnez **Critique**.
5. Dans le volet droit, dans la section **Définir l'état comme "Critique" si les options suivantes sont définies**, activez la condition pour basculer un appareil en état *Critique*.

   Vous pouvez modifier seulement les paramètres qui ne sont pas verrouillés dans la stratégie parent.

6. Sélectionnez le bouton radio à côté de la condition dans la liste.
7. Dans le coin supérieur gauche de la liste, cliquez sur le bouton **Modifier**.
8. Définissez la valeur requise pour la condition sélectionnée.

   Certaines conditions n'acceptent pas de valeurs.

9. Cliquez sur le bouton **OK**.

Lorsque les conditions spécifiées sont remplies, l'appareil administré se voit affecter l'état *Critique*.

Pour activer le changement d'état de l'appareil sur Avertissement :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Hiérarchie des groupes**.
2. Dans la liste des groupes qui s'affiche, cliquez sur le lien portant le nom d'un groupe dont vous voulez changer les états de l'appareil.
3. Dans la fenêtre des propriétés qui s'ouvre, sélectionnez l'onglet **État de l'appareil**.
4. Dans le volet gauche, sélectionnez **Avertissement**.
5. Dans le volet droit, dans la section **Définir l'état comme "Avertissement" si les options suivantes sont définies,** activez la condition pour basculer un appareil en état *Avertissement*.

   Vous pouvez modifier seulement les paramètres qui ne sont pas verrouillés dans la stratégie parent.

6. Sélectionnez le bouton radio à côté de la condition dans la liste.
7. Dans le coin supérieur gauche de la liste, cliquez sur le bouton **Modifier**.

8. Définissez la valeur requise pour la condition sélectionnée.

   Certaines conditions n'acceptent pas de valeurs.

9. Cliquez sur le bouton **OK**.

Lorsque certaines conditions spécifiées sont remplies, l'appareil administré se voit affecter l'état *Avertissement*.

Configuration des paramètres d'envoi des notifications

Vous pouvez configurer la notification par email à propos d'événements se produisant dans Kaspersky Security Center Cloud Console.

Pour configurer l'envoi de notifications d'événements survenant dans Kaspersky Security Center Cloud Console :

1. Dans le menu principal, cliquez sur l'icône des paramètres ( ) en regard du nom du Serveur d'administration requis.

   La fenêtre des propriétés du Serveur d'administration s'ouvre avec l'onglet **Général** sélectionné.

2. Cliquez sur la section **Notification** et, dans le volet droit, définissez les paramètres de la notification par email :

   Destinataires (adresses email)

   Indiquez les adresses email des utilisateurs auxquels Kaspersky Security Center Cloud Console doit envoyer les notifications. Vous pouvez spécifier plusieurs adresses dans ce champ, en les séparant par un point-virgule.

   Vous pouvez renseigner un maximum de 24 adresses emails.

3. 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.

4. Cliquez sur **OK** pour fermer la fenêtre de 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 Cloud Console.

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.

Annonces de Kaspersky

Cette section décrit comment utiliser, configurer et désactiver les annonces de Kaspersky.

À propos des annonces de Kaspersky

La section des annonces de Kaspersky (**Surveillance et rapports → Annonces de Kaspersky**) vous tient informé en fournissant des informations relatives à Kaspersky Security Center Cloud Console et aux applications administrées installées sur les appareils administrés. Kaspersky Security Center Cloud Console met régulièrement à jour les informations de la section en supprimant les annonces obsolètes et en ajoutant de nouvelles informations.

Kaspersky Security Center Cloud Console 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.

Si plusieurs administrateurs utilisent Kaspersky Security Center Cloud Console et qu'ils définissent diverses langues d'interface, Kaspersky Security Center Cloud Console affiche les annonces de Kaspersky dans toutes les langues utilisées par les administrateurs. Lorsque vous modifiez la langue de l'interface, les annonces de Kaspersky dans la langue sélectionnée sont automatiquement ajoutées à la section une fois que vous vous êtes déconnecté de la console, puis que vous vous êtes reconnecté.

Les annonces contiennent des informations des types suivants :

- Annonces relatives à la sécurité

  Les annonces relatives à la sécurité visent à maintenir les applications Kaspersky installées sur votre réseau à jour et pleinement fonctionnelles. Les annonces peuvent inclure des informations concernant les mises à jour critiques des applications Kaspersky, des correctifs pour des vulnérabilités détectées et des moyens de résoudre d'autres problèmes dans les applications Kaspersky. Les annonces relatives à la sécurité sont activées par défaut. Si vous ne souhaitez pas recevoir les annonces, vous pouvez désactiver cette fonctionnalité.

  > Vous ne pouvez pas désactiver les annonces relatives à la sécurité dans le mode d'essai de Kaspersky Security Center Cloud Console.

  Pour vous montrer les informations correspondant à la configuration de la protection de votre réseau, Kaspersky Security Center Cloud Console envoie des données aux serveurs cloud de Kaspersky et ne reçoit que les annonces relatives aux applications Kaspersky installées sur votre réseau. Le jeu de données pouvant être envoyé aux serveurs est décrit dans le Contrat de Kaspersky Security Center Cloud Console que vous acceptez lorsque vous créez un espace de travail d'entreprise.

- 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 Cloud Console envoie des données aux serveurs cloud de Kaspersky et reçoit les annonces appropriées. L'ensemble des données qui peut être envoyé aux serveurs est décrit dans la section Données traitées de la Déclaration KSN.

Les nouvelles informations sont réparties dans les catégories suivantes, selon leur importance :

1. Informations critiques
2. Nouvelles importantes
3. Avertissement
4. Information

Lorsque de nouvelles informations apparaissent dans la section des annonces de Kaspersky, Kaspersky Security Center Cloud 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.

Désactivation des annonces de Kaspersky

La section Annonces de Kaspersky (**Surveillance et rapports → Annonces de Kaspersky**) vous tient informé en fournissant des informations relatives à votre version de Kaspersky Security Center Cloud Console et aux applications administrées installées sur les appareils administrés. Si vous ne souhaitez pas recevoir les annonces de Kaspersky, vous pouvez désactiver cette fonctionnalité.

Les annonces de Kaspersky incluent deux types d'informations : les annonces relatives à la sécurité et les annonces marketing. Vous pouvez désactiver les annonces de chaque type séparément.

> Vous ne pouvez pas désactiver les annonces relatives à la sécurité dans le mode d'essai de Kaspersky Security Center Cloud Console.

Pour désactiver les annonces relatives à la sécurité, procédez comme suit :

1. Dans le menu principal, cliquez sur l'icône des paramètres ( ) à côté du nom du Serveur d'administration.
   La fenêtre des propriétés du Serveur d'administration s'ouvre.
2. Sous l'onglet **Général**, sélectionnez la section **Annonces de Kaspersky**.
3. Basculez le commutateur sur la position **Annonces relatives à la sécurité Désactivées**.
4. Cliquez sur le bouton **Enregistrer**.
   Les annonces de Kaspersky sont désactivées.

Les annonces marketing sont désactivées par défaut. Vous ne recevez des annonces marketing que si vous avez activé Kaspersky Security Network (KSN). Vous pouvez désactiver ce type d'annonces en désactivant KSN.

Pour désactiver les annonces marketing, procédez comme suit :

1. Dans le menu principal, cliquez sur l'icône des paramètres ( ) à côté du nom du Serveur d'administration.
   La fenêtre des propriétés du Serveur d'administration s'ouvre.
2. Sous l'onglet **Général**, sélectionnez la section **Paramètres KSN**.
3. Désactivez l'option **J'accepte les termes du Kaspersky Security Network**.
4. Cliquez sur le bouton **Enregistrer**.
   Les annonces marketing sont désactivées.

Réception d'un avertissement d'expiration de licence

Pour ajouter une clé de licence Kaspersky Endpoint Security for Business Select au Serveur d'administration, procédez comme suit :

1. Dans le menu principal, cliquez sur l'icône des paramètres ( ) à côté du nom du Serveur d'administration.

   La fenêtre des propriétés du Serveur d'administration s'ouvre.

2. Sous l'onglet **Général**, sélectionnez la section **Clés de licence**.

3. Cliquez sur **Sélectionner**.

4. Dans la fenêtre qui s'ouvre, sélectionnez votre licence et cliquez sur **OK**.

   Sinon, si aucune licence ne s'affiche, vous pouvez cliquer sur **Ajouter une nouvelle clé de licence** et utiliser votre code d'activation.

La licence est ajoutée dans le stockage du Serveur d'administration. Le Serveur d'administration génère ainsi l'événement critique *La licence expire bientôt* un jour avant la fin de la validité de la licence et l'événement critique *Mode limité* après la fin de la durée de validité de la licence. Si vous le souhaitez, vous pouvez configurer la remise des notifications.

Si vous ajoutez une licence Kaspersky Endpoint Security for Business Select au stockage du Serveur d'administration, la clé de licence est considérée comme étant utilisée sur un appareil.

Cloud Discovery

Kaspersky Security Center Cloud Console 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 fonctionnalité Cloud Discovery est disponible uniquement si vous avez acheté une licence Kaspersky Next. Pour en savoir plus, consultez la section Licences et nombre minimum d'appareils pour chaque licence.

Vous pouvez activer la fonctionnalité Cloud Discovery et sélectionner les stratégies ou les profils de sécurité pour lesquels vous souhaitez activer la fonctionnalité. Vous pouvez également activer ou désactiver la fonctionnalité séparément dans chaque stratégie ou profil de sécurité. Vous pouvez interdire l'accès aux services cloud auxquels vous ne souhaitez pas que les utilisateurs accèdent.

Pour pouvoir interdire l'accès aux services cloud indésirables, assurez-vous que les conditions préalables suivantes sont remplies :

- Vous utilisez Kaspersky Endpoint Security 11.2 for Windows ou une version ultérieure. Les versions antérieures de l'application de sécurité vous permettent uniquement de surveiller l'utilisation des services cloud.
- Vous avez acheté une 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 Cloud Console obtient les informations sur l'utilisation des services cloud pour tous les appareils administrés qui sont protégés uniquement par des stratégies de sécurité ou des profils pour lesquels cette 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 Cloud Console.
2. Dans le menu principal, accédez à **Surveillance et rapports** → **Tableau de bord**.
3. Sur le widget **Cloud Discovery**, cliquez sur le bouton **Activer**.
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 Cloud Console.

2. Dans le menu principal, accédez à **Surveillance et rapports → Tableau de bord**.

3. Cliquez sur le bouton **Ajouter ou restaurer un widget web**.

4. Dans la liste des widgets disponibles, cliquez sur l'icône en forme de chevron (>) en regard de la catégorie **Autres**.

5. Sélectionnez le widget **Cloud Discovery**, puis cliquez sur le bouton **Ajouter**.

   Si la fonctionnalité Cloud Discovery est désactivée, suivez les instructions de la section Activation de Cloud Discovery à l'aide du widget.

Le widget sélectionné est ajouté à la fin du tableau de bord.

Affichage d'informations sur l'utilisation des services cloud

Vous pouvez afficher le widget **Cloud Discovery** qui affiche des informations sur les tentatives d'accès aux services cloud. Le widget affiche également le niveau de risque de chaque service cloud. Kaspersky Security Center Cloud Console obtient les informations sur l'utilisation des services cloud pour tous les appareils administrés qui sont protégés uniquement par des stratégies de sécurité pour lesquelles la fonctionnalité est activée.

Avant d'afficher les informations, assurez-vous que :

- le widget Cloud Discovery est ajouté au tableau de bord.
- la fonctionnalité Cloud Discovery est activée.
- le droit **Lecture** figure dans la zone fonctionnelle **Caractéristiques générales : fonctionnalité de base**.

Pour afficher le widget Cloud Discovery, procédez comme suit :

1. Accédez à Kaspersky Security Center Cloud Console.

2. Dans le menu principal, accédez à **Surveillance et rapports → Tableau de bord**.

   Le widget **Cloud Discovery** s'affiche sur le tableau de bord.

3. Dans la partie gauche du widget **Cloud Discovery**, sélectionnez une catégorie de services cloud.

   Le tableau à droite du widget affiche jusqu'à cinq services, issus de la catégorie sélectionnée, auxquels les utilisateurs tentent le plus souvent d'accéder. Les tentatives réussies et bloquées sont comptabilisées.

4. Dans la partie droite du widget, sélectionnez un service spécifique.

   Le tableau ci-dessous affiche une dizaine d'appareils qui tentent le plus souvent d'accéder au service. Ce tableau permet de créer deux types de rapports : le rapport sur les tentatives d'accès réussies et le rapport sur les tentatives d'accès bloquées.

   De plus, ce tableau permet de bloquer l'accès au service cloud pour un appareil défini.

Le widget affiche les informations demandées.

À partir du widget affiché, vous pouvez effectuer les opérations suivantes :

- Passer à la section **Surveillance et rapports → Rapports** pour consulter les rapports de Cloud Discovery.
- Interdire ou autoriser l'accès au service cloud sélectionné.

La fonctionnalité Cloud Discovery est disponible uniquement si vous avez acheté une licence Kaspersky Next. Pour en savoir plus, consultez la section Licences et nombre minimum d'appareils pour chaque licence.

Niveau de risque d'un service cloud

Cloud Discovery indique un niveau de risque pour chaque service cloud. Le niveau de risque vous aide à déterminer les services qui ne correspondent pas aux exigences de sécurité de votre organisation. Par exemple, vous souhaiterez peut-être prendre en considération le niveau de risque lorsque vous déciderez d'interdire ou non l'accès à un service.

Le niveau de risque est un indice estimé et ne dit rien sur la qualité d'un service cloud ou sur le fabricant du service. Le niveau de risque est simplement une recommandation des experts de Kaspersky.

Le widget Cloud Discovery affiche les niveaux de risque des services cloud dans la liste de tous les services cloud surveillés.

Bloquer l'accès aux services cloud indésirables

Vous pouvez bloquer l'accès aux services cloud auxquels vous ne souhaitez pas que les utilisateurs accèdent. Vous pouvez également autoriser l'accès à des services cloud qui ont été précédemment bloqués.

Vous souhaiterez peut-être prendre, entre autres, le niveau de risque en considération lorsque vous déciderez d'interdire ou non l'accès à un service.

Vous pouvez interdire ou autoriser l'accès aux services cloud pour une stratégie ou un profil de sécurité.

Il existe deux manières de bloquer l'accès aux services cloud indésirables :

- En utilisant le widget Cloud Discovery.

  Dans ce cas, vous pouvez bloquer l'accès aux services un par un.

- Dans les propriétés de la stratégie Kaspersky Endpoint Security for Windows.

  Dans ce cas, vous pouvez interdire l'accès aux services un par un ou interdire l'ensemble d'une catégorie à la fois.

  Pour en savoir plus sur l'activation de la fonctionnalité Cloud Discovery dans les propriétés de la stratégie Kaspersky Endpoint Security for Windows, veuillez consulter la section Cloud Discovery de l'aide de Kaspersky Endpoint Security for Windows.

Pour interdire ou autoriser l'accès à un service cloud en utilisant le widget, procédez comme suit :

1. Ouvrez le widget Cloud Discovery, puis sélectionnez le service cloud requis.
2. Dans le **Les 10 principaux appareils qui utilisent le service**, trouvez la stratégie ou le profil de sécurité pour lequel vous souhaitez interdire ou autoriser le service.
3. Sur la ligne requise, dans la colonne **État d'accès dans la stratégie/le profil**, exécutez une des actions suivantes :

- Pour bloquer le service, sélectionnez **Bloqué** dans la liste déroulante.
- Pour autoriser le service, sélectionnez **Autorisé** dans la liste déroulante.

4. Cliquez sur **Enregistrer**.

L'accès au service sélectionné est bloqué ou autorisé pour la stratégie ou le profil de sécurité.

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 principal, accédez à **Ressources (Appareils)** → **Groupes** → **<nom du groupe>** → **Appareils administrés**.
   - Si l'appareil appartient au groupe Appareils non définis, dans le menu principal, accédez à **Découverte et déploiement** → **Appareils non définis**.
2. Cliquez sur le nom de l'appareil concerné.
3. Dans la fenêtre des propriétés de l'appareil qui s'ouvre, sélectionnez l'onglet **Avancé**.
4. Dans 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, un 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 paramètres suivants sont disponibles :

   - Niveau de traçage

     Le niveau de traçage définit le volume de détails repris dans le fichier de traçage.

   - Traçage sur la base d'une rotation

     L'application écrase les informations de traçage afin d'empêcher l'augmentation excessive de la taille du fichier de traçage. Indiquez le nombre maximal de fichiers à utiliser pour stocker les informations de traçage ainsi que la taille maximale de chaque fichier. Quand le nombre maximum de fichiers de traçage de la taille maximale est atteint, le fichier de traçage le plus ancien est supprimé afin de pouvoir écrire un nouveau fichier de traçage.

     Ce paramètre est disponible uniquement pour Kaspersky Endpoint Security.

   c. Cliquez sur **Enregistrer**.

   Le traçage est activé pour l'application sélectionnée. Dans certains cas, pour activer le traçage de l'application de sécurité, il faut relancer cette application et sa tâche.

   Sur les appareils clients basés sur Linux, le traçage pour le module Programme de mise à jour de Kaspersky Security Agent 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 **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

Vous pouvez télécharger des fichiers de traçage à partir d'un appareil client si l'une des conditions suivantes est remplie : l'option **Maintenir la connexion au Serveur d'administration** est activée dans les paramètres de l'appareil, un serveur push ou une passerelle de connexion est en cours d'utilisation. Dans le cas contraire, il n'est pas possible d'effectuer de téléchargement.

Le total des appareils pour lesquels l'option **Maintenir la connexion au Serveur &d'administration** a été sélectionnée ne peut être supérieur à 300.

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 l'option **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.

   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.

Télécharger les paramètres de l'application

Vous pouvez télécharger les paramètres d'application à partir d'un appareil client si l'une des conditions suivantes est remplie : l'option **Maintenir la connexion au Serveur d'administration** est activée dans les paramètres de l'appareil, un serveur push ou une passerelle de connexion est en cours d'utilisation. Dans le cas contraire, il n'est pas possible d'effectuer de téléchargement.

Le total des appareils pour lesquels l'option **Maintenir la connexion au Serveur &d'administration** a été sélectionnée ne peut être supérieur à 300.

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

Vous pouvez télécharger les informations système sur votre appareil à partir d'un appareil client uniquement si l'une des conditions suivantes est remplie : l'option **Maintenir la connexion au Serveur d'administration** est activée dans les paramètres de l'appareil, un serveur push ou une passerelle de connexion est en cours d'utilisation. Dans le cas contraire, il n'est pas possible d'effectuer de téléchargement.

Le total des appareils pour lesquels l'option **Maintenir la connexion au Serveur &d'administration** a été sélectionnée ne peut être supérieur à 300.

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.

Le fichier avec les informations est téléchargé à l'emplacement indiqué.

Téléchargement des journaux des événements

Vous pouvez télécharger les journaux d'événements sur votre appareil à partir d'un appareil client uniquement si l'une des conditions suivantes est remplie : l'option **Maintenir la connexion au Serveur d'administration** est activée dans les paramètres de l'appareil, un serveur push ou une passerelle de connexion est en cours d'utilisation. Dans le cas contraire, il n'est pas possible d'effectuer de téléchargement.

Le total des appareils pour lesquels l'option **Maintenir la connexion au Serveur &d'administration** a été sélectionnée ne peut être supérieur à 300.

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.

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.

Exécution du diagnostic à distance d'une application et téléchargement des résultats

Pour lancer le diagnostic de l'application sur l'appareil distant 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 l'application pour laquelle vous souhaitez exécuter un diagnostic à distance.

   La liste des options de diagnostic à distance s'ouvre.
4. Dans la section **Rapport de diagnostic**, cliquez sur le bouton **Poser le diagnostic**.

   Cette action permet de lancer le processus de diagnostic à distance et de générer un rapport de diagnostic. Le processus de diagnostic est terminé, le bouton **Télécharger le rapport des diagnostics** devient accessible.

5. Cliquez sur le bouton **Télécharger le rapport des diagnostics** pour télécharger le rapport.

Le rapport est téléchargé à l'emplacement indiqué.

Exécution d'une application sur un appareil client

Vous devrez peut-être exécuter une application sur l'appareil client si un expert du support Kaspersky vous le demande. Vous n'avez pas besoin d'installer l'application sur cet appareil.

Pour exécuter une application sur l'appareil client, procédez comme suit :

1. Ouvrez la fenêtre de diagnostic à distance d'un l'appareil client.
2. Dans la fenêtre de diagnostic à distance, sélectionnez l'onglet **Exécution d'une application à distance**.
3. Dans le 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 dans le dossier que vous souhaitez exécuter sur l'appareil client. 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. Dans le groupe **Exécution d'une application à distance**, cliquez sur le bouton **Charger** afin de sélectionner une archive ZIP contenant l'application que vous souhaitez exécuter sur l'appareil client.
7. Cliquez sur le bouton **Charger et exécuter** pour lancer l'application indiquée sur l'appareil client.
8. 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.

Génération d'un fichier dump pour une application

Le fichier de sauvegarde de l'application vous permet de consulter les paramètres de l'application exécutée sur l'appareil client à un moment donné. Ce fichier contient également des informations sur les modules chargés pour une application.

La génération de fichiers de vidage est disponible uniquement pour les processus 32 bits s'exécutant sur les appareils clients Windows. Pour les appareils clients exécutant Linux et pour les processus 64 bits, cette fonctionnalité n'est pas prise en charge.

Pour créer un fichier de vidage pour une application :

1. Ouvrez la fenêtre de diagnostic à distance d'un l'appareil client.
2. Dans la fenêtre de diagnostic à distance, sélectionnez l'onglet **Exécution d'une application à distance**.
3. Dans la section **Génération du fichier dump du processus**, indiquez le fichier exécutable de l'application pour lequel vous souhaitez générer le fichier dump.
4. Cliquez sur le bouton **Télécharger** afin d'enregistrer le fichier de vidage pour l'application indiquée.

   Si l'application indiquée n'est pas en cours d'exécution sur l'appareil client, le message d'erreur s'affiche.

Exécution de diagnostics à distance sur un appareil client basé sur Linux

Kaspersky Security Center Cloud Console vous permet de télécharger les informations de diagnostic de base à partir d'un appareil client. Vous pouvez également obtenir les informations de diagnostic sur un appareil basé sur Linux à l'aide du script collect.sh de Kaspersky. Ce script est exécuté sur l'appareil client Linux qui doit être diagnostiqué, puis génère un fichier contenant les informations de diagnostic, les informations système sur cet appareil, les fichiers de traçage des applications, les journaux de l'appareil et un fichier de vidage pour les applications terminées en urgence.

Nous vous recommandons d'utiliser le script collect.sh pour obtenir simultanément toutes les informations de diagnostic sur l'appareil client Linux. Si vous téléchargez les informations de diagnostic à distance via Kaspersky Security Center Cloud Console, 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.

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

Cette section fournit un scénario de configuration de l'exportation d'événements du Serveur d'administration vers des systèmes SIEM externes. L'exportation des informations relatives aux événements vers des systèmes SIEM externes permet à l'administrateur des systèmes SIEM de réagir efficacement aux événements du système de sécurité survenus sur un appareil administré ou dans les groupes d'appareils.

Prérequis

Avant de lancer l'exportation de la configuration des événements dans Kaspersky Security Center Cloud Console :

- En savoir plus sur les méthodes d'export d'événements.
- Assurez-vous de connaître les valeurs des paramètres système.

Vous pouvez exécuter les étapes de ce scénario dans n'importe quel ordre.

Étapes

Le processus d'exportation des événements vers un système SIEM comprend les étapes suivantes :

- **Configuration du système SIEM pour recevoir les événements de Kaspersky Security Center Cloud Console**

  Vous devez configurer la réception des événements de Kaspersky Security Center Cloud Console dans le système SIEM.

- **Marquage d'événements à exporter**

  Vous devez marquer 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. De plus, vous pouvez marquer les événements pour des applications Kaspersky administrées spécifiques.

- **Configuration de Kaspersky Security Center Cloud Console pour l'exportation des événements vers le système SIEM**

  Vous devez configurer Kaspersky Security Center Cloud Console pour commencer à exporter des événements vers un système SIEM.

Résultats

Après avoir configuré l'exportation des événements vers un système SIEM, vous pouvez afficher exporter les résultats si vous avez sélectionné des événements que vous souhaitez exporter.

Conditions préalables

Dans le cadre de la configuration de l'exportation automatique des événements dans Kaspersky Security Center Cloud Console, 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 Cloud Console.

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 la connexion entre Kaspersky Security Center Cloud Console et le serveur du système SIEM. Il faut définir cette valeur dans les paramètres de Kaspersky Security Center Cloud Console et les paramètres du récepteur du système SIEM.

- **Protocole**

  Le protocole utilisé pour la transmission des messages depuis Kaspersky Security Center Cloud Console vers le système SIEM. Il faut définir cette valeur dans les paramètres de Kaspersky Security Center Cloud Console et les paramètres du récepteur du système SIEM.

À propos de l'exportation des événements

Kaspersky Security Center Cloud Console 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 alertes 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 Cloud Console vers les systèmes SIEM fait intervenir deux parties : l'expéditeur des événements (Kaspersky Security Center Cloud Console), 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 la Kaspersky Security Center Cloud Console. L'ordre des configurations n'a pas d'importance : Vous pouvez soit choisir de commencer par configurer l'envoi des événements à la Kaspersky Security Center Cloud Console, puis configurer leur réception par le système SIEM, soit l'inverse.

Format Syslog d'exportation d'événements

Vous pouvez envoyer des événements au format Syslog vers n'importe quel système SIEM. Le protocole Syslog permet de transmettre n'importe quel événement survenu sur le Serveur d'administration et dans les applications de Kaspersky installées sur les appareils administrés. Lors de l'exportation des événements au format Syslog vous pouvez choisir exactement les événements qu'il faut transmettre au système SIEM.

Réception des événements par le système SIEM

Le système SIEM doit accepter et analyser correctement les événements en provenance de Kaspersky Security Center Cloud Console. Il faut pour cela configurer le système SIEM. La configuration dépend du système SIEM utilisé en particulier. Toutefois, il existe une série d'étapes communes à l'ensemble des systèmes SIEM : la configuration du récepteur et de l'analyseur.

Configuration de l'export d'événements dans le système SIEM

La procédure d'exportation des événements de Kaspersky Security Center Cloud Console vers les systèmes SIEM fait intervenir deux parties : l'expéditeur des événements (Kaspersky Security Center Cloud Console), et le destinataire de ceux-ci (le système SIEM). Il est nécessaire de configurer l'exportation dans le système SIEM utilisé et dans Kaspersky Security Center Cloud Console.

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 Cloud Console. En général, il faut définir les paramètres suivants dans le système SIEM :

- **Port**

  Indiquez le numéro de port pour vous connecter à Kaspersky Security Center Cloud Console. Il est nécessaire d'indiquer le même numéro de port que celui qui a été choisi dans Kaspersky Security Center Cloud Console lors de la configuration avec un système SIEM.

- **Protocole de transfert de messages ou type de données sortantes**

  Spécifiez le format Syslog.

En fonction du système SIEM utilisé, vous devrez peut-être définir des paramètres avancés pour le récepteur de messages.

Analyseur des messages

Les événements exportés sont transmis au systèmes SIEM sous la forme de messages. Ces messages sont ensuite soumis à l'analyseur afin que les informations relatives aux événements soient transmises correctement au système SIEM. L'analyseur des messages est inséré au système SIEM il permet de décomposer le message en ses champs comme l'identifiant du message, le niveau de gravité, la description et d'autres paramètres. Le système SIEM peut ainsi traiter les événements envoyés par Kaspersky Security Center Cloud Console afin qu'ils soient enregistrés dans la base de données du système SIEM.

Marquage des événements pour l'export vers les systèmes SIEM au format Syslog

Une fois que l'exportation automatique des événements a été activée, il faut sélectionner les événements à exporter dans le système SIEM externe.

Vous pouvez configurer l'exportation des événements au format Syslog dans le système externe selon une des conditions suivantes :

- Marquage d'événements généraux. Si vous marquez des événements à exporter dans une stratégie, dans les paramètres d'un événement ou dans les paramètres du Serveur d'administration, le système SIEM recevra les événements marqués qui se sont produits dans toutes les applications administrées par la stratégie spécifique. Si des événements à exporter ont été choisis dans la stratégie, vous ne serez pas en mesure de les redéfinir pour une application distincte administrée par cette stratégie.

- Marquage des événements pour une application administrée. Si vous marquez les événements à exporter pour une application administrée installée sur un appareil administré, le système SIEM reçoit uniquement les événements survenus dans cette application.

Marquage des événements d'une application Kaspersky pour l'exportation au format Syslog

Si vous souhaitez exporter des événements qui se sont produits dans une application administrée spécifique installée sur les appareils administrés, marquez les événements à exporter dans la stratégie de l'application. Dans ce cas, les événements marqués sont exportés depuis tous les appareils inclus dans la zone de la stratégie.

Pour marquer les événements à exporter pour une application administrée spécifique, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Stratégies et profils**.

2. Cliquez sur la stratégie de l'application pour laquelle vous souhaitez marquer des événements.

   La fenêtre des paramètres de la stratégie s'ouvre.

3. Passez à la section **Configuration des événements**.

4. Cochez la case en regard des événements que vous souhaitez exporter dans un système SIEM.

5. Cliquez sur le bouton **Marquer pour l'exportation vers le système SIEM en utilisant Syslog**.

   Vous pouvez aussi marquer un événement pour l'exporter vers le système SIEM dans la section **Enregistrement des événements**, qui s'ouvre en cliquant sur le lien de l'événement.

6. Une coche (✓) s'affiche dans la colonne **Syslog** de l'événement ou des événements que vous avez marqués pour l'exportation vers le système SIEM.

7. Cliquez sur le bouton **Enregistrer**.

Les événements marqués de l'application administrée sont prêts à être exportés vers un système SIEM.

Vous pouvez marquer les événements à exporter vers un système SIEM pour un appareil administré spécifique. Si des événements précédemment exportés ont été marqués dans une stratégie de l'application, vous ne pourrez pas redéfinir les événements marqués pour un appareil administré.

Pour marquer les événements à exporter pour un appareil administré, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Appareils administrés**.

   La liste des appareils administrés s'affiche.

2. Cliquez sur le lien avec le nom de l'appareil requis dans la liste des appareils administrés.

   La fenêtre des propriétés de l'appareil sélectionné s'affiche.

3. Accédez à la section **Applications**.

4. Cliquez sur le lien avec le nom de l'application requise dans la liste des applications.

5. Passez à la section **Configuration des événements**.

6. Cochez la case en regard des événements que vous souhaitez exporter dans un système SIEM.

7. Cliquez sur le bouton **Marquer pour l'exportation vers le système SIEM en utilisant Syslog**.

   En outre, vous pouvez marquer un événement pour l'exporter vers le système SIEM dans la section **Enregistrement des événements**, qui s'ouvre en cliquant sur le lien de l'événement.

8. Une coche (✓) s'affiche dans la colonne **Syslog** de l'événement ou des événements que vous avez marqués pour l'exportation vers le système SIEM.

Désormais, le Serveur d'administration envoie au système SIEM les événements marqués si l'exportation vers le système SIEM est configurée.

Marquage d'événements généraux pour l'exportation au format Syslog

Vous pouvez marquer les événements généraux que le Serveur d'administration exportera vers les systèmes SIEM en utilisant le format Syslog.

Pour marquer des événements généraux à exporter vers un système SIEM, procédez comme suit :

1. Exécutez une des actions suivantes :

   - Dans le menu principal, cliquez sur l'icône des paramètres (⚙) en regard du nom du Serveur d'administration requis.

- Dans le menu principal, accédez à **Ressources (Appareils)** → **Stratégies et profils**, puis cliquez sur le lien d'une stratégie.

2. Dans la fenêtre qui s'ouvre, sélectionnez l'onglet **Configuration des événements**.

3. Cliquez sur **Marquer pour l'exportation vers le système SIEM en utilisant Syslog**.

   En outre, vous pouvez marquer un événement pour l'exporter vers le système SIEM dans la section **Enregistrement des événements**, qui s'ouvre en cliquant sur le lien de l'événement.

4. Une coche (✓) s'affiche dans la colonne **Syslog** de l'événement ou des événements que vous avez marqués pour l'exportation vers le système SIEM.

Désormais, le Serveur d'administration envoie au système SIEM les événements marqués si l'exportation vers le système SIEM est configurée.

À propos de l'exportation des événements via le format Syslog

Le format Syslog permet d'exporter dans les systèmes SIEM les événements survenus sur le Serveur d'administration et dans d'autres applications de Kaspersky installées sur les appareils administrés.

Syslog est un protocole standard d'enregistrement des messages. Ce protocole permet de distinguer le logiciel qui génère les messages, le système dans lequel les messages sont enregistrés et le logiciel qui analyse les messages et génère les rapports. Chaque message reçoit un code d'appareil qui indique le type de logiciel qui a permis de créer le message et le niveau de gravité.

Le format Syslog est défini par les documents Request for Comments, RFC, publié par l'Internet Engineering Task Force (standards Internet). Le standard RFC 5424 est le standard utilisé pour exporter les événements de Kaspersky Security Center Cloud Console vers les systèmes externes.

Il est possible de configurer l'exportation des événements vers des systèmes externes via le format Syslog dans Kaspersky Security Center Cloud Console.

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 Cloud Console de telle sorte que les événements soient envoyés au système SIEM. L'envoi des événements de Kaspersky Security Center Cloud Console 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 Cloud Console 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 Cloud Console.

Pour configurer l'exportation vers les systèmes SIEM dans Kaspersky Security Center Cloud Console :

1. Dans le menu principal, cliquez sur l'icône des paramètres ( ) en regard du nom du Serveur d'administration requis.

   La fenêtre des propriétés du Serveur d'administration s'ouvre.

2. Sous l'onglet **Général**, sélectionnez la section **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 la connexion entre Kaspersky Security Center Cloud Console et le serveur du système SIEM. Il faut définir cette valeur dans les paramètres de Kaspersky Security Center Cloud Console et les paramètres du récepteur du système SIEM.

   - Protocole

Vous ne pouvez utiliser que le protocole TLS par TCP pour transférer des messages vers le système SIEM. Pour ce faire, indiquez les paramètres TLS :

- **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 Cloud Console. Kaspersky Security Center Cloud Console vérifie si la chaîne de certificat du serveur du système SIEM est également signée 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 Cloud Console. 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 Cloud Console. Ainsi, vous utiliserez un certificat auto-signé délivré par Kaspersky Security Center Cloud Console. 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 Cloud Console 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 des sujets spécifiés correspond au nom du sujet du certificat du système SIEM, Kaspersky Security Center Cloud Console 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 Cloud Console.

  - **Insérer le certificat**. Vous pouvez utiliser un certificat que vous avez reçu de n'importe quelle source, par exemple, de n'importe quelle autorité de certification de confiance. Vous devez spécifier le certificat et sa clé privée en utilisant l'un des types de certificats suivants :

    - **Certificat X.509 PEM**. Téléchargez un fichier avec un certificat dans le champ **Fichier avec certificat** et un fichier avec une clé privée dans le champ **Fichier avec clé**. Les deux fichiers ne dépendent pas l'un de l'autre, et l'ordre de chargement des fichiers est sans importance. Lorsque les deux fichiers sont téléchargés, indiquez le mot de passe pour le décodage de la clé privée dans le champ **Vérification du mot de passe ou du certificat**. Le mot de passe peut présenter une valeur vide si la clé privée n'est pas encodée.

    - **Certificat X.509 PKCS12**. Téléchargez un seul fichier qui contient un certificat et sa clé privée dans le champ **Fichier avec certificat**. Lors du téléchargement du fichier, indiquez le mot de passe pour le décodage de la clé privée dans le champ **Vérification du mot de passe ou du certificat**. Le mot de passe peut présenter une valeur vide si la clé privée n'est pas encodée.

- **Générer une clé**. Vous pouvez générer un certificat auto-signé dans Kaspersky Security Center Cloud Console. Par conséquent, Kaspersky Security Center Cloud Console stocke le certificat auto-signé généré, et vous pouvez transmettre la partie publique du certificat ou l'empreinte SHA1 au système SIEM.

5. Si vous le souhaitez, vous pouvez exporter des événements archivés à partir de la base de données du Serveur d'administration et définir la date de début à partir de laquelle vous souhaitez lancer l'exportation des événements archivés :

   a. Cliquez sur le lien **Définir la date de début de l'exportation**.

   b. Dans la section qui s'ouvre, indiquez la date de début dans le champ **Date de début de l'exportation**.

   c. Cliquez sur le bouton **OK**.

6. Basculez l'option en position **Exporter automatiquement les événements dans la base du système SIEM Activé**.

7. Pour vérifier que la connexion au système SIEM a été configurée, cliquez sur le bouton **Analyser la connexion**.

   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.

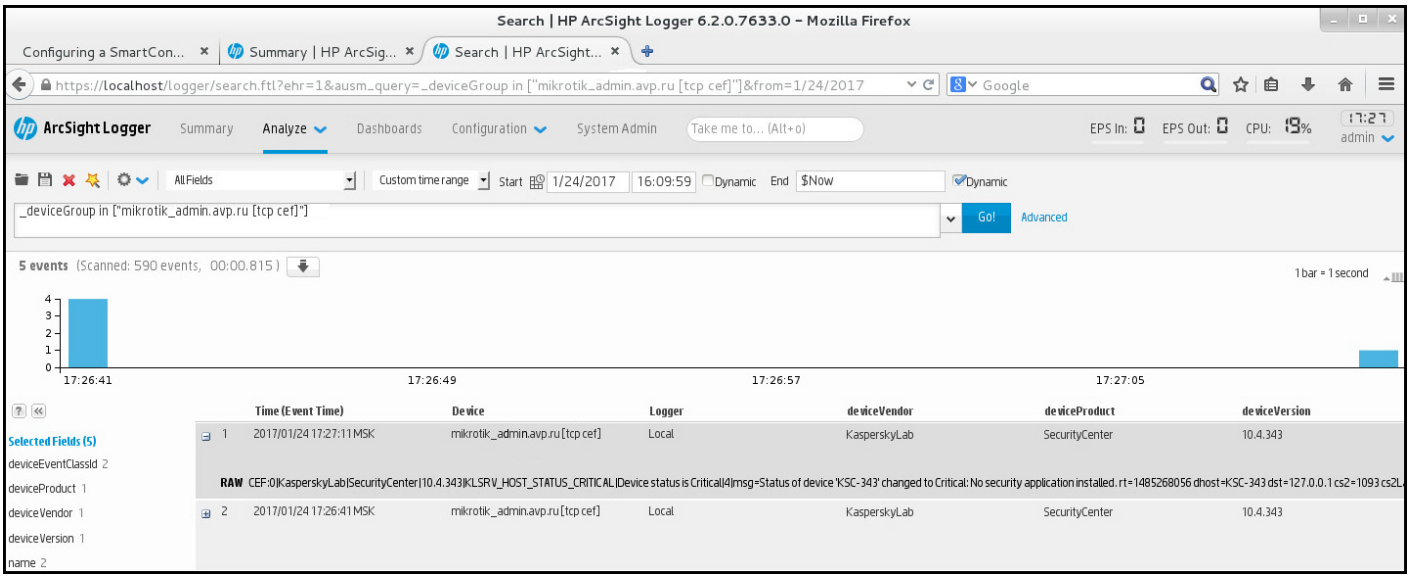
Consultation des résultats de l'exportation

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 Cloud Console 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 Cloud Console 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

Guide de démarrage rapide pour les fournisseurs de services gérés (MSP)

Ce guide de démarrage rapide est destiné aux administrateurs de prestataires de services gérés (MSP).

Kaspersky Security Center Cloud Console prend en charge l'architecture en multilocation. Le guide contient des conseils et des meilleures pratiques pour gérer les comptes de vos clients (locataires) et installer des applications de sécurité sur leurs appareils.

À propos de Kaspersky Security Center Cloud Console

Kaspersky Security Center Cloud Console est une application hébergée et maintenue par Kaspersky. Vous n'avez pas besoin d'installer Kaspersky Security Center Cloud Console sur votre ordinateur ou votre serveur. Kaspersky Security Center Cloud Console permet à l'administrateur d'installer des applications de sécurité 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. L'administrateur peut 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.

Fonctionnalités principales de Kaspersky Security Center Cloud Console

Kaspersky Security Center Cloud Console vous permet d'effectuer les opérations suivantes :

- Installer des applications de Kaspersky sur les appareils de votre réseau et administrer les applications installées.
- Former une hiérarchie des groupes d'administration pour administrer les appareils (les appareils clients et les machines virtuelles) comme un ensemble.
- Créez des serveurs d'administration virtuels et organisez-les dans une hiérarchie.
- Protégez vos appareils réseau, y compris les postes de travail et les serveurs :
  - Administrer le système de protection anti-malware fondé sur les applications de Kaspersky.
  - Utilisez les fonctionnalités de détection et de réponse (EDR et MDR) (une licence pour Kaspersky Endpoint Detection and Response et/ou pour Kaspersky Managed Detection and Response est requise), notamment :
    - Enquêter sur les incidents et les analyser
    - Visualisation des incidents par la création d'un graphique de la chaîne de développement des menaces
    - Accepter ou rejeter les réponses manuellement ou configurer l'acceptation automatique de toutes les réponses
- Utiliser Kaspersky Security Center Cloud Console comme application multi-locataire.
- Administrer à distance les applications de Kaspersky installées sur les appareils clients.
- Effectuer un déploiement centralisé des clés de licence pour les applications Kaspersky sur les appareils client.
- Créer et gérer des stratégies de sécurité pour les appareils de votre réseau.

- Créer et gérer des comptes utilisateurs.
- Créer et gérer des rôles d'utilisateur (RBAC).
- Créer et administrer les tâches pour les applications installées sur vos appareils dans le réseau.
- Affichez les rapports sur l'état du système de sécurité pour chaque entreprise cliente individuellement.

À propos des licences de Kaspersky Security Center Cloud Console pour MSP

Lorsque vous commencez à utiliser Kaspersky Security Center Cloud Console, vous pouvez soit demander d'utiliser un espace de travail d'essai (dans ce cas, vous bénéficiez d'une licence d'évaluation de 30 jours intégrée à votre espace de travail), soit saisir un code d'activation pour une licence commerciale.

Il est impossible de convertir un espace de travail d'essai en un espace commercial. Pour continuer à utiliser Kaspersky Security Center Cloud Console après l'expiration de la durée de validité de la licence d'évaluation, vous devez supprimer l'espace de travail d'essai et en créer un autre avec une licence commerciale.

Plus tard, vous allez pouvoir ajouter une ou plusieurs clés de licences commerciales au stockage du Serveur d'administration.

À propos des capacités de Detection and Response pour MSPs

Kaspersky Security Center Cloud Console peut intégrer des fonctionnalités d'autres applications Kaspersky à l'interface de la console. Par exemple, vous pouvez ajouter les fonctionnalités de Detection and Response aux fonctionnalités de Kaspersky Security Center Cloud Console en intégrant les applications suivantes :

- Kaspersky Endpoint Detection and Response Optimum

  Kaspersky Endpoint Detection and Response Optimum est une solution conçue pour protéger l'infrastructure informatique d'une organisation contre les cybermenaces complexes. La fonctionnalité de la solution combine la détection automatique des menaces avec la capacité de répondre à ces menaces pour résister aux attaques complexes, y compris les nouveaux exploits, les ransomwares, les attaques sans fichier et les méthodes qui utilisent des outils système légitimes.

  Lorsqu'une application Kaspersky Endpoint Protection Platform (EPP) détecte un incident de sécurité, une carte détaillée contenant des données importantes sur l'incident de sécurité est générée dans Kaspersky Security Center Cloud Console. La carte d'incident est générée par l'une des applications suivantes :

  - Kaspersky Endpoint Agent installé avec une application Kaspersky EPP
  - Kaspersky Endpoint Security 11.7.0 for Windows ou suivant qui intègre la fonctionnalité EDR Optimum et ne nécessite pas d'installation supplémentaire de Kaspersky Endpoint Agent

  La fiche d'incident vous permet d'analyser et d'enquêter sur l'incident. Vous pouvez également visualiser l'incident en créant un graphique de la chaîne de développement des menaces. Le graphique décrit les étapes de déploiement de l'attaque détectée dans la durée. Le graphique créé comprend des informations sur les modules impliqués dans l'attaque et les actions effectuées par ces modules.

Vous pouvez également initier une chaîne d'actions de réponse : créer une règle de prévention d'exécution pour un objet non approuvé ; rechercher des incidents similaires dans le groupe d'appareils, sur la base des indicateurs de compromission sélectionnés (IOC) ; isoler un objet non fiable ; isoler un appareil compromis du réseau.

Pour plus d'informations sur l'activation de l'application, consultez la documentation de Kaspersky Endpoint Detection and Response Optimum.

Si elle est intégrée, cette application ajoute la section **Alertes** à l'interface de Kaspersky Security Center Cloud Console (**Surveillance et rapports** → **Alertes**).

- Kaspersky Managed Detection and Response

  Kaspersky Managed Detection and Response offre une protection 24 heures sur 24 contre le volume croissant de menaces qui contournent les barrières de sécurité automatisées aux organisations qui ont du mal à trouver l'expertise et le personnel, ou à celles dont les ressources internes sont limitées. Les analystes MDR SOC de Kaspersky ou d'une entreprise tierce enquêtent sur les incidents et proposent des réponses pour résoudre les incidents. Vous pouvez accepter ou rejeter les mesures proposées manuellement, ou activer l'option d'acceptation automatique de toutes les réponses.

  Pour plus d'informations sur l'activation de l'application, consultez la documentation de Kaspersky Managed Detection and Response.

  Si elle est intégrée, cette application ajoute la section **Incidents** à l'interface de Kaspersky Security Center Cloud Console (**Surveillance et rapports** → **Incidents**).

Vous pouvez afficher ou masquer les éléments de l'interface faisant référence aux fonctionnalités de Kaspersky Endpoint Detection and Response ou Kaspersky Managed Detection and Response à tout moment dans la section **Options d'interface** de Kaspersky Security Center Cloud Console.

Prise en main de Kaspersky Security Center Cloud Console

Une fois que le scénario de cette section est terminé, Kaspersky Security Center Cloud Console est prêt à l'emploi.

Scénario de prise en main

Le scénario se déroule par étapes :

1. **Créez un compte.**

   Pour commencer à utiliser Kaspersky Security Center Cloud Console, vous avez besoin d'un compte.

   Pour créer un compte utilisateur :

   1. Ouvrez votre navigateur et saisissez l'adresse suivante : https://ksc.kaspersky.com.
   2. Cliquez sur le bouton **Créer un compte**.
   3. Suivez les instructions à l'écran.

2. **Créez un espace de travail.**

   Après avoir créé le compte, vous pouvez enregistrer votre entreprise et créer votre espace de travail.

   Lorsque vous commencez à utiliser Kaspersky Security Center Cloud Console, vous pouvez soit demander d'utiliser un espace de travail d'essai (dans ce cas, vous bénéficiez d'une licence d'évaluation de 30 jours intégrée à votre espace de travail), soit saisir un code d'activation pour une licence commerciale.

Il est impossible de convertir un espace de travail d'essai en un espace commercial. Pour continuer à utiliser Kaspersky Security Center Cloud Console après l'expiration de la durée de validité de la licence d'évaluation, vous devez supprimer l'espace de travail d'essai et en créer un autre avec une licence commerciale.

Pour enregistrer une entreprise et créer un espace de travail, procédez comme suit :

1. Ouvrez votre navigateur et saisissez l'adresse suivante : https://ksc.kaspersky.com.
2. Cliquez sur le bouton **S'identifier**.
3. Suivez les instructions indiquées à l'écran.

3. **Réalisez la configuration initiale de Kaspersky Security Center Cloud Console.**

   Lorsque vous vous connectez pour la première fois à l'espace de travail créé, vous êtes automatiquement invité à exécuter l'assistant de démarrage rapide de l'application. L'assistant de configuration initiale de l'application vous guide pour créer un nombre minimum de tâches et de stratégies nécessaires, pour configurer un minimum de paramètres et pour commencer à créer des paquets d'installation pour les applications Kaspersky. Suivez les instructions indiquées à l'écran.

Une fois la configuration initiale terminée, Kaspersky Security Center Cloud Console est prêt à l'emploi.

Recommandations sur la gestion des appareils de vos clients

Cette section contient des recommandations pour organiser les appareils clients à protéger.

Les recommandations varient selon que vous utilisez Kaspersky Security Center pour la première fois ou que vous avez déjà utilisé la version sur site :

- Si vous n'avez jamais utilisé Kaspersky Security Center, vous avez deux possibilités :
  - Créer un serveur d'administration virtuel pour les appareils de chaque client (option recommandée). Dans ce cas, les appareils de chaque client peuvent être administrés via un Serveur d'administration virtuel dédié indépendamment des autres clients. En même temps, vous pouvez utiliser le serveur d'administration principal pour créer des stratégies et des tâches communes pour tous les clients. Les rapports générés sur le Serveur d'administration principal peuvent inclure des données de tous les Serveurs d'administration virtuels.
  - Créer un groupe d'administration pour les appareils de chaque client. Si vous souhaitez diviser davantage les appareils clients, vous pouvez créer une hiérarchie de groupes d'administration subordonnés sous chaque groupe parent. Par exemple, vous pouvez avoir besoin de groupes subordonnés si vous souhaitez utiliser différents paramètres de protection pour les appareils des employés travaillant dans différents départements.
- Si vous avez déjà utilisé Kaspersky Security Center sur site, vous pouvez migrer vos groupes d'administration existants et les objets associés de Kaspersky Security Center sur site vers Kaspersky Security Center Cloud Console.

  Il n'est pas possible de migrer les Serveurs d'administration virtuels. Après la migration des groupes d'administration et autres objets, vous pouvez créer des serveurs d'administration virtuels dans la Kaspersky Security Center Cloud Console.

  Passez à la configuration de la migration.

L'administrateur d'un Serveur d'administration virtuel ne peut accéder à ce Serveur virtuel qu'à partir du Serveur d'administration principal. Tous les objets créés sur le Serveur d'administration principal sont disponibles en lecture pour l'administrateur d'un Serveur d'administration virtuel (par exemple, les widgets, les rapports ou les rôles utilisateurs).

Schéma de déploiement typique pour les MSP

Cette section fournit une description du schéma de déploiement généralement utilisé par les MSP pour gérer plusieurs locataires. Le schéma est basé sur une gestion via des serveurs d'administration virtuels créés individuellement pour chaque locataire.

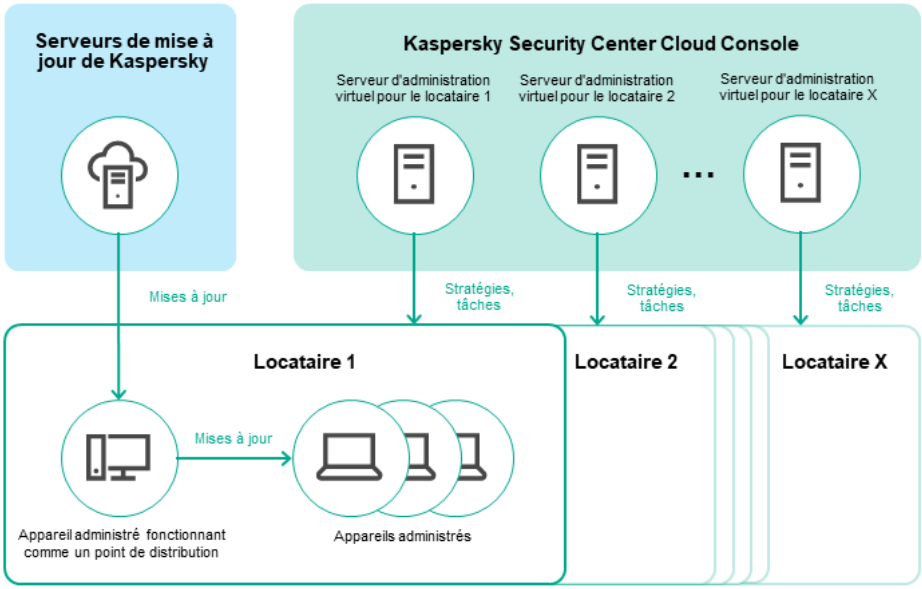


Schéma de déploiement typique pour les MSP

Le schéma comprend les principaux éléments suivants :

- *Kaspersky Security Center Cloud Console*. fournit une interface utilisateur aux services d'administration de votre espace de travail. Nous nous servons de Kaspersky Security Center Cloud Console pour le déploiement, l'administration et la maintenance du système de protection du réseau de l'entreprise cliente.
- *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 d'administration virtuels*. Un administrateur MSP crée généralement un serveur d'administration virtuel pour permettre à chaque locataire de déployer, administrer et assurer la maintenance du système de protection du réseau de l'entreprise cliente correspondante.
- *Locataires*. Entreprises clientes dont les appareils doivent être protégés.
- *Appareils administrés*. Appareils de l'entreprise cliente protégés à l'aide de Kaspersky Security Center Cloud Console. L'une des applications de sécurité Kaspersky et un Agent d'administration doivent être installés sur chacun des appareils à protéger.
- *Appareil administré fonctionnant comme un point de distribution*. Ordinateur avec un Agent d'administration installé, utilisé pour la diffusion des mises à jour, le sondage du réseau, l'installation à distance des applications, la collecte d'informations sur les ordinateurs faisant partie du groupe d'administration et/ou d'un domaine multidiffusion. L'administrateur sélectionne les appareils appropriés et leur attribue manuellement des points de distribution.

Scénario : déploiement de la protection (gestion des locataires via des serveurs d'administration virtuels)

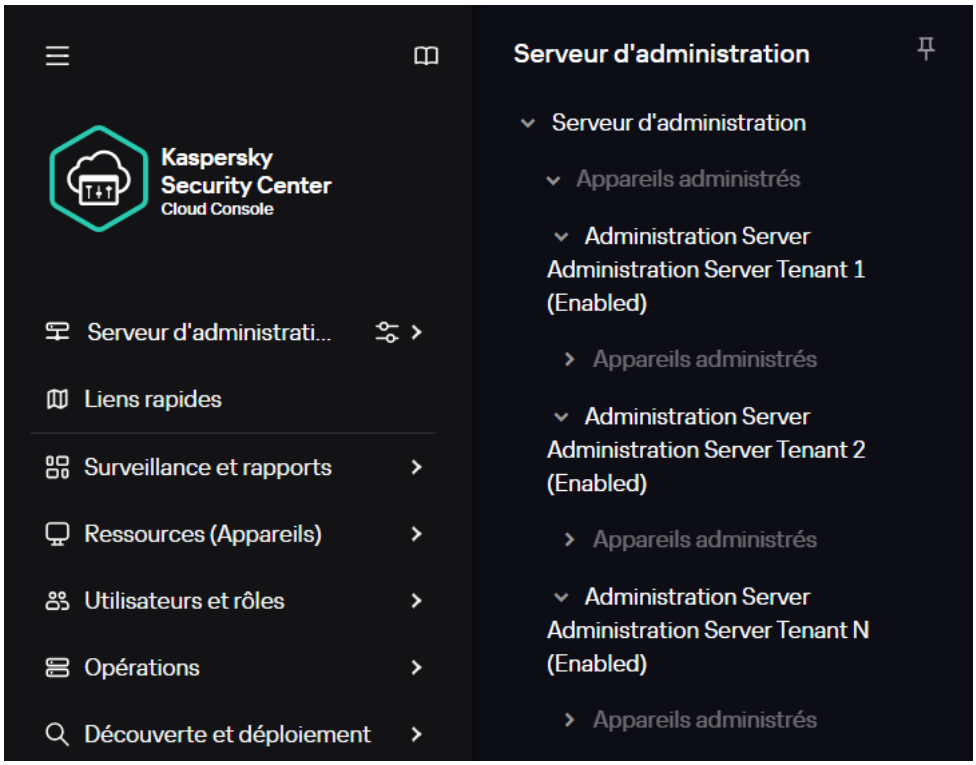
Si vous n'avez jamais utilisé Kaspersky Security Center et que vous souhaitez administrer vos locataires via des serveurs d'administration virtuels, procédez comme indiqué dans cette section. Une fois ce scénario terminé, les appareils de vos clients seront protégés.

Si vous gérez plusieurs locataires, exécutez le scénario pour chacun des locataires séparément.

Le scénario se déroule par étapes :

1. **Création d'un Serveur d'administration virtuel**

   Créer un serveur d'administration virtuel pour votre client. Le nouveau Serveur d'administration virtuel s'affiche dans la hiérarchie des Serveurs d'administration :



   Serveurs d'administration virtuels dans la hiérarchie des Serveurs d'administration

2. **Sélection d'un appareil qui va jouer le rôle de point de distribution**

   Parmi les appareils de chaque client, choisissez l'appareil qui servira du point de distribution.

   > Il est impossible d'avoir plus de 100 points de distribution dans un espace de travail.

3. **Création d'un paquet d'installation autonome pour l'Agent d'administration**

   Basculez vers le Serveur d'administration virtuel créé, puis créez un paquet d'installation autonome pour l'Agent d'administration. Vous pouvez changer de Serveur d'administration dans le menu principal en cliquant sur l'icône en forme de chevron (›) à droite du nom actuel du Serveur d'administration, puis en sélectionnant le Serveur d'administration voulu. Lors de la création du paquet d'installation autonome, spécifiez le groupe d'administration des appareils administrés vers lequel déplacer l'appareil.

4. **Installation de l'Agent d'administration sur l'appareil sélectionné pour qu'il serve de point de distribution**

Vous pouvez utiliser n'importe quelle méthode qui vous convient :

- Installation manuelle

  Pour transmettre le paquet d'installation autonome à l'appareil, vous pouvez, par exemple, le copier sur un disque amovible (une clé USB, par exemple), ou bien le placer dans un dossier partagé.

- Déploiement à l'aide d'Active Directory

- Déploiement à l'aide de votre solution logicielle de surveillance et de gestion à distance (RMM)

5. **Attribuer un point de distribution**

   Affectation de l'appareil avec l'Agent d'administration installé en tant que point de distribution.

6. **Sondage réseau**

   Configuration et exécution d'un sondage réseau via le point de distribution.

   Kaspersky Security Center Cloud Console fournit les méthodes suivantes pour effectuer le sondage du réseau :

   - Sondage des plages IP
   - Sondage du réseau Windows
   - Sondage Active Directory

   Une fois le sondage du réseau selon la planification terminé, les appareils de vos clients sont détectés et placés dans le groupe **Appareils non définis**.

7. **Déplacement des appareils détectés vers les groupes d'administration**

   Configurez les règles pour automatiquement déplacer les appareils découverts dans les groupes d'administration requis ; ou déplacez ces appareils manuellement dans groupes d'administration requis. Si vous prévoyez de gérer les appareils du client dans un seul groupe d'administration, vous pouvez déplacer les appareils vers le groupe Appareils administrés.

8. **Création de paquets d'installation pour l'Agent d'administration et les applications Kaspersky administrées**

   Création de paquets d'installation pour les applications Kaspersky.

9. **Remplacement des applications de sécurité d'éditeurs tiers**

   Si des applications de sécurité tierces sont installées sur les appareils de vos clients, supprimez-les avant l'installation des applications Kaspersky.

10. **Installation d'applications Kaspersky sur des appareils clients**

    Créez des tâches d'installation à distance pour installer l'Agent d'administration et les applications Kaspersky administrées sur les appareils de vos clients.

    Si nécessaire, vous pouvez créer plusieurs tâches d'installation à distance pour installer des applications Kaspersky administrées pour différents groupes d'administration ou différentes sélections d'appareils.

    Une fois les tâches créées, vous pouvez configurer leurs paramètres. Assurez-vous que la programmation pour chaque tâche répond à vos exigences. Tout d'abord, la tâche pour installer l'Agent d'administration doit être exécutée. Une fois l'Agent d'administration installé sur les appareils de vos clients, vous devez exécuter la tâche d'installation des applications Kaspersky administrées.

11. **Vérification du déploiement initial des applications Kaspersky**

    Générer et afficher le **Rapport sur les versions de l'application Kaspersky**. Assurez-vous que les applications Kaspersky administrées sont installées sur tous les appareils client.

12. **Création des stratégies pour les applications Kaspersky**

    Créez une stratégie pour l'application Kaspersky requise. Si vous souhaitez créer une stratégie universelle pour tous vos clients, basculez le Serveur d'administration virtuel actuel vers le Serveur d'administration principal, puis créez une stratégie pour l'application Kaspersky requise.

Scénario : déploiement de la protection (gestion des locataires via des groupes d'administration)

Si vous n'avez jamais utilisé Kaspersky Security Center et que vous souhaitez gérer vos locataires via des groupes d'administration, procédez comme décrit dans cette section. Une fois ce scénario terminé, les appareils de vos clients seront protégés.

Le scénario se déroule par étapes :

1. **Création des groupes d'administration**

   Créez un groupe d'administration pour chacun de vos clients.

2. **Planification de la structure des points de distribution**

   Parmi les appareils de chaque client, choisissez l'appareil qui servira de point de distribution.

   > Il est impossible d'avoir plus de 100 points de distribution dans un espace de travail.

3. **Création d'un paquet d'installation autonome pour l'Agent d'administration**

   Créez un paquet d'installation autonome pour l'Agent d'administration.

4. **Installation de l'Agent d'administration sur les appareils sélectionnés pour qu'il serve de point de distribution.**

   Installation de l'Agent d'administration sur les appareils sélectionnés pour qu'ils servent de points de distribution.

   Vous pouvez utiliser n'importe quelle méthode qui vous convient :

   - Installation manuelle

     Pour fournir le paquet d'installation autonome aux appareils, vous pouvez, par exemple, le copier sur un disque amovible (comme un disque flash) ou le placer dans un dossier partagé.

   - Déploiement à l'aide d'Active Directory

   - Déploiement à l'aide de votre solution logicielle de surveillance et de gestion à distance (RMM)

5. **Assignation des points de distribution**

   Désignez les appareils sur lesquels l'Agent d'administration est installé comme points de distribution.

6. **Sondage réseau**

   Configuration et exécution d'un sondage réseau via le point de distribution.

   Kaspersky Security Center Cloud Console fournit les méthodes suivantes pour effectuer le sondage du réseau :

   - Sondage des plages IP

   - Sondage du réseau Windows

- Sondage Active Directory

Une fois le sondage du réseau selon la planification terminé, les appareils de vos clients sont détectés et placés dans le groupe **Appareils non définis**.

7. **Déplacement des appareils détectés vers les groupes d'administration**

   Configurez les règles pour automatiquement déplacer les appareils découverts dans les groupes d'administration requis ; ou déplacez ces appareils manuellement dans groupes d'administration requis.

8. **Création de paquets d'installation pour l'Agent d'administration et les applications Kaspersky administrées**

   Si vous n'avez pas lancé l'assistant de démarrage rapide de l'application ou si vous avez ignoré l'étape de création des paquets d'installation, créez des paquets d'installation pour les applications Kaspersky.

9. **Remplacement des applications de sécurité d'éditeurs tiers**

   Si des applications de sécurité tierces sont installées sur les appareils de vos clients, supprimez-les avant l'installation des applications Kaspersky.

10. **Installation des applications Kaspersky sur les appareils de vos clients**

    Créez des tâches d'installation à distance pour installer l'Agent d'administration et les applications Kaspersky administrées sur les appareils de vos clients.

    Si nécessaire, vous pouvez créer plusieurs tâches d'installation à distance pour installer des applications Kaspersky administrées pour différents groupes d'administration ou différentes sélections d'appareils.

    Une fois les tâches créées, vous pouvez configurer leurs paramètres. Assurez-vous que la programmation pour chaque tâche répond à vos exigences. Tout d'abord, la tâche pour installer l'Agent d'administration doit être exécutée. Une fois l'Agent d'administration installé sur les appareils de vos clients, vous devez exécuter la tâche d'installation des applications Kaspersky administrées.

11. **Vérification du déploiement initial des applications Kaspersky**

    Générer et afficher le **Rapport sur les versions de l'application Kaspersky**. Assurez-vous que les applications Kaspersky administrées sont installées sur tous les appareils de vos clients.

12. **Création des stratégies pour les applications Kaspersky**

    Ouvrez le menu **Ressources (Appareils)** → **Groupes** ;si vous souhaitez créer une stratégie universelle pour l'ensemble de vos clients, sélectionnez **Serveur d'administration.** Si vous souhaitez créer une stratégie particulière pour un client individuel, sélectionnez le groupe d'administration correspondant à ce client. Créez une stratégie pour l'application Kaspersky requise.

Utilisation conjointe de Kaspersky Security Center fonctionnant sur site et de Kaspersky Security Center Cloud Console

Si vous avez déjà utilisé Kaspersky Security Center fonctionnant sur site, vous pouvez convertir vos Serveurs d'administration existants fonctionnant sur site en Serveurs d'administration secondaires de votre nouveau Serveur d'administration de Kaspersky Security Center Cloud Console, comme décrit dans cette section.

Si vous configurez l'utilisation conjointe de Kaspersky Security Center fonctionnant sur site et de Kaspersky Security Center Cloud Console, vous ne pourrez pas effectuer de migration à partir de Kaspersky Security Center fonctionnant sur site vers Kaspersky Security Center Cloud Console, sauf si vous supprimez la hiérarchie des Serveurs d'administration.

Pour créer une hiérarchie de Serveurs d'administration,

Ajoutez vos Serveurs d'administration existants fonctionnant sur site en tant que Serveurs d'administration secondaires.

Licences des applications Kaspersky pour les MSP

Kaspersky Security Center Cloud Console permet de diffuser de manière centralisée les clés de licence des applications de Kaspersky sur les appareils de vos clients, de suivre l'utilisation des clés et de prolonger la durée de validité des licences.

Si vous gérez plusieurs locataires, vous pouvez distribuer les clés de licence selon les approches suivantes :

- Une clé de licence pour tous les locataires.
- Une clé de licence individuelle pour chaque locataire.

Pour distribuer des clés de licence sur les appareils de vos clients, procédez comme suit :

1. Ajoutez la clé de licence requise dans le stockage du Serveur d'administration.
2. Exécutez une des actions suivantes :
   - Configurez la diffusion automatique de la clé de licence.

     Dans ce cas, Kaspersky Security Center Cloud Console sélectionne l'une des clés de licence applicables et la déploie automatiquement chaque fois qu'un nouvel appareil est détecté.
   - Configurez la tâche Ajouter une clé pour distribuer une clé de licence aux appareils.

     Lors de la configuration de la tâche, vous sélectionnez la clé de licence qui doit être déployée sur les appareils et sélectionnez le groupe d'administration qui contient les appareils requis.

     Une tâche ne peut distribuer qu'une seule clé de licence. Cela implique que si vous souhaitez distribuer plusieurs clés de licence, vous devez créer une tâche pour chacune d'elles.

   Les applications Kaspersky installées sur les appareils de vos clients sont activées.

L'ajout d'une clé de licence active au Serveur d'administration principal est obligatoire. Dans le cas contraire, l'espace de travail associé sera supprimé au bout de 90 jours, quel que soit l'état des clés de licence sur les autres Serveurs d'administration de cet espace de travail.

Capacités de surveillance et de reporting pour les MSP

Kaspersky Security Center Cloud Console vous offre des fonctionnalités de surveillance et de génération de rapports. Ces capacités offrent un aperçu de l'infrastructure de votre organisation, des états de la protection et des statistiques.

Une fois que vous avez déployé Kaspersky Security Center Cloud Console, vous pouvez configurer les fonctionnalités de surveillance et de génération de rapports en fonction de vos besoins.

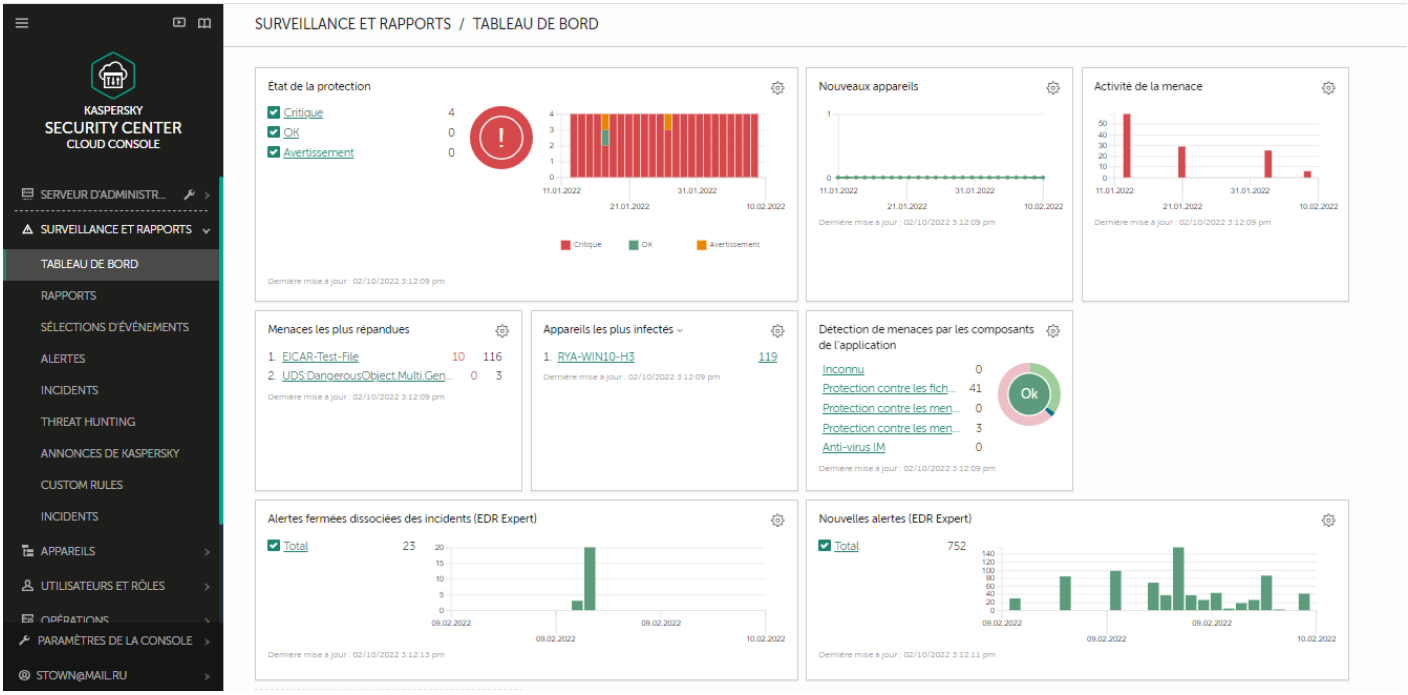
Kaspersky Security Center Cloud Console propose les types de fonctionnalités de surveillance et de génération de rapports suivants :

- Tableau de bord
- Rapports

- Sélections d'événements
- Notifications par email

Tableau de bord

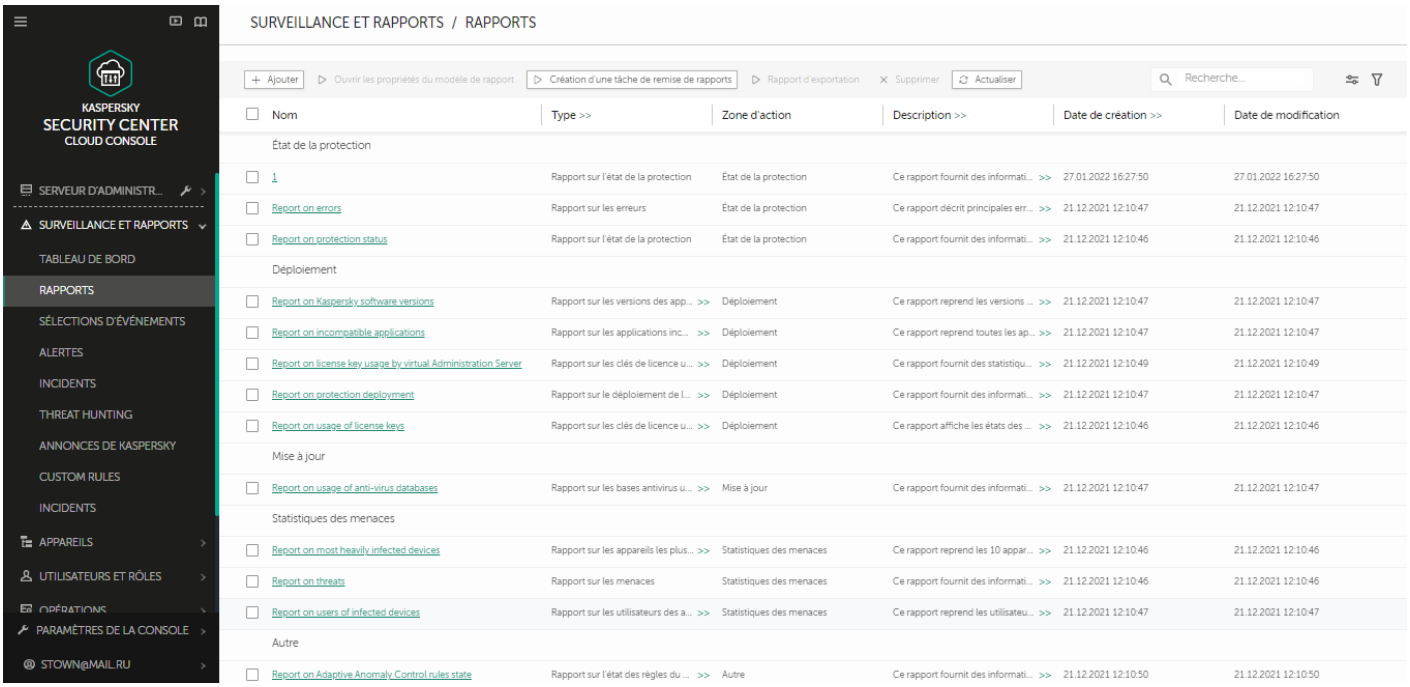
Le tableau de bord vous permet de contrôler visuellement les données graphiques des tendances de la sécurité du réseau de votre organisation. (Voir la figure ci-dessous.)



La rubrique Tableau de bord

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. Vous pouvez aussi planifier la livraison du rapport par email (voir la figure ci-dessous).



La rubrique Rapports

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. Kaspersky Security Center Cloud Console contient un certain nombre de sélections d'événements prédéfinies (par exemple, **Derniers événements** et **Événements critiques**). Vous pouvez également créer des sélections d'événements personnalisées.

Notifications par email

Vous pouvez configurer la notification par email à propos d'événements se produisant dans Kaspersky Security Center Cloud Console et sur les appareils de vos clients.

Utilisation de Kaspersky Security Center Cloud Console dans l'environnement cloud

Cette section fournit des informations sur les fonctionnalités de Kaspersky Security Center Cloud Console relatives à l'exploitation et à la maintenance de Kaspersky Security Center Cloud Console dans les environnements cloud comme Amazon Web Services, Microsoft Azure ou Google Cloud.

Pour travailler dans un environnement cloud, vous avez besoin d'une licence spéciale. Si vous ne disposez pas d'une telle licence, les éléments d'interface liés aux appareils Cloud ne sont pas exploitables.

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.

Options de licence pour l'environnement cloud

Travailler dans un environnement cloud est possible à la fois en mode d'essai et en mode commercial de Kaspersky Security Center Cloud Console :

- En mode d'essai, toutes les fonctionnalités de l'environnement cloud sont disponibles pendant toute la période de validité de votre espace de travail. Aucune licence n'est requise.
- En mode commercial, les fonctionnalités de l'environnement cloud ne sont disponibles que si une clé de licence Kaspersky Hybrid Cloud Security a été ajoutée comme active dans les propriétés du Serveur d'administration.

Dans les deux cas, la fonction de la gestion des vulnérabilités et des correctifs est automatiquement activée.

Vous pouvez rencontrer une erreur lors de la tentative d'activation de la fonctionnalité Prise en charge de l'environnement cloud à l'aide de la licence pour Kaspersky Hybrid Cloud Security.

Préparation au travail dans l'environnement cloud via Kaspersky Security Center Cloud Console

Cette section explique les étapes à suivre pour utiliser Kaspersky Security Center Cloud Console dans les environnements Cloud suivants :

- Amazon Web Services
- Microsoft Azure
- Google Cloud

Utilisation de l'environnement cloud Amazon Web Services

Cette section explique les préparatifs à suivre pour utiliser Kaspersky Security Center Cloud Console dans Amazon Web Services.

Les adresses des pages Web citées dans le présent document sont correctes à la date de publication de Kaspersky Security Center Cloud Console.

À propos de l'utilisation de l'environnement cloud d'Amazon Web Services

Pour utiliser la plateforme AWS et plus particulièrement, pour créer des instances, il faut disposer d'un compte utilisateur dans Amazon Web Services. Vous pouvez créer un compte gratuit à l'adresse https://aws.amazon.com/fr/. Vous pouvez aussi utiliser un compte utilisateur Amazon existant.

Pour en savoir plus sur les images AMI et sur le fonctionnement de la boutique d'apps AWS Marketplace, consultez la page d'aide d'AWS Marketplace. Pour en savoir plus sur l'utilisation de la plateforme AWS, sur l'utilisation d'instances et sur les notions liées à celles-ci, consultez la documentation d'Amazon Web Services.

Les adresses des pages Web citées dans le présent document sont correctes à la date de publication de Kaspersky Security Center Cloud Console.

Création de comptes utilisateurs IAM pour les instances d'Amazon EC2

Cette section décrit les actions à exécuter pour garantir le bon fonctionnement de Kaspersky Security Center Cloud Console. Ces actions comprennent l'utilisation des comptes utilisateurs IAM (gestion des identités et des accès) d'AWS. Elle décrit également les actions à exécuter sur les appareils clients pour y installer l'Agent d'administration, puis installer Kaspersky Security for Windows Server et Kaspersky Endpoint Security for Linux.

Garantie des privilèges pour le fonctionnement de Kaspersky Security Center Cloud Console avec AWS

Pour fonctionner dans l'environnement cloud Amazon Web Services à l'aide de Kaspersky Security Center Cloud Console, vous devez créer un *Compte utilisateur IAM*, qui sera utilisé par Kaspersky Security Center Cloud Console pour fonctionner avec les services AWS. Avant de commencer à utiliser le Serveur d'administration, créez un compte utilisateur IAM avec une *clé d'accès AWS IAM* (par la suite *clé d'accès IAM*).

La création d'un compte utilisateur IAM requiert une console de gestion AWS. Pour pouvoir utiliser la console de gestion AWS, il vous faut un nom d'utilisateur et un mot de passe d'un compte utilisateur dans AWS.

Création d'un compte utilisateur IAM pour utiliser la Kaspersky Security Center Cloud Console

Un compte utilisateur IAM est requis pour travailler avec Kaspersky Security Center Cloud Console. Vous pouvez créer un compte utilisateur IAM avec toutes les permissions nécessaires ou vous pouvez créer deux comptes utilisateurs séparés.

La *clé d'accès IAM* est créée automatiquement pour l'utilisateur IAM. Cette clé doit être présentée à Kaspersky Security Center Cloud Console lors de la configuration initiale. La clé d'accès IAM est composée de l'ID de clé d'accès et de la clé secrète. Pour en savoir plus sur le service IAM, consultez les pages d'aide d'AWS suivantes :

- https://docs.aws.amazon.com/fr_fr/IAM/latest/UserGuide/introduction.html.
- https://docs.aws.amazon.com/fr_fr/IAM/latest/UserGuide/IAM_UseCases.html#UseCase_EC2.

Pour créer un compte utilisateur IAM doté des privilèges requis, procédez comme suit :

1. Ouvrez la console de gestion AWS et connectez-vous sous votre compte utilisateur.
2. Dans la liste des services AWS, sélectionnez **IAM**.

   Une fenêtre contenant une liste de noms d'utilisateur et le menu qui permet d'utiliser l'outil s'ouvre.
3. Parcourez les zones de la console qui traitent des comptes utilisateurs et ajoutez un ou plusieurs noms d'utilisateur ou noms.
4. Pour chaque utilisateur que vous ajoutez, définissez les propriétés AWS suivantes :
   - Type d'accès : **accès programmé**.
   - Limite des permissions non définies.
   - Autorisation : **ReadOnlyAccess**.

     Après avoir ajouté des permissions, révisez-les pour confirmer leur exactitude. En cas d'erreur de sélection, revenez à l'écran précédent et opérez une nouvelle sélection.
5. Après la création du compte utilisateur, un tableau contenant la clé d'accès IAM du nouvel utilisateur IAM s'affiche. L'ID de clé d'accès s'affiche dans la colonne **ID de clé d'accès**. La clé secrète s'affiche sous forme d'astérisques dans la colonne **Clé d'accès secrète**. Pour voir la clé secrète, cliquez sur **Afficher**.

Le compte utilisateur créé apparaît dans la liste des comptes utilisateurs IAM qui correspondent à votre compte utilisateur dans AWS.

Les adresses des pages Web citées dans le présent document sont correctes à la date de publication de Kaspersky Security Center Cloud Console.

Manipulation dans l'environnement cloud Microsoft Azure

Cette section fournit des informations sur la manière d'exploiter et de maintenir Kaspersky Security Center Cloud Console dans l'environnement cloud de la plateforme Microsoft Azure et sur la manière de déployer la protection sur les des machines virtuelles au sein de l'environnement cloud.

À propos de l'utilisation de Microsoft Azure

Pour utiliser la plateforme Microsoft Azure et plus particulièrement, pour pouvoir acheter des applications dans la place de marché Azure et créer des machines virtuelles, il faut disposer d'un abonnement Azure. Avant de commencer à utiliser Microsoft Azure dans Kaspersky Security Center Cloud Console, créez un identifiant de l'application Azure avec les autorisations requises pour l'installation d'applications sur des machines virtuelles.

Création d'un abonnement, d'un identifiant de l'application et d'un mot de passe

Pour travailler avec Kaspersky Security Center Cloud Console dans l'environnement Microsoft Azure, il vous faut un abonnement Azure, un identifiant de l'application Azure et un mot de passe de l'application Azure. Vous pouvez utiliser un abonnement existant si vous en possédez déjà un.

L'abonnement Azure permet à son détenteur d'accéder au portail d'administration de la plateforme Microsoft Azure et aux services Microsoft Azure. L'abonné peut utiliser la plateforme Microsoft Azure pour gérer des services comme Azure SQL et le Stockage Azure.

Pour créer un abonnement Microsoft Azure,

Accédez à https://learn.microsoft.com/en-us/azure/cost-management-billing/manage/create-subscription et suivez les instructions qui s'y trouvent.

Pour en savoir plus sur la création d'un abonnement, consultez le site Internet de Microsoft. Vous obtiendrez un ID d'abonnement que vous communiquerez plus tard à Kaspersky Security Center Cloud Console avec l'identifiant de l'application et le mot de passe.

Pour créer et enregistrer l'identifiant de l'application Azure et le mot de passe,

1. Rendez-vous sur https://portal.azure.com et confirmez que vous êtes connecté.
2. A l'aide des instructions reprises sur la page de référence, créez votre identifiant de l'application.
3. Accédez à la section **Clés** des paramètres de l'application.
4. Dans la section **Clés**, remplissez les champs **Description** et **Expire le** et laissez le champ **Valeur** vide.
5. Cliquez sur **Enregistrer**.

   Quand vous cliquez sur **Enregistrer**, le système remplit automatiquement le champ **Valeur** avec une longue séquence de caractères. Cette séquence est votre mot de passe de l'application Azure (par exemple, yXyPOy6Tre9PYgP/j4XVyJCvepPHk2M/UYJ+QlfFvdU=). La description est affichée comme vous l'avez saisie.
6. Copiez le mot de passe et enregistrez-le afin que vous puissiez transmettre plus tard l'identifiant de l'application et le mot de passe à Kaspersky Security Center Cloud Console.

   Vous pouvez copier le mot de passe uniquement lors de sa création. Par la suite, le mot de passe ne sera plus affiché et il ne peut être récupéré.

Les adresses des pages Web citées dans le présent document sont correctes à la date de publication de Kaspersky Security Center Cloud Console.

Attribution d'un rôle à un identifiant de l'application Azure

Si vous souhaitez uniquement détecter les machines virtuelles à l'aide de la recherche d'appareils, votre identifiant de l'application Azure doit avoir le rôle de Lecteur. Si vous voulez non seulement détecter les machines virtuelles, mais également déployer la protection via votre identifiant de l'application Azure, votre identifiant de l'application Azure doit avoir le rôle de contributeur des machines virtuelles.

Suivez les instructions reprises sur le site Internet de Microsoft pour attribuer un rôle à votre identifiant de l'application Azure.

Travailler dans Google Cloud

Cette section fournit des informations sur l'utilisation de Kaspersky Security Center Cloud Console dans l'environnement cloud fourni par Google.

Vous pouvez utiliser l'API Google pour travailler avec Kaspersky Security Center Cloud Console dans Google Cloud Platform. Un compte Google est requis. Pour en savoir plus, veuillez consulter la documentation Google à l'adresse https://cloud.google.com.

Vous devrez créer et fournir à Kaspersky Security Center Cloud Console les informations d'identification suivantes :

- **Email client**

  L'email client est l'adresse email que vous avez utilisée pour enregistrer votre projet sur Google Cloud.

- **Identifiant du projet**

  L'identifiant du projet est l'identifiant que vous avez reçu lors de l'enregistrement de votre projet sur Google Cloud.

- **Clé privée**

  La clé privée est la séquence de caractères que vous avez reçue comme clé privée lors de l'enregistrement de votre projet sur Google Cloud. Envisagez de copier et coller cette séquence pour éviter les erreurs.

Assistant de configuration pour une utilisation dans le Cloud dans Kaspersky Security Center Cloud Console

Pour configurer Kaspersky Security Center Cloud Console à l'aide de cet Assistant, vous devez avoir les éléments suivants :

- Les informations d'identification particulières pour un environnement cloud :
  - Un compte utilisateur IAM qui a obtenu le droit d'interroger le segment dans le Cloud (pour travailler avec Amazon Web Services)
  - Un identifiant de l'application Azure, un mot de passe et un abonnement (pour une utilisation avec Microsoft Azure)
  - Adresse email du client Google, ID du projet et clé privée (pour une utilisation avec Google Cloud)

- Paquets d'installation :
  - Agent d'administration pour Windows
  - Agent d'administration pour Linux
  - Kaspersky Endpoint Security for Linux
- Plug-in Internet pour Kaspersky Endpoint Security for Linux
- Au moins un des éléments suivants :
  - Paquet d'installation et plug-in Internet pour Kaspersky Endpoint Security for Windows (recommandé)
  - Paquet d'installation et plug-in Internet pour Kaspersky Security for Windows Server

L'Assistant de configuration pour une utilisation dans le Cloud démarre automatiquement à la première connexion à Kaspersky Security Center Cloud Console si votre espace de travail a été créé à l'aide de la licence Kaspersky Hybrid Cloud Security. Vous pouvez également lancer l'assistant de configuration pour une utilisation dans le Cloud manuellement à tout moment.

Pour lancer l'assistant de configuration pour une utilisation dans le Cloud manuellement,

Dans le menu principal, accédez à **Découverte et déploiement → Déploiement et attribution → Configurer l'environnement cloud**.

L'Assistant démarre.

Une session de travail moyenne de cet Assistant dure environ 15 minutes.

Étape 1. Vérification des plug-ins et des paquets d'installation requis

Cette étape ne s'affiche pas si vous disposez de tous les plug-ins Internet et paquets d'installation requis répertoriés ci-dessous.

Pour configurer un environnement cloud, vous devez disposer des modules suivants :

- Paquets d'installation :
  - Agent d'administration pour Windows
  - Agent d'administration pour Linux
  - Kaspersky Endpoint Security for Linux
- Plug-in Internet pour Kaspersky Endpoint Security for Linux
- Au moins un des éléments suivants :
  - Paquet d'installation et plug-in Internet pour Kaspersky Endpoint Security for Windows (recommandé)

- Paquet d'installation et plug-in Internet pour Kaspersky Security for Windows Server

  Nous vous recommandons d'utiliser Kaspersky Endpoint Security for Windows au lieu de Kaspersky Security for Windows Server.

Kaspersky Security Center Cloud Console détecte automatiquement les modules dont vous disposez déjà et répertorie uniquement ceux qui manquent. Téléchargez les modules répertoriés en cliquant sur le bouton **Sélectionner les applications à télécharger**, puis en sélectionnant les plug-ins et les paquets d'installation requis. Après avoir téléchargé un module, vous pouvez utiliser le bouton **Actualiser** pour mettre à jour la liste des modules manquants.

Étape 2. Sélection de la méthode d'activation de l'application

Cette étape s'affiche uniquement si vous avez utilisé une licence autre que Kaspersky Hybrid Cloud Security lors de la création de l'espace de travail. Vous n'avez jamais ajouté de clé de licence Kaspersky Hybrid Cloud Security dans le champ d'activation du Serveur d'administration. Dans ce cas, vous devez activer le Serveur d'administration en utilisant une licence Kaspersky Hybrid Cloud Security.

Étape 3. Sélection de l'environnement cloud et de l'autorisation

Définissez les paramètres suivants :

- **Environnement cloud**

  Sélectionnez l'environnement cloud dans lequel vous déployez Kaspersky Security Center Cloud Console : AWS, Azure ou Google Cloud.

  Si vous prévoyez de travailler avec plusieurs environnements cloud, sélectionnez un environnement, puis exécutez de nouveau l'assistant.

- **Nom de la connexion**

  Saisissez un nom pour la connexion. Le nom ne peut pas contenir plus de 256 caractères. Seuls les caractères Unicode sont admis.

  Ce nom servira aussi pour le groupe d'administration des appareils dans le cloud.

  Si vous prévoyez de travailler avec plusieurs environnements Cloud, vous pourriez inclure le nom de l'environnement dans le nom de la connexion, par exemple, " Segment Azure ", " Segment AWS " ou " Segment Google ".

Entrez vos informations d'identification pour recevoir l'autorisation dans l'environnement cloud que vous avez indiqué.

AWS

Si vous avez sélectionné AWS comme type de segment dans le Cloud, utilisez une clé d'accès AWS IAM pour sonder davantage le segment dans le Cloud. Saisissez les données clés suivantes :

- **ID de clé d'accès**

L'ID de clé d'accès IAM est une suite de caractères alphanumériques. Vous avez reçu l'ID de clé lors de la création du compte utilisateur IAM.

Ce champ est accessible après avoir opté pour l'autorisation à l'aide d'une clé d'accès AWS IAM.

- **Clé secrète**

  La clé secrète que vous avez reçue avec l'ID de clé d'accès quand vous avez créé le compte utilisateur IAM.

  Les caractères de la clé secrète s'affichent sous la forme d'astérisques. Après que vous avez commencé à saisir la clé secrète, le bouton **Afficher** apparaît. Cliquez sur ce bouton pendant le temps qu'il vous faut pour consulter les caractères saisis.

  Ce champ est accessible après avoir opté pour l'autorisation à l'aide d'une clé d'accès AWS IAM.

  Pour afficher les caractères que vous avez entrés, cliquez sur le bouton **Afficher** et maintenez-le enfoncé.

Azure

Si vous avez choisi Azure comme le type de segment dans le Cloud, configurez les paramètres suivants de la connexion qui interviendra à l'avenir dans le sondage des segments dans le Cloud :

- **Identifiant de l'application Azure**

  Vous avez créé cet identifiant de l'application sur le portail Azure.

  Vous pouvez fournir un identifiant de l'application Azure pour le sondage et d'autres fins. Si vous souhaitez sonder un autre segment Azure, il faut d'abord supprimer la connexion Azure existante.

- **Identifiant de l'abonnement Azure**

  Vous avez créé l'abonnement sur le portail Azure.

- **Mot de passe de l'application Azure**

  Vous avez obtenu le mot de passe de l'identifiant de l'application quand vous avez créé celui-ci.

  Les caractères de la mot de passe s'affichent sous la forme d'astérisques. Après que vous avez commencé à saisir le mot de passe, le bouton **Afficher** apparaît. Maintenez ce bouton enfoncé pour voir les caractères saisis.

  Pour afficher les caractères que vous avez entrés, cliquez sur le bouton **Afficher** et maintenez-le enfoncé.

- **Nom du compte de stockage Azure**

  Vous avez créé le nom du Compte de stockage Azure pour utiliser Kaspersky Security Center Cloud Console.

- **Clé d'accès au stockage Azure**

Vous avez reçu un mot de passe (une clé) lorsque vous avez créé le compte de stockage Azure pour utiliser Kaspersky Security Center Cloud Console.

La clé est disponible dans la section " Aperçu du compte de stockage Azure ", dans la sous-section " Clés ".

Pour afficher les caractères que vous avez entrés, cliquez sur le bouton **Afficher** et maintenez-le enfoncé.

Google Cloud

Si vous avez choisi Google Cloud comme le type de segment dans le Cloud, configurez les paramètres suivants de la connexion qui interviendra à l'avenir dans le sondage segments dans le Cloud :

- **Adresse email du client**

  L'email client est l'adresse email que vous avez utilisée pour enregistrer votre projet sur Google Cloud.

- **Identifiant du projet**

  L'identifiant du projet est l'identifiant que vous avez reçu lors de l'enregistrement de votre projet sur Google Cloud.

- **Clé privée**

  La clé privée est la séquence de caractères que vous avez reçue comme clé privée lors de l'enregistrement de votre projet sur Google Cloud. Envisagez de copier et coller cette séquence pour éviter les erreurs.

  Pour afficher les caractères que vous avez entrés, cliquez sur le bouton **Afficher** et maintenez-le enfoncé.

La connexion que vous avez définie est enregistrée dans les paramètres de l'application.

L'Assistant de configuration pour une utilisation dans le Cloud vous permet de définir un seul segment. Par la suite, vous pouvez indiquer d'autres connexions pour l'administration d'autres segments dans le Cloud.

Cliquez sur **Suivant** pour continuer.

Étape 4. Sondage par segment et configuration de la synchronisation avec le Cloud

Cette étape marque le début du sondage des segments dans le Cloud et la création automatique d'un groupe d'administration pour les appareils Cloud. Les appareils trouvés lors du sondage sont placés dans ce groupe. C'est ici aussi que vous allez programmer le sondage du segment dans le Cloud (par défaut, toutes les 5 minutes ; vous pouvez modifier ce paramètre ultérieurement).

La règle de déplacement automatique **Synchronisation avec Cloud** est créée à cette étape. À chaque analyse ultérieure du réseau Cloud, les appareils virtuels détectés sont déplacés dans le sous-groupe correspondant au sein du groupe **Appareils administrés\Cloud**.

Définissez le paramètre **Synchroniser les groupes d'administration avec la structure Cloud**.

Quand cette option est activée, le groupe **Cloud** est créé automatiquement dans le groupe **Appareils administrés** et la Recherche d'appareils dans le Cloud démarre. Les machines virtuelles détectées à chaque analyse du réseau Cloud sont déplacées dans le groupe Cloud. La structure des sous-groupes d'administration au sein de ce groupe correspond à la structure de votre segment dans le Cloud (dans AWS, les zones d'accessibilité et les groupes de déplacement ne sont pas représentés dans la structure dans Azure, les sous-réseaux ne sont pas représentés dans la structure). Les appareils qui ne sont pas identifiés en tant qu'instances dans l'environnement cloud se trouvent dans le groupe **Appareils non définis**. Cette structure de groupe permet d'installer les applications antivirus sur les instances à l'aide des tâches d'installation de groupe et de configurer de différentes stratégies pour différents groupes.

Quand l'option est désactivée, le groupe **Cloud** est aussi créé et une recherche d'appareil est lancée toutefois, les sous-groupes qui correspondent à la structure du segment dans le Cloud ne sont pas créés au sein du groupe. Toutes les instances détectées se trouvent dans le groupe d'administration **Cloud** et s'affichent dans une liste commune. Si lors de l'utilisation de Kaspersky Security Center Cloud Console, vous devez effectuer une synchronisation, vous pourrez modifier les propriétés de la règle **Synchronisation avec Cloud** et la forcer. Le forcement de la règle reconstruit la structure des groupes à l'intérieur du groupe Cloud de manière à ce qu'elle corresponde à la structure de votre segment dans le Cloud.

Cette option est Inactif par défaut.

Cliquez sur **Suivant** pour continuer.

Étape 5. Sélection de l'application pour laquelle créer une stratégie et des tâches

Cette étape s'affiche uniquement si vous disposez de paquets d'installation et de plug-ins pour Kaspersky Endpoint Security for Windows et Kaspersky Security for Windows Server. Si vous disposez d'un plug-in et d'un paquet d'installation pour une seule de ces applications, cette étape est ignorée et Kaspersky Security Center Cloud Console crée une stratégie et des tâches pour l'application existante.

Sélectionnez une application pour laquelle vous souhaitez créer une stratégie et des tâches :

- Kaspersky Endpoint Security for Windows
- Kaspersky Security for Windows Server

Étape 6. Configuration de Kaspersky Security Network pour Kaspersky Security Center Cloud Console

Cette étape est ignorée lors de l'exécution de Kaspersky Security Center Cloud Console en mode d'évaluation ou sur un Serveur d'administration virtuel.

Indiquez les paramètres du transfert des informations sur le fonctionnement de Kaspersky Security Center Cloud Console dans la base de connaissances de Kaspersky Security Network (KSN). Sélectionnez l'une des options ci-dessous :

- **J'accepte les termes du Kaspersky Security Network**

Kaspersky Security Center Cloud Console 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 Cloud Console et les applications administrées ne fourniront aucune information à Kaspersky Security Network.

  Si vous sélectionnez cette option, l'utilisation de Kaspersky Security Network sera désactivée.

Kaspersky recommande la participation au Kaspersky Security Network.

Les accords KSN pour les applications administrées peuvent également être affichés. Si vous acceptez d'utiliser Kaspersky Security Network, l'application administrée enverra des données à Kaspersky. Si vous n'acceptez pas d'utiliser Kaspersky Security Network, l'application administrée n'enverra aucune donnée à Kaspersky. Vous pouvez modifier ce paramètre ultérieurement dans la stratégie de l'application.

Cliquez sur **Suivant** pour continuer.

Étape 7. Création d'une configuration initiale de protection

Vous pouvez consulter une liste de stratégies et de tâches créées.

Attendez la fin de la création des stratégies et des tâches, puis cliquez sur **Suivant** pour continuer. Sur la dernière page de l'assistant, cliquez sur le bouton **Terminer** pour quitter.

Sondage de segments du réseau via Kaspersky Security Center Cloud Console

Les informations sur la structure du réseau (et sur les appareils qui en font partie) sont reçues au cours des sondages réguliers des segments dans le Cloud à l'aide des outils de l'API d'AWS, de l'API d'Azure et de l'API de Google. Sur la base des informations obtenues, Kaspersky Security Center Cloud Console actualise le contenu des dossiers Appareils non définis et Appareils administrés. Si vous avez configuré le déplacement automatique des appareils dans les groupes d'administration, les appareils détectés sont inclus dans les groupes d'administration.

Pour pouvoir sonder les segments dans le Cloud, vous devez posséder les privilèges correspondants fournis avec le compte utilisateur IAM (dans AWS), avec l'identifiant de l'application et le mot de passe (dans Azure) ou avec un email client de Google, un identifiant de projet Google et une clé privée (dans Google Cloud).

Vous pouvez ajouter et supprimer des connexions, ainsi que configurer une programmation du sondage pour chaque segment dans le Cloud.

Ajout de connexions pour le sondage des segments dans le Cloud via Kaspersky Security Center Cloud Console

Pour ajouter une connexion pour le sondage des segments dans le Cloud à la liste des connexions disponibles, procédez comme suit :

1. Dans le menu principal, accédez à **Découverte et déploiement → Découverte → Dans le Cloud**.
2. Dans la fenêtre qui s'ouvre, cliquez sur **Propriétés**.
3. Dans la fenêtre **Configuration** qui s'ouvre, cliquez sur **Ajouter**.

   La fenêtre **Paramètres du segment dans le cloud** s'ouvre.
4. Définissez le nom de l'environnement cloud de la connexion qui interviendra à l'avenir dans le sondage des segments dans l'environnement cloud :

   - **Environnement cloud**

     Sélectionnez l'environnement cloud dans lequel vous déployez Kaspersky Security Center Cloud Console : AWS, Azure ou Google Cloud.

     Si vous prévoyez de travailler avec plusieurs environnements cloud, sélectionnez un environnement, puis exécutez de nouveau l'assistant.

   - **Nom de la connexion**

     Saisissez un nom pour la connexion. Le nom ne peut pas contenir plus de 256 caractères. Seuls les caractères Unicode sont admis.

     Ce nom servira aussi pour le groupe d'administration des appareils dans le cloud.

     Si vous prévoyez de travailler avec plusieurs environnements Cloud, vous pourriez inclure le nom de l'environnement dans le nom de la connexion, par exemple, " Segment Azure ", " Segment AWS " ou " Segment Google ".
5. Entrez vos informations d'identification pour recevoir l'autorisation dans l'environnement cloud que vous avez indiqué.

   - Si vous avez sélectionné AWS, spécifiez les éléments suivants :

     - **ID de clé d'accès**

       L'ID de clé d'accès IAM est une suite de caractères alphanumériques. Vous avez reçu l'ID de clé lors de la création du compte utilisateur IAM.

       Ce champ est accessible après avoir opté pour l'autorisation à l'aide d'une clé d'accès AWS IAM.

     - **Clé secrète**

       La clé secrète que vous avez reçue avec l'ID de clé d'accès quand vous avez créé le compte utilisateur IAM.

       Les caractères de la clé secrète s'affichent sous la forme d'astérisques. Après que vous avez commencé à saisir la clé secrète, le bouton **Afficher** apparaît. Cliquez sur ce bouton pendant le temps qu'il vous faut pour consulter les caractères saisis.

       Ce champ est accessible après avoir opté pour l'autorisation à l'aide d'une clé d'accès AWS IAM.

     Pour afficher les caractères que vous avez entrés, cliquez sur le bouton **Afficher** et maintenez-le enfoncé.

- Si vous avez sélectionné Azure, spécifiez les paramètres suivants :
  - **Identifiant de l'application Azure**

    Vous avez créé cet identifiant de l'application sur le portail Azure.

    Vous pouvez fournir un identifiant de l'application Azure pour le sondage et d'autres fins. Si vous souhaitez sonder un autre segment Azure, il faut d'abord supprimer la connexion Azure existante.

  - **Identifiant de l'abonnement Azure**

    Vous avez créé l'abonnement sur le portail Azure.

  - **Mot de passe de l'application Azure**

    Vous avez obtenu le mot de passe de l'identifiant de l'application quand vous avez créé celui-ci.

    Les caractères de la mot de passe s'affichent sous la forme d'astérisques. Après que vous avez commencé à saisir le mot de passe, le bouton **Afficher** apparaît. Maintenez ce bouton enfoncé pour voir les caractères saisis.

    Pour afficher les caractères que vous avez entrés, cliquez sur le bouton **Afficher** et maintenez-le enfoncé.

  - **Nom du compte de stockage Azure**

    Vous avez créé le nom du Compte de stockage Azure pour utiliser Kaspersky Security Center Cloud Console.

  - **Clé d'accès au stockage Azure**

    Vous avez reçu un mot de passe (une clé) lorsque vous avez créé le compte de stockage Azure pour utiliser Kaspersky Security Center Cloud Console.

    La clé est disponible dans la section " Aperçu du compte de stockage Azure ", dans la sous-section " Clés ".

    Pour afficher les caractères que vous avez entrés, cliquez sur le bouton **Afficher** et maintenez-le enfoncé.

Si vous avez sélectionné Google Cloud, spécifiez les paramètres suivants :

- **Adresse email du client**

  L'email client est l'adresse email que vous avez utilisée pour enregistrer votre projet sur Google Cloud.

- **Identifiant du projet**

  L'identifiant du projet est l'identifiant que vous avez reçu lors de l'enregistrement de votre projet sur Google Cloud.

- **Clé privée**

La clé privée est la séquence de caractères que vous avez reçue comme clé privée lors de l'enregistrement de votre projet sur Google Cloud. Envisagez de copier et coller cette séquence pour éviter les erreurs.

Pour afficher les caractères que vous avez entrés, cliquez sur le bouton **Afficher** et maintenez-le enfoncé.

6. Si vous le souhaitez, cliquez sur **Définir la programmation du sondage du réseau** et modifiez les paramètres par défaut.

La connexion est enregistrée dans les paramètres de l'application.

Après le premier sondage du nouveau segment dans le Cloud, le sous-groupe qui correspond à ce segment apparaît dans le groupe d'administration **Appareils administrés\Cloud**.

Si vous utilisez des identifiants incorrects, aucune instance ne sera détectée lors du sondage des segments dans le Cloud et le nouveau sous-groupe n'apparaîtra pas dans le groupe d'administration **Appareils administrés\Cloud**.

Suppression d'une connexion pour le sondage des segments dans le Cloud

Si vous n'avez plus besoin de sonder un segment dans le Cloud en particulier, vous pouvez supprimer la connexion qui correspond à celui-ci dans la liste des connexions disponibles. Vous pouvez également supprimer la connexion si, par exemple, les droits de sondage du segment dans le Cloud ont été transmis à un autre utilisateur utilisant d'autres informations d'identification.

Pour supprimer une connexion, procédez comme suit :

1. Dans le menu principal, accédez à **Découverte et déploiement → Découverte → Dans le Cloud**.
2. Dans la fenêtre qui s'ouvre, cliquez sur **Propriétés**.
3. Dans la fenêtre **Configuration** qui s'ouvre, cliquez sur le nom du segment que vous souhaitez supprimer.
4. Cliquez sur **Supprimer**.
5. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **OK** pour confirmer votre choix.

La connexion est supprimée. Les appareils du segment dans le Cloud correspondant à cette connexion sont automatiquement supprimés des groupes d'administration.

Configuration de la programmation du sondage via Kaspersky Security Center Cloud Console

Le sondage du segment dans le Cloud est programmé. Vous pouvez définir la fréquence du sondage.

Pendant le fonctionnement de l'assistant de configuration pour une utilisation dans le Cloud, la fréquence du sondage est définie automatiquement sur 5 minutes. Vous pouvez modifier cette valeur à tout moment. Toutefois, il est déconseillé de réaliser un sondage à une fréquence supérieure à 5 minutes, car cela pourrait provoquer des erreurs dans le fonctionnement de l'API.

Pour configurer la programmation du sondage du segment dans le Cloud, procédez comme suit :

1. Dans le menu principal, accédez à **Découverte et déploiement** → **Découverte** → **Dans le Cloud**.
2. Dans la fenêtre qui s'ouvre, cliquez sur **Propriétés**.
3. Dans la fenêtre **Configuration** qui s'ouvre, cliquez sur le nom du segment pour lequel vous souhaitez configurer une programmation de sondage.

   La fenêtre **Paramètres du segment dans le cloud** s'ouvre.
4. Dans la fenêtre **Paramètres du segment dans le cloud**, cliquez sur le bouton **Définir la programmation du sondage du réseau**.

   La fenêtre **Programmation** s'ouvrira.
5. Dans la fenêtre **Programmation**, configurez les paramètres suivants :

   - **Lancement planifié**

     Options de programmation du sondage :

     - Tous les N jours

       Le sondage s'exécute régulièrement, selon l'intervalle défini en jours, à partir de la date et heure définis.

       Le sondage s'exécute par défaut chaque jour, à partir de la date et de l'heure actuelle du système.

     - Toutes les N minutes

       Le sondage s'exécute régulièrement, selon l'intervalle défini en minutes, à partir de l'heure définie.

       Le sondage s'exécute par défaut toutes les cinq minutes, à partir de l'heure actuelle du système.

     - Selon les jours de la semaine

       Le sondage s'exécute régulièrement les jours définis de la semaine, à l'heure indiquée.

       Par défaut, le sondage s'exécute chaque vendredi à 18h00.

     - Mensuellement, les jours indiqués des semaines sélectionnées

       Le sondage s'exécute régulièrement les jours définis de chaque mois, à l'heure indiquée.

       Par défaut, aucun jour du mois n'est sélectionné. L'heure de lancement par défaut est 18h00.

   - Intervalle de démarrage (en jours)

     Définissez la valeur de N (pour les minutes ou les jours).

- **À partir de**

  Déterminez quand vous souhaitez commencer le premier sondage.

- **Lancer les tâches non exécutées**

  Si votre espace de travail n'est pas disponible pendant la période pour laquelle le sondage est planifié, Kaspersky Security Center Cloud Console peut soit démarrer le sondage immédiatement après que l'espace de travail soit à nouveau disponible, soit attendre la prochaine fois pour laquelle le sondage est planifié.

  Si cette option est activée, Kaspersky Security Center Cloud Console commence à interroger immédiatement après que l'espace de travail est à nouveau disponible.

  Si cette option est désactivée, Kaspersky Security Center Cloud Console attend la prochaine programmation du sondage.

  Cette option est activée par défaut.

6. Cliquez sur le bouton **Enregistrer** afin d'enregistrer les modifications.

La programmation du sondage pour le segment est configurée et enregistrée.

Affichage des résultats du sondage des segments dans le Cloud via Kaspersky Security Center Cloud Console

Vous pouvez afficher les résultats du sondage des segments dans le Cloud, c'est-à-dire afficher la liste des appareils dans le Cloud administrés par le Serveur d'administration.

Pour afficher les résultats du sondage des segments dans le Cloud,

Dans le menu principal, accédez à **Découverte et déploiement** → **Découverte** → **Dans le Cloud**.

Les segments dans le cloud disponibles pour le sondage sont affichés.

Affichage des propriétés des appareils du Cloud via Kaspersky Security Center Cloud Console

Vous pouvez afficher les propriétés de chaque appareil du Cloud.

Pour afficher les propriétés d'un appareil du Cloud, procédez comme suit :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Appareils administrés**.
2. Cliquez sur le nom de l'appareil dont vous souhaitez voir les propriétés.

   La fenêtre des propriétés s'ouvre et la section **Général** est sélectionnée.

3. Si vous souhaitez afficher les propriétés propres aux appareils du Cloud, sélectionnez la section **Système** dans la fenêtre des propriétés.

   Les propriétés sont affichées en fonction de la plateforme Cloud de l'appareil.

   Pour les appareils dans AWS, les propriétés suivantes sont affichées :

   - **Appareil découvert à l'aide de l'API** (valeur : **AWS**)
   - **Région du cloud**
   - **Cloud VPC**
   - **Zone de disponibilité du cloud**
   - **Sous-réseau du cloud**
   - **Groupe de placement Cloud** (cette unité n'est affichée que si l'instance appartient à un groupe de placement ; dans le cas contraire, elle n'est pas affichée)

   Pour les appareils dans Azure, les propriétés suivantes sont affichées :

   - **Appareil découvert à l'aide de l'API** (valeur : **Microsoft Azure**)
   - **Région du cloud**
   - **Sous-réseau du cloud**

   Pour les appareils dans Google Cloud, les propriétés suivantes sont affichées :

   - **Appareil découvert à l'aide de l'API** (valeur : **Google Cloud**)
   - **Région du cloud**
   - **Cloud VPC**
   - **Zone de disponibilité du cloud**
   - **Sous-réseau du cloud**

Synchronisation avec le Cloud : Configuration de la règle de déplacement

Pendant l'utilisation de l'assistant de configuration pour une utilisation dans le Cloud, la règle Synchronisation avec Cloud est créée automatiquement dans le Cloud. La règle permet de déplacer automatiquement les appareils trouvés à chaque sondage à partir du groupe Appareils non définis vers le groupe Appareils administrés\Cloud pour que ces appareils soient accessibles pour l'administration centralisée. La règle par défaut est activée une fois créée. Vous pouvez désactiver, modifier ou forcer une règle à tout moment.

Pour modifier les propriétés de la règle Synchronisation avec Cloud et/ou forcer une règle, procédez comme suit :

1. Dans le menu principal, accédez à **Découverte et déploiement → Déploiement et attribution → Règles de déplacement**.

   La liste des règles de déplacement s'ouvre.

2. Dans la liste des règles de déplacement, sélectionnez **Synchronisation avec le cloud**.

La fenêtre de propriétés de la règle s'affiche.

3. Si nécessaire, sous l'onglet **Conditions de la règle**, puis sous l'onglet **Segments dans le Cloud**, définissez les paramètres suivants :

- **L'appareil se trouve dans le segment dans le Cloud**

  La règle s'applique uniquement aux appareils qui se trouvent dans le segment dans le Cloud sélectionné. Si la case est décochée, la règle s'applique à tous les appareils trouvés.

  Cette option est sélectionnée par défaut.

- **Objets enfants inclus**

  Si la case est cochée, cette règle exécutée pour tous les appareils du segment choisi et dans toutes les sous-sections du Cloud. Dans le cas contraire, la règle s'applique uniquement aux appareils qui se trouvent dans le segment racine.

  Cette option est sélectionnée par défaut.

- **Déplacer les appareils des objets enfants vers les sous-groupes correspondants**

  Si la case est Activé, les appareils des objets enfants sont déplacés dans les sous-groupes correspondant à leur structure.

  Si l'option est désactivée, les appareils des objets enfants sont déplacés dans la racine du sous-groupe AWS sans décomposition en sous-groupes.

  Cette option est activée par défaut.

- **Créer des sous-groupes qui correspondent aux conteneurs des appareils détectés pour la première fois**

  Quand cette option est activée, quand la structure du groupe **Appareils administrés\Cloud** ne contient aucun sous-groupe correspondant à la section qui contient l'appareil, Kaspersky Security Center Cloud Console crée ces sous-groupes. Par exemple, si un nouveau sous-réseau est découvert pendant la Recherche d'appareils, un nouveau groupe portant le même nom est créé dans le groupe **Appareils administrés\Cloud**.

  Si cette option est désactivée, Kaspersky Security Center Cloud Console ne crée aucun nouveau sous-groupe. Par exemple, si un nouveau sous-réseau est découvert lors du sondage du réseau, un nouveau groupe portant le même nom ne sera pas créé dans le groupe **Appareils administrés\Cloud** et les appareils qui se trouve dans ce sous-réseau seront déplacés vers le groupe **Appareils administrés\Cloud**.

  Cette option est activée par défaut.

- **Supprimer les sous-groupes n'ayant pas de correspondance dans les segments du Cloud**

  Si cette option est activée, l'application supprime du groupe Cloud tous les sous-groupes qui ne correspondent à aucun objet dans le cloud.

  Si cette option est désactivée, les sous-groupes qui ne correspondent à aucun objet dans le Cloud sont conservés.

  Cette option est activée par défaut.

Si vous avez activé l'option **Synchroniser les groupes d'administration avec la structure Cloud** lors de l'utilisation de l'assistant de configuration pour une utilisation dans le Cloud, la règle **Synchronisation avec le cloud** est créée et les options **Créer des sous-groupes qui correspondent aux conteneurs des appareils détectés pour la première fois** et **Supprimer les sous-groupes n'ayant pas de correspondance dans les segments du Cloud** sont activées.

Si vous n'avez pas activé l'option **Synchroniser les groupes d'administration avec la structure Cloud**, la règle **Synchronisation avec le cloud** est créée et ces options sont désactivées (décochées). Si votre travail avec Kaspersky Security Center Cloud Console nécessite que la structure des sous-groupes du sous-groupe **Appareils administrés\Cloud** corresponde à la structure des segments dans le Cloud, activez les options **Créer des sous-groupes qui correspondent aux conteneurs des appareils détectés pour la première fois** et **Supprimer les sous-groupes n'ayant pas de correspondance dans les segments du Cloud** dans les propriétés de la règle, puis appliquez la règle.

4. Sélectionnez la valeur dans la liste déroulante **L'appareil est détecté via l'utilisation de l'API** :

   - **Non**. L'appareil n'est pas détecté à l'aide de l'API AWS, Azure ou Google, c'est-à-dire qu'il se trouve soit en dehors de l'environnement cloud, soit dans l'environnement cloud, mais il ne peut pas être détecté à l'aide d'une API pour une raison quelconque.
   - **AWS**. L'appareil est détecté via l'utilisation de l'API AWS, autrement dit, l'appareil est bel et bien dans l'environnement cloud AWS.
   - **Azure**. L'appareil est détecté via l'utilisation de l'API Azure, autrement dit, l'appareil est bel et bien dans l'environnement cloud Azure.
   - **Google Cloud**. L'appareil est détecté via l'utilisation de l'API Google, autrement dit, l'appareil est bel et bien dans l'environnement cloud Google.
   - Pas de valeur. Le critère n'est pas appliqué.

5. En cas de besoin, configurez d'autres propriétés de la règle dans les autres sections.

La règle de déplacement est configurée.

Installation à distance d'applications sur les machines virtuelles Azure

Vous devez posséder une licence valide afin de pouvoir installer les applications sur les machines virtuelles Microsoft Azure.

Kaspersky Security Center Cloud Console prend en charge les scénarios suivants :

- Un appareil client est découvert par le biais d'une API Azure ; l'installation est également réalisée par le biais d'une API. L'utilisation de l'API Azure signifie que vous ne pouvez installer que les applications suivantes :
  - Kaspersky Endpoint Security for Linux
  - Kaspersky Endpoint Security for Windows
  - Kaspersky Security for Windows Server
- Un appareil client est découvert au moyen de l'API Azure ; l'installation est effectuée au moyen d'un point de distribution ou, s'il n'y a pas de point de distribution, manuellement, à l'aide de paquets d'installation autonomes. Vous pouvez ainsi installer n'importe quelle application prise en charge par Kaspersky Security Center Cloud Console.

Pour créer une tâche d'installation à distance de l'application sur les machines virtuelles Azure :

1. Dans le menu principal, accédez à **Ressources (Appareils)** → **Tâches**.
2. Cliquez sur **Ajouter**.

   Ceci permet de lancer l'assistant de création d'une tâche.
3. Suivez les instructions de l'assistant :

   a. Sélectionnez **Installation à distance d'une application** comme type de tâche.

   b. Sur la page **Paquets d'installation**, sélectionnez **Installation à distance par l'API Microsoft Azure**.

   c. Lorsque vous sélectionnez le compte pour accéder aux appareils, utilisez un compte Azure existant ou cliquez sur **Ajouter** et saisissez les identifiants de votre compte Azure :

   - **Nom du compte Azure**

     Saisissez n'importe quel nom pour les identifiants que vous précisez. Ce nom s'affichera dans la liste des comptes pour l'exécution de la tâche.

   - **Identifiant de l'application Azure**

     Vous avez créé cet identifiant de l'application sur le portail Azure.

     Vous pouvez fournir un identifiant de l'application Azure pour le sondage et d'autres fins. Si vous souhaitez sonder un autre segment Azure, il faut d'abord supprimer la connexion Azure existante.

   - **Mot de passe de l'application Azure**

     Vous avez obtenu le mot de passe de l'identifiant de l'application quand vous avez créé celui-ci.

     Les caractères de la mot de passe s'affichent sous la forme d'astérisques. Après que vous avez commencé à saisir le mot de passe, le bouton **Afficher** apparaît. Maintenez ce bouton enfoncé pour voir les caractères saisis.

   d. Sélectionnez les appareils concernés dans le groupe **Appareils administrés\Cloud**.

Quand l'assistant a terminé, la tâche d'installation à distance de l'application apparaît dans la liste des tâches.

Contacter le Support Technique

Cette section décrit comment profiter du support technique et les conditions d'accès à celui-ci.

Façons de profiter du support technique

Si vous ne trouvez pas de solution à votre problème dans la documentation de Kaspersky Security Center Cloud Console ou dans les sources d'information relatives à Kaspersky Security Center Cloud Console, contactez le Support Technique de Kaspersky. Les experts du Support Technique répondront à toutes vos questions concernant l'installation et l'utilisation de Kaspersky Security Center Cloud Console.

Kaspersky apporte un soutien en relation avec Kaspersky Security Center Cloud Console pendant son cycle de vie (voir la page du cycle de vie du support de l'application). Avant de contacter le Support Technique, il est recommandé de lire les règles d'octroi du support technique.

Vous pouvez contacter les experts du Support Technique d'une des manières suivantes :

- En vous rendant sur le site Internet du Support Technique
- En envoyant une demande au Support Technique via le portail Kaspersky CompanyAccount

Support technique via le Kaspersky CompanyAccount

Kaspersky CompanyAccount est un portail dédié aux entreprises utilisant les applications Kaspersky. Le portail Kaspersky CompanyAccount vise à permettre l'interaction entre les utilisateurs et les spécialistes de Kaspersky via des requêtes en ligne. Vous pouvez utiliser Kaspersky CompanyAccount pour suivre l'état des requêtes en ligne et en stocker également un historique.

Vous pouvez enregistrer tous les employés de votre entreprise dans un seul compte utilisateur Kaspersky CompanyAccount. Ce compte utilisateur unique vous permet de centraliser l'administration des requêtes électroniques envoyées à Kaspersky et provenant des employés enregistrés. Il vous permet également d'administrer les privilèges de ces employés Kaspersky CompanyAccount.

Le portail Kaspersky CompanyAccount est disponible dans les langues suivantes :

- anglais ;
- espagnol ;
- italien ;
- allemand ;
- polonais ;
- portugais ;
- russe ;

- français ;
- japonais.

Pour en savoir plus sur le Kaspersky CompanyAccount, veuillez consulter le site Internet du Service de Support Technique.

Informations requises pour les spécialistes du Support Technique de Kaspersky

Lorsque vous contactez les spécialistes du Support Technique de Kaspersky, ils peuvent vous demander de fournir les informations suivantes :

- Informations générales à propos de Kaspersky Security Center Cloud Console
- Identifiant de l'espace de travail
- Informations sur la licence
- Nombre d'applications installées
- Identifiant et état du locataire

Vous pouvez trouver ces informations dans la section **Menu de votre compte** → **Support technique**. Copiez et partagez ces informations pour obtenir de l'aide à propos de votre problème.

Sources d'informations sur l'application

Page Kaspersky Security Center Cloud Console sur le site Web Kaspersky

La page de Kaspersky Security Center Cloud Console sur le site Internet de Kaspersky fournit des informations générales sur l'application, ses possibilités et ses particularités.

Page Kaspersky Security Center Cloud Console dans la Base de connaissances

La *Base de connaissances* est une section du site Internet du Support Technique de Kaspersky.

Sur la page Kaspersky Security Center Cloud Console 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 Cloud Console et à d'applications de Kaspersky. Les articles de la Base de connaissances peuvent également contenir des actualités du Support Technique.

Discuter des applications Kaspersky avec la communauté

Si votre question n'est pas urgente, vous pouvez la poser aux experts de Kaspersky et aux autres utilisateurs de notre forum.

Le forum vous permet d'afficher des sujets de discussion, d'envoyer des commentaires et de créer de nouveaux sujets de discussion.

> L'accès aux sites Internet requiert une connexion à Internet.

Si vous ne trouvez pas la solution à votre problème, contactez le Support Technique.

Problèmes connus

Kaspersky Security Center Cloud Console présente une série de restrictions qui n'ont pas une incidence critique sur le fonctionnement de l'application :

- Vous ne pouvez pas ajouter plusieurs fois un paquet d'installation avec la même langue de localisation. Par exemple, si vous avez déjà ajouté le paquet d'installation de Kaspersky Endpoint Security for Windows (anglais), vous pouvez ajouter des paquets d'installation de Kaspersky Endpoint Security for Windows localisés dans d'autres langues, à l'exception de l'anglais.

- Lorsque vous essayez d'activer la solution MDR de Kaspersky, une erreur se produit si les services MDR ne sont pas disponibles.

- Dans la stratégie de Kaspersky Endpoint Security for Mac, dans la section **Protection avancée contre les menaces**, si vous cliquez plusieurs fois sur le bouton **Déclaration de KSN**, la fenêtre contenant la Déclaration KSN s'ouvre autant de fois que vous avez cliqué sur le bouton.

- Dans la fenêtre **Détails de l'alerte**, si vous cliquez sur un lien qui ouvre une autre section, puis essayez de revenir et cliquez sur le bouton **Précédent** de votre navigateur (ou appuyez sur **`Alt`** + **`Gauche`**), la fenêtre **Détails de l'alerte** se charge indéfiniment.

- Lorsque vous essayez de supprimer la dernière clé de licence dans la section **Licences pour les logiciels de Kaspersky**, le bouton **Supprimer** dans la fenêtre de confirmation n'est pas visible si le thème de l'interface sombre de Web Console est activé.

- Dans la stratégie Kaspersky Endpoint Security for Mac, si vous activez l'intégration avec KATA et que vous n'indiquez pas l'adresse du serveur ni le certificat, toute tentative d'activation de la fonctionnalité de Contrôle Internet renvoie une erreur.

- 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.

- Une fois que la tâche *Analyse d'inventaire* est terminée pour un appareil Linux, une tentative d'envoi des fichiers reçus à Kaspersky pour analyse renvoie une erreur.

- Si vous essayez de vous connecter à Kaspersky Security Center Cloud Console en vous servant des Active Directory Federation Services (AD FS), mais que les autorisations requises sont manquantes, Kaspersky Security Center Cloud Console renvoie toujours l'erreur « Identifiants non valides » au lieu d'avertir l'utilisateur des autorisations manquantes.

- La tâche Administrer les appareils ne fonctionne pas correctement pour les appareils fonctionnant sous macOS.

- Dans la fenêtre de Diagnostic à distance, cliquer sur le bouton **Télécharger le fichier entier** peut entraîner un téléchargement incorrect.

- Une vulnérabilité tierce (hors logiciels Microsoft) ignorée n'apparaît pas dans le diagramme des **Statistiques de vulnérabilité sur les appareils**.

Glossaire

Administrateur de Kaspersky Security Center Cloud Console

Personne qui gère les opérations de l'application via le système d'administration centralisé à distance Kaspersky Security Center Cloud Console.

Agent d'administration

Le module de l'application Kaspersky Security Center Cloud Console qui coordonne les interactions entre le Serveur d'administration et les applications Kaspersky installées sur un poste spécifique du réseau (un poste de travail ou un serveur). Ce module est commun à toutes les applications de l'entreprise développées pour Microsoft® Windows®. Il existe d'autres versions de l'Agent d'administration pour les applications Kaspersky développées pour les SE Unix et MacOS.

Agent d'authentification

Interface permettant après le chiffrement du disque dur de chargement de passer la procédure d'authentification pour accéder aux disques durs chiffrés et charger le système d'exploitation.

Appareil administré

Un ordinateur sur lequel l'Agent d'administration est installé ou un appareil mobile sur lequel une application de sécurité Kaspersky est installée.

Appareil protégé au niveau UEFI

Appareil doté au niveau BIOS d'une solution ou d'une application Kaspersky pour UEFI. La protection intégrée assure la sécurité de l'appareil au début du lancement du système quand la protection des appareils qui ne sont pas dotés de l'application intégrée commence à fonctionner uniquement après le lancement de l'application de sécurité.

Application incompatible

Application antivirus d'un éditeur tiers ou application de Kaspersky qui n'est pas compatible avec l'administration par Kaspersky Security Center Cloud Console.

AWS Application Program Interface (AWS API)

Interface logicielle de l'application de la plateforme AWS utilisée par l'application Kaspersky Security Center Cloud Console. Plus précisément, les outils de l'API AWS sont utilisés pour le sondage des segments dans le Cloud.

Base antivirus

Bases de données contenant des informations sur les menaces informatiques connues de Kaspersky au moment de la publication des bases antivirus. Les entrées dans les bases antivirus permettent de détecter les codes malveillants dans les objets analysés. Les bases antivirus sont créées par les experts de Kaspersky et sont actualisées toutes les heures.

Clé active

Une clé en cours d'utilisation par l'application.

Clé d'accès AWS IAM

Combinaison comprenant l'identifiant de la clé (de type " AKIAIOSFODNN7EXAMPLE ") et la clé secrète (de type " wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY "). Une paire appartient à l'utilisateur IAM et est utilisée pour avoir accès aux services AWS.

Clé de licence complémentaire (ou de réserve)

La clé qui confirme le droit d'utilisation de l'application, mais non utilisée au moment actuel.

Cloud Discovery

Cloud Discovery est un module de la solution Cloud Access Security Broker (CASB) qui protège l'infrastructure cloud d'une organisation. Cloud Discovery gère l'accès des utilisateurs aux services cloud. Les services cloud incluent, par exemple, Microsoft Teams, Salesforce et Microsoft Office 365. Les services cloud sont regroupés en catégories, par exemple, *Échange de données*, *Messageries*, *Email*.

Compte utilisateur sur Kaspersky Security Center Cloud Console

Compte utilisateur que vous devez avoir pour configurer Kaspersky Security Center Cloud Console, par exemple, en ajoutant et en supprimant des comptes utilisateurs et en configurant des profils de sécurité (stratégies de sécurité). Ce compte permet d'utiliser le service My Kaspersky. Vous créez ce compte lorsque vous commencez à utiliser Kaspersky Security Center Cloud Console.

Console de gestion AWS

L'interface Internet pour voir et administrer les ressources AWS. La console de gestion AWS est accessible sur Internet à la page https://aws.amazon.com/console/.

Domaine 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).

Durée de validité de la licence

Période au cours de laquelle vous pouvez utiliser les fonctions de l'application et les services complémentaires. Le volume des fonctions accessibles et des services complémentaires dépend du type de licence.

Espace de travail

Une instance de Kaspersky Security Center Cloud Console créée pour une entreprise en particulier. Lorsqu'un client crée un espace de travail, Kaspersky crée et configure l'infrastructure et une Console d'administration basée sur le cloud qui sont nécessaires pour gérer les applications de sécurité installées sur les appareils de l'entreprise.

État de la protection

État actuel de la protection qui représente le niveau de sécurité de l'ordinateur.

État de la protection du réseau

L'état actuel de la protection qui caractérise le niveau de sécurité des appareils du réseau de l'entreprise. L'état de la protection du réseau inclut les éléments suivants : la présence des applications de sécurité installées sur les appareils du réseau, l'utilisation de clés de licence, le nombre et les types des menaces détectées.

Fichier clé

Le fichier de type xxxxxxx.key qui permet d'utiliser l'application de Kaspersky à l'aide de la licence d'évaluation ou commerciale.

Gestion centralisée des applications

Gestion à distance des applications à l'aide des services d'administration proposés par Kaspersky Security Center Cloud Console.

Gestion des identités et des accès (IAM)

Un service d'AWS qui permet d'administrer l'accès des utilisateurs aux autres services et ressources d'AWS.

Gestion directe des applications

Gestion des applications par l'interface locale.

Gravité de l'événement

Caractéristique de l'événement consigné dans le fonctionnement de l'application de Kaspersky. Les niveaux de gravité sont les suivants :

- Événement critique
- Erreur de fonctionnement
- Avertissement
- Information

Les événements du même type peuvent avoir différents niveaux de gravité, en fonction du moment où l'événement s'est produit.

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.

HTTPS

Le protocole protégé du transfert de données entre le navigateur et le serveur Web avec l'utilisation du chiffrement. HTTPS est utilisé pour accéder aux informations internes telles que les données corporatives et financières.

Image machine Amazon (AMI)

Un modèle contenant la configuration du logiciel indispensable au lancement de la machine virtuelle. Il est possible de créer plusieurs instances au départ d'une seule AMI.

Installation à distance

Installation des applications de Kaspersky à l'aide des outils offerts par l'application Kaspersky Security Center Cloud Console.

Installation forcée

Méthode d'installation à distance des applications de Kaspersky qui permet de réaliser l'installation à distance de l'application sur des appareils clients définis. Pour garantir la réussite de l'exécution de la tâche via la méthode de l'installation forcée, le compte utilisateur de lancement de la tâche doit posséder les autorisations de lancement des applications sur les appareils clients. La méthode donnée est recommandée pour l'installation des applications sur les appareils administrés sous les systèmes d'exploitation Microsoft Windows qui permettent cette possibilité.

Installation locale

Installation de l'application de sécurité sur l'appareil du réseau de l'entreprise qui prévoit le lancement manuel d'installation à partir du paquet de distribution de l'application de sécurité ou le lancement manuel du paquet d'installation publié préalablement téléchargé sur l'appareil.

Instance d'Amazon EC2

Une machine virtuelle créée sur la base d'une image AMI à l'aide d'Amazon Web Services.

JavaScript

Le langage de programmation qui élargit les possibilités des pages Web. Les pages Web créées avec JavaScript sont capables d'exécuter les actions complémentaires (par exemple, modifier les types des éléments de l'interface ou ouvrir les fenêtres supplémentaires) sans la mise à jour de la page Web par les données depuis le serveur Web. Pour consulter les pages Web créées à l'aide de JavaScript, il faut activer le support JavaScript dans les paramètres du navigateur.

Kaspersky Next Expert View

Une application conçue pour l'exécution centralisée des tâches d'administration et de gestion de base sur le réseau d'une organisation. Kaspersky Next Expert View est hébergé et géré par Kaspersky. L'application fait partie de la solution cloud Kaspersky Next. Dans le cadre de cette solution, vous pouvez également utiliser Kaspersky Next Pro View.

Kaspersky Private Security Network (KPSN)

Kaspersky Private Security Network est une solution qui permet aux utilisateurs d'appareils qui ont installé des applications Kaspersky d'accéder aux bases de données de réputation de Kaspersky Security Network et à d'autres données statistiques sans envoyer de données de leurs appareils à Kaspersky Security Network. Kaspersky Private Security Network est conçu pour les entreprises qui ne peuvent pas participer à Kaspersky Security Network pour l'une des raisons suivantes :

- Les appareils ne sont pas connectés à Internet.

- La loi ou les stratégies de sécurité de l'entreprise interdisent la transmission de données en hors du pays ou du réseau local de l'entreprise.

Kaspersky Security Network (KSN)

Infrastructure des services cloud et offrant l'accès à la base de données de Kaspersky avec des informations constamment mises à jour sur la réputation des fichiers, des ressources Internet et du logiciel. L'utilisation des données de Kaspersky Security Network assure une vitesse de réaction plus élevée des applications de Kaspersky sur les menaces, augmente l'efficacité de fonctionnement de certains modules de protection, ainsi que diminue la possibilité des faux positifs.

Mise à jour

Procédure de remplacement ou d'ajout de nouveaux fichiers (bases de données ou modules de l'application) récupérés sur les serveurs de mise à jour de Kaspersky.

Mise à jour disponible

Un ensemble de mises à jour pour les composants d'applications de Kaspersky, y compris les mises à jour critiques accumulées au fil d'une certaine période.

Niveau d'importance du correctif

Attribut du correctif. Il existe cinq niveaux d'importance pour les correctifs de Microsoft et les correctifs d'éditeurs tiers :

- Critique
- Élevé
- Moyen
- Faible
- Inconnu

Le niveau d'importance du correctif d'un éditeur étranger ou de Microsoft est défini par le niveau de gravité le plus défavorable de la vulnérabilité corrigé par le correctif.

Opérateur de Kaspersky Security Center Cloud Console

Utilisateur qui est responsable de l'état et du fonctionnement du système de protection administré à l'aide de Kaspersky Security Center Cloud Console.

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 Cloud Console. Le paquet d'installation contient un ensemble de paramètres nécessaires pour installer une application et assurer son efficacité immédiatement après l'installation. Les valeurs des paramètres correspondent aux valeurs des paramètres de l'application par défaut. Le paquet d'installation est créé sur la base de fichiers aux extensions .kpd et .kud inclus dans la distribution de l'application.

Paramètres de l'application

Paramètres des applications, communs à tous les types de tâches et servant au fonctionnement de l'application dans son ensemble, par exemple : paramètres de performances de l'application, paramètres de gestion des rapports, paramètres de la Sauvegarde.

Paramètres de la tâche

Paramètres des applications propres pour chaque type de tâche.

Passerelle des connexions

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

Plug-in Web d'administration

Un module spécial utilisé pour l'administration à distance du logiciel Kaspersky via Kaspersky Security Center Cloud Console. Un plug-in d'administration est une interface entre Kaspersky Security Center Cloud Console et une application spécifique de Kaspersky. Un plug-in d'administration permet de configurer des tâches et des stratégies pour l'application.

Point de distribution

Ordinateur avec un Agent d'administration installé, utilisé pour la diffusion des mises à jour, le sondage du réseau, l'installation à distance des applications, la collecte d'informations sur les ordinateurs faisant partie du groupe d'administration et/ou d'un domaine multidiffusion. L'administrateur sélectionne les appareils appropriés et leur attribue manuellement des points de distribution.

Profil de la stratégie

Sous-ensemble nommé de paramètres de stratégie. Ce sous-ensemble est diffusé sur les appareils avec la stratégie et vient compléter la stratégie quand une condition définie, la condition d'activation du profil, est remplie.

Propagation de virus

Tentatives multiples d'infection d'un appareil par un virus.

Propriétaire de l'appareil

Le propriétaire de l'appareil est un utilisateur que l'administrateur peut contacter lorsqu'il faut exécuter certaines opérations sur un appareil.

Protection antivirus du réseau

L'ensemble de mesures techniques et d'organisation qui diminuent la possibilité d'intrusion des virus et du spam sur les appareils de réseau de l'entreprise et qui empêchent les attaques de réseau, le phishing et les autres menaces. La protection antivirus du réseau est augmentée lors de l'utilisation des applications de sécurité et des services, et lors de la présence et l'observation de la stratégie de la protection d'information dans l'entreprise.

Quarantaine

Un stockage spécial qui contient les fichiers probablement infectés par les virus ou irréparables lors de la découverte.

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.

Rôle IAM

Ensemble de droits pour l'exécution des demandes vers les services AWS. Les rôles IAM ne sont liés à aucun utilisateur ou groupe existant et octroient des droits d'accès sans utilisation des clés d'accès AWS IAM. Vous pouvez attribuer un rôle IAM aux utilisateurs IAM, aux instances EC2 et aux applications ou services basés sur AWS.

Serveur d'administration

Composant de Kaspersky Security Center Cloud Console qui stocke de manière centralisée des informations sur toutes les applications Kaspersky installées sur le réseau d'entreprise. et d'un outil efficace d'administration de ces applications.

Serveur d'administration domestique

Le Serveur d'administration domestique est le Serveur d'administration qui a été indiqué lors de l'installation de l'Agent d'administration. Le Serveur d'administration domestique peut être utilisé dans les paramètres des profils de connexion de l'Agent d'administration.

Serveur d'administration virtuel

Le module de l'application Kaspersky Security Center Cloud Console 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 secondaire.
- La création des Serveurs d'administration secondaires (y compris les Serveurs virtuels) n'est pas prise en charge par le Serveur d'administration virtuel.

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.

Seuil d'activité de virus

Nombre d'événements d'un type donné et générés dans un intervalle de temps déterminé qui, une fois dépassé, permettra à l'application de considérer qu'il y a augmentation de l'activité virale et développement d'une menace de propagation de virus. Ces données peuvent être utiles en période de propagation de virus et permettent à l'administrateur de réagir opportunément aux menaces d'une attaque de virus.

SSL

Le protocole du chiffrement des données dans les réseaux locaux et dans Internet. SSL est utilisé dans les applications Web afin de créer les connexions sécurisées entre client et serveur.

Stockage d'événements

Partie de la base de données du Serveur d'administration conçue pour le stockage des information sur les événements qui se produisent dans Kaspersky Security Center Cloud Console.

Stratégie

Une stratégie détermine les paramètres d'une application et gère la capacité de configurer cette application sur les ordinateurs d'un groupe d'administration. Pour chaque application, il est nécessaire de créer une stratégie. Vous pouvez créer plusieurs stratégies différentes pour les applications installées sur les ordinateurs dans chaque groupe d'administration, mais il n'est possible d'appliquer qu'une seule stratégie à la fois à chaque application dans un groupe d'administration.

Tâche

Fonctions exécutées par une application de Kaspersky sont effectuées sous la forme de tâches, par exemple : Protection en temps réel des fichiers, Analyse complète de l'ordinateur et mise à jour des bases de données de données.

Tâche de groupe

Tâche définie pour un groupe d'administration et exécutée sur tous les appareils clients de ce groupe.

Tâche locale

La tâche définie et exécutée sur un ordinateur client particulier.

Tâches pour l'ensemble d'appareils

La tâche définie pour un ensemble d'appareils clients parmi des groupes d'administration aléatoires et exécutée sur ces derniers.

Tag de l'appareil

Un identificateur de l'appareil qui peut être utilisé pour regrouper, décrire ou rechercher des appareils.

Tag de l'application

Libellé pour les applications tierces 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.

Utilisateur IAM

Utilisateur des services AWS. Un utilisateur IAM peut posséder les privilèges de sondage du segment dans le Cloud.

Vulnérabilité

Un défaut au sein d'un système d'exploitation ou d'une application qui pourrait être exploité par un auteur d'application malveillante afin de s'introduire dans le système d'exploitation ou l'application et d'en endommager l'intégrité. Un nombre important de vulnérabilités dans un système d'exploitation fragilise ce dernier car les virus qui s'installent dans le système d'exploitation peuvent provoquer des échecs du système d'exploitation en lui-même et des applications installées.

Zone démilitarisée (DMZ)

La zone démilitarisée est un segment du réseau local où se trouvent les serveurs qui répondent aux requêtes Internet. Afin de garantir la sécurité du réseau local, l'accès à celui-ci depuis la zone démilitarisée est limité et protégé par un pare-feu.

Informations sur le code tiers

Des informations sur le code tiers sont contenues dans le fichier legal_notices.txt.

Le fichier legal_notices.txt se trouve également dans le dossier d'installation de l'Agent d'administration pour Windows et de l'Agent d'administration pour Linux.

Pour plus d'informations sur le code tiers utilisé pour les espaces de travail, consultez la documentation de Kaspersky Endpoint Security Cloud.

Avis de marques déposées

Les autres noms et marques déposés appartiennent à leurs propriétaires respectifs.

Adobe, Acrobat, Flash, PostScript, Reader, Shockwave sont des marques commerciales ou déposées d'Adobe aux États-Unis et/ou dans d'autres pays.

AMD64 est une marque ou une marque déposée d'Advanced Micro Devices, Inc.

Amazon, Amazon EC2, Amazon Web Services, AWS et AWS Marketplace sont des marques commerciales d'Amazon.com, Inc. ou de ses sociétés affiliées.

Apache est soit une marque déposée, soit une marque d'Apache Software Foundation.

Apple, App Store, AppleScript, FileVault, iPhone, iTunes, Mac, Mac OS, macOS, OS X, Safari et QuickTime sont des marques d'Apple Inc.

Arm est une marque déposée d'Arm Limited (ou de ses filiales) aux États-Unis et/ou ailleurs.

Le nom commercial Bluetooth et le logo appartiennent à Bluetooth SIG, Inc.

Ubuntu, LTS sont des marques déposées de Canonical Ltd.

Cisco, IOS, Cisco Jabber sont des marques ou des marques déposées de Cisco Systems, Inc. et/ou de ses filiales enregistrées aux États-Unis et dans certains pays.

Citrix, XenServer sont des marques déposées ou des marques commerciales de Cloud Software Group, Inc. et/ou de ses filiales aux États-Unis et/ou dans d'autres pays.

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.

Corel et CorelDRAW sont des marques ou des marques déposées de Corel Corporation et/ou de ses filiales au Canada, aux États-Unis et/ou dans d'autres pays.

Dropbox est une marque déposée de Dropbox.

Radmin est une marque déposée de Famatech.

Firebird est une marque déposée de la Fondation Firebird.

Foxit est une marque déposée de Foxit Corporation.

FreeBSD est une marque déposée de The FreeBSD Foundation.

Google, Android, Chrome, Dalvik, Firebase, Google Chrome, Google Earth, Google Maps, Google Play, Google Public DNS sont des marques de Google LLC.

HUAWEI, HUAWEI CLOUD et EulerOS sont des marques commerciales de Huawei Technologies Co., Ltd.

Intel et Core 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, ActiveX, BitLocker, Excel, Hyper-V, InfoPath, Internet Explorer, Microsoft Edge, MS-DOS, MultiPoint, Office 365, OneNote, Outlook, PowerPoint, PowerShell, Segoe, Skype, SQL Server, Tahoma, Visio, Win32, Windows, Windows Azure, Windows Media, Windows Mobile, Windows Phone, Windows Server et Windows Vista sont des marques du groupe Microsoft.

CVE est une marque commerciale déposée de The MITRE Corporation.

Mozilla, Thunderbird, Firefox sont des marques déposées de la Fondation Mozilla aux États-Unis et dans d'autres pays.

Novell est une marque commerciale de Novell Enterprises Inc. déposée aux États-Unis et dans d'autres pays.

NetWare est une marque commerciale de Novell Inc. déposée aux États-Unis et dans d'autres pays.

OpenVPN est une marque commerciale d'OpenVPN, Inc.

Oracle, Java, JavaScript 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.

Python est une marque ou une marque déposée de Python Software Foundation.

Red Hat, Red Hat Enterprise Linux, CentOS et Fedora sont des marques ou des marques déposées de Red Hat, Inc. ou de ses filiales aux États-Unis et dans d'autres pays.

BlackBerry appartient à Research In Motion Limited, déposée aux États-Unis et peut être en cours de dépôt déposée dans d'autres pays.

SAMSUNG est une marque de SAMSUNG aux États-Unis ou dans d'autres pays.

Debian une marque déposée de Software in the Public Interest, Inc.

Splunk est une marque commerciale et une marque déposée 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.

Rocky Linux est une marque déposée de The Rocky Enterprise Software Foundation.

UNIX est une marque commerciale déposée aux États-Unis et dans d'autres pays, sous licence exclusive via X/Open Company Limited.